Mykhailo Fedorov, Leading Figure of Ukraine's Drone War

From the State in a Smartphone to the Defense Ministry of the Drone War

Kim Kyung-jin

Table of Contents

Preface. From a Nation Inside a Smartphone to the Battlefield

The promise to put the government onto a smartphone screen sounded, in peacetime, like the language of convenience. It was a promise that pulling documents, paying taxes, and proving who you are would take only a few movements of a finger. When Russian forces crossed the border in February 2022, that screen took on other work. It became the counter where money was sent to refugees, where destroyed homes were reported, where the positions of enemy troops were gathered, and where communications at the front were kept alive.

The man who pushed that change through is Mykhailo Fedorov. He handled digital work in Zelensky's election campaign, and then became a minister at twenty-eight. Diia, the IT Army, Starlink, UNITED24, Brave1, an army of drones — these names attached themselves to his record one after another. In January 2026 he became minister of defense. The man who had designed a nation inside a smartphone was handed the weapons and manpower, the procurement and the data, of a country at war.

No heroic tale was constructed here. Government announcements are left in the government's words, corporate announcements in the companies' words, criticism from YouTube broadcasts as the claims of whoever spoke them. Where a number had no denominator, the blank was left visible. The reason his childhood and family history are not written at length is the same. The moment a gap is filled with a plausible sentence, biography turns into a novel.

Fedorov's career shows how quickly technology and power can draw close to one another. The team that built an app came to handle battlefield data, and the man who nurtured startups took charge of the ministry that signs contracts with those very companies. In a war where speed saves lives, slow procedure is hard to bear. Yet where procedure has been stripped away, the question of who decided and who answers for it remains.

The reference date is July 13, 2026. Neither the war nor Fedorov's term has ended. This is not a completed life but an interim record of power still in motion. Even in the final chapter, judgment was not rushed. What has come to light is written precisely, and claims not yet verified are marked at their edges. Before a reader comes to like or to hate Fedorov, I hope they can first see how the circuitry he built actually worked.

July 2026, Attorney Kim Kyung-jin

Chapter 1. A Twenty-Eight-Year-Old Minister and the Diia Revolution

On 29 August 2019, Ukraine's parliament confirmed the roster of a new cabinet. The Ministry of Digital Transformation came into existence for the first time that day, and twenty-eight-year-old Mykhailo Fedorov became its first minister. The goal he announced was "the state in a smartphone."

Within the public record, his birth in 1991 and everything he did before 2019 rest on a single tertiary document. The arithmetic that makes him twenty-eight at the moment of appointment holds up. But no primary document has been secured to support the phrase that usually trails after his name, "the youngest minister in Ukraine's history." So instead of reconstructing his youth, we begin from what remains: an app, a body of law, a data exchange platform, reports from international organizations, and the criticism that attached itself to all of it. Filling an undocumented role with story lengthens the sentences without adding anything underneath them.

1. A Campaign's Digital Strategist Enters Government

In Ukraine's 2019 presidential election, the weapons in Volodymyr Zelensky's campaign were social media, video platforms, and messaging apps. The evening news on broadcast television and the front pages of the national dailies were not on that stage. Fedorov ran the digital side of this campaign, and once the election was over he entered government.

No primary document showing what decisions he made inside the campaign, or what he said to whom, appears in the secured list of sources. It would be easy enough to write in the air of a meeting room or a scene of working through the night, but sentences written that way cannot carry any of the weight of the foundation. What can be confirmed is the outcome. The new government created a ministry devoted entirely to digital transformation, and the campaign's digital director took its chair.

Create a ministry and a budget is allocated to it, the power to demand things of other ministries comes with it, and a standard for measuring results is set. The goals Ukraine's government handed this ministry survive in writing. Move public services online by 2024, provide digital skills training to millions of citizens, widen internet access across the country, and grow information technology's share of the economy.

What is contained here are targets the Ukrainian government set for itself, which differ from achievements verified by an outside body. A government's goals, a government's announcements, and third-party verification carry different weights. Line all three up in the same size of type and the reader will, without noticing, take promotional copy for fact. This distinction is a line that must be applied again every time one of the numbers that follows appears.

Digital technology sat at the center of his work from the start. Reports from various international organizations and research institutes repeat a similar diagnosis. Ukrainian administration had long stood on service windows, paper forms, and middlemen. Getting a single title certificate meant visiting government offices several times, and the citizen had to carry the paper received at one window over

to another window personally. The longer the line and the murkier the procedure, the more room opens for someone to step in offering to let you skip that line. Reports from the Brookings Institution and the Organisation for Economic Co-operation and Development (OECD) describe moving services online as reducing the points where person meets person, and they record the logic that fewer such points mean fewer roles for money to change hands under the table. The Stanford Social Innovation Review reads Ukraine's digital administration not as a question of administrative efficiency but as a question of trust in the state. In a country where citizens do not believe their state, changing the way the state and its citizens meet is a technical project and a political project at once.

This explanation has not yet been verified. The proposition that removing the service window reduces corruption is plausible. But where the window disappears, a database remains, and so do the few hands that manage that database. In place of the person who hid the paper file, there is now a person who holds the right to reach the data. Whether corruption vanished or merely moved to a different place where it can happen is a question that remains to be confirmed separately.

From 2019, Fedorov led the ministry from a position that also carried a deputy prime ministership. The title "First Deputy Prime Minister" was attached during the July 2025 cabinet reshuffle and lasted until he became defense minister in January 2026. Because what this ministry set out to do did not end inside its own walls, rank was authority. The interior ministry held driver's license and vehicle registration information. The justice ministry held title deeds and birth records; the tax authority held taxpayer numbers. A bundle of official records like these is called a "registry" in administrative language. Think of it as an official roster, organized by category, of what the state knows about a single citizen. The trouble was that these registries sat in different systems in each ministry, in different formats, under different rules. Some used current databases; some were closer to old ledgers. To put a state on a single smartphone screen, these scattered things had to be joined first, and to demand that they be joined, one had to hold the authority to demand.

It is hard to call Diia one man's work. The reports record that money and technical support from international donor agencies, the participation of private development firms, and the data-linking model Estonia had built first were all layered over this project. The minister set the pace at the middle of that layering; other hands wrote the app's code. To name him precisely, one should say assembler, or the man who pushed, rather than inventor. Any assessment of a man who pushes must include what he pushed and also what he pushed off until later.

A ministry's existence does not bring authority along with it automatically. Opening a registry held by another ministry meant amending laws and implementing regulations, and amending a law meant passing a vote in parliament. At the Ministry of Digital Transformation the visible share of the work was the app, but the share that took long hands was legislation. One later case shows this character. Days before the full-scale invasion, Ukraine's parliament passed a cloud services law allowing core state data to be kept in clouds outside the country. Until that law stood, placing state data on foreign servers was not legal. An app appears on a screen within months; the law it stands on moves at the speed of a vote.

The government had to persuade other ministries and other civil servants. Seen from the side that holds the data, data is authority, and a demand to hand over authority is not a welcome one. A role that also carried a deputy prime ministership was a role that could push such demands through. But a rule forced through by strength and a rule built by agreement leave different shapes behind them. When the man who pushed leaves the role, the rules he pushed into being are the first to shake. No primary document recording how this ministry actually handled the fights between ministries appears in the secured list of sources, and so nothing is guessed at here.

The standard by which results are measured also deserves scrutiny. The government set itself the goal of moving services online by 2024, and later offered usage rates and service counts as its report card. The figure of 63 percent, obtained by the United Nations Development Programme in 2023 by asking citizens directly, carries a different weight from a number the government announced about itself, because the one asking stood outside the government. Even so, what this number tells us is how much people use it, not whether money under the table fell by as much as the service window disappeared. No document measuring from outside whether corruption actually fell appears in the secured list of sources.

Evaluating results also means looking at where the money and the technology came from. The reports record that money from international donor agencies, the hands of private development firms, and the model Estonia built first were layered over this project. A system built with outside money and outside technology must be able to stand the day those things are cut off. On how Ukraine's government prepared for that day, the public record stops here. Founding a ministry and making a ministry able to stand alone are different jobs, and the public record shows only the first.

2. Diia and Trembita: Designing the State Inside a Smartphone

In February 2020, the Diia mobile app was released. The first documents it carried were the electronic driver's license and vehicle registration certificate. What had meant pulling a plastic card from a wallet moved onto a smartphone screen. A web portal opened in the same period, and the structure in which app and portal move as a pair was made then.

The Ukrainian word "Diia" (Дія) means "action." On top of this, within Ukraine, people also read the name as an acronym for "Derzhava i ya" (Держава і я), meaning "the state and I." The two explanations are not mutually exclusive, but neither are they the same fact: one is the meaning of a word, the other a play on that word attached afterward. Korean-language introductions often blur the two together and write, "Diia means 'the state and I,'" which is a sentence at odds with the original. It looks like a small problem, but the habit of carrying over even a name without checking the source repeats itself identically in numbers and quotations.

For Diia to work, something must connect the documents of government agencies to one another. The name of that plumbing is Trembita. Trembita is a government data exchange platform that links the state registries held separately by ministries and agencies, letting them pass data back and forth according to fixed rules. Ukraine adapted the X-Road family of data-linking models, built first by Estonia, to its own circumstances.

Trembita's operation is easy to describe. Suppose every ministry has a warehouse where it stacks its documents. The old way had the citizen visit each warehouse, copy a document, and carry it to another warehouse; the citizen was the courier. Trembita laid a corridor of fixed specification between warehouse and warehouse. Which warehouse can release which document under which conditions is decided in advance, and anything meeting the specification travels automatically. Now the system moves the documents, and Diia remains as the screen fixed to the end of that corridor.

The central claim of Diia's design comes out of this structure: that the Diia app itself does not stockpile citizens' personal information. The explanation is that the app pulls information from the original registry through Trembita at the moment it is needed and puts it on the screen, and when the screen closes, that information does not stay in the app. Fedorov called this a "data in transit" structure. Since the data does not pool in one place, the logic runs, breaking into the app yields no heap of data to carry off.

It is a convincing design, but the source must be recorded precisely. The main basis for the statement that the app stores no personal information is the explanation given by Ukraine's government and the responsible minister himself. Within the public record there is no report from an outside body that independently audited Diia's source code or server configuration. Design intent and actual implementation can diverge, and whether the implementation matched the intent is only meaningful when confirmed from outside the party that built it. What can be said now goes as far as "Ukraine's government stated that it designed the system this way," and sentences that went further have been left out of the main text.

The documents and services carried in the app grew quickly. Electronic student IDs, taxpayer numbers, birth registration, business registration, and infectious disease vaccination certificates came in one after another. Things that had required a trip to a service window if you wanted them on paper moved one by one onto the screen. In 2021 Ukraine's government introduced a digital passport with the same legal force as a paper passport and announced it as a "world first." That "world first" is a Ukrainian government announcement, and no independent document comparing it point by point against other countries' systems appears in the secured list of sources. Such phrasing is powerful as promotional copy, but when it is carried over into a statement of fact, the party making the announcement must be named alongside it.

Diia's users grew quickly. In a survey the United Nations Development Programme (UNDP) conducted in 2023, 63 percent of Ukrainians said they used state electronic services. Public services reachable through the app and portal later grew to around 150. Both numbers are values from several years after launch, and a full-scale invasion happened in between. The endpoint of a growth curve must not be used as the report card for the starting point. Diia in 2020 was an app with a driver's license in it; 150 services and 63 percent are what that app looked like after growing for several years.

If Diia was the app for citizens, a different mechanism was placed on the industry side. Diia.City is a legal institution. It is an institutional zone letting information technology firms operate inside Ukraine under separate tax and contract rules; the enabling law was prepared in 2021 and it began operating in early 2022. The purpose was clear. Rather than have Ukraine's software developers be employed

by foreign entities or leave the country, get them to found companies at home and pay taxes here. Holding on to a country's talent is slower and noisier work than building one more app, because it means touching tax and employment rules, and the moment you touch them, interests collide.

Diia is the screen citizens use, Trembita is the foundation joining agencies' documents, and Diia.City is the institution for information technology firms. With only a screen there is no data to show, with only plumbing there is no way for citizens to use it, and with only an institution there is no one to build anything.

The Brookings Institution points to the fact that this combination was already running at a considerable level before the war as the precondition for Ukraine's digital resilience. What was built before the war was what got used in the war. Analysis from Harvard's Kennedy School likewise refuses to read the Ukrainian case as a story of crisis breeding innovation. It reads it as a story of capacity accumulated before the crisis being revealed by the crisis. Many sentences render a few days of February 2022 dramatically, but what made those few days possible were the several years before them.

The same reports attach conditions. The Organisation for Economic Co-operation and Development notes that Ukraine's digital transformation did not reach evenly into regions the internet does not touch, or to the elderly, or to low-income households. Without a smartphone you cannot enter the state inside a smartphone. This problem is solved by political choices: how many offline service windows to keep, and how much budget to spend on the windows kept. Technology alone does not solve it, and statistics boasting of the speed of the shift online do not capture the results of that choice well.

They also tested in advance whether the system could hold up under attack. In an interview, Minister Fedorov said that in 2021 they gathered ethical hackers from around the world and offered bounties of several million hryvnia to try to break into Diia. Ethical hackers are people who attack a system with permission in order to find its weak points. Three or four months before the invasion, he said, they created an in-house attacking unit inside the government called a "red team" and had it hammer Diia, the government portal, and the energy sector without a day's rest. The source for this statement is the minister's own interview, and among the secured public documents there is no outside report separately recording the results of that testing. Attacking yourself and being audited from outside are different things. The first lets the builder decide for itself what it will find; the second finds even what the builder would rather hide.

Where to keep the data was also settled in this period. The cloud services law passed just before the full-scale invasion opened the way to keeping core state data in foreign clouds. Moving servers out of the country means escaping the bombing, and it also means moving under another country's law and another country's corporate terms of service. No document showing what contract set those conditions appears in the secured list of sources. What such a structure costs — the screen and the plumbing built at home, the data entrusted to a foreign company's warehouse — remains a matter that can only be argued on paper until the bill actually comes due.

Diia.City's effects must be verified separately. This zone, applying different tax and contract rules to information technology firms, was a device for holding developers inside the country. But a system that cuts taxes means money leaving the treasury by the amount cut. Whether that money is larger or smaller than the worth of the talent held on to is a calculation that must be done separately. Within the public record there are no statistics measuring from outside how much this institution stopped developers from leaving. Recording an institution's purpose and confirming an institution's effect are different jobs.

3. The Role Where Convenience, Security, and Surveillance Fears Collided

The more convenient a service becomes, the more information travels within one system. Diia was no different. Saying that one person's driver's license and taxpayer number and birth record and business registration can be reached through a single screen also means that whoever holds the key to that screen can see the whole content of that person's life.

Security fears were raised first. The international citizen media outlet Global Voices, in an article titled "Security concerns and legal ambiguity threaten the future of Ukraine's 'state in a smartphone,'" pointed to the vulnerabilities and legal gaps arising as citizens' data gathered into a single system. Ukraine's government answered with the "app that stores no data" logic seen earlier. But the focus of the criticism was the registries behind the app, and the corridors joining those registries. The better the corridor between warehouses is bored, the more opens along with any single warehouse that gets opened.

The fears had precedent. In 2018 it was reported that the personal information of 500,000 customers of Nova Poshta, a large Ukrainian logistics company, had reportedly leaked onto the dark web. The dark web is the region of the internet unreachable by ordinary search and accessed with identity hidden, and inside it are the marketplaces where stolen personal information is bought and sold. It was an incident at a private company, but it is cited in Ukrainian society as a case showing by what route large volumes of personal information get out and where they are traded.

Several years later, in 2023, the National Bank of Ukraine (NBU) announced that losses from financial fraud had risen 73 percent over the previous year. This figure is the central bank's own tally, and it differs from a value calculated by separating out only the losses caused by flaws in Diia. Place the two facts side by side, but do not read one as the cause of the other. The commonsense connection that fraud gets easier in a society where a lot of personal information is loose on the market can be drawn, but no document fixing that connection as causation appears in the secured list of sources.

Alongside security, the surveillance question grew. In 2019 the capital, Kyiv, appeared in survey results naming it among the world's fifty cities with the highest density of surveillance cameras. Ukraine's cities expanded camera networks under the name "Safe City," and facial recognition began to be layered on top. Facial recognition is technology that matches a face captured by a camera against a stored list of photographs and automatically judges who the person is. Unlike a human peering at a screen one image at a time, the machine does not tire and inspects every face. The

Ukrainian social research institute Cedos, in a report titled "Surveillance cameras and the municipal guard. How safe is the 'Safe City'?", noted that this expansion could chill citizens' freedom, and activists likened it to George Orwell's novel, calling it "Big Brother's sharp eye."

Adding cameras and building an app are separate undertakings by separate ministries. Within the public record there is no basis for saying the Ministry of Digital Transformation directed the expansion of urban surveillance networks. But in citizens' eyes they looked like movement in the same direction, because the flow was one in which the state could identify its citizens more finely, record more of them, and stitch those records together faster. The fact that the ministry that made the convenience and the ministry that added the surveillance were different bodies matters administratively, but it is no comfort to the citizen who bears the result.

The manufacturers of the surveillance cameras also became a controversy. A substantial share of the surveillance cameras installed across Ukraine were products of the Chinese firms Hikvision and Dahua. In 2023 the Kyiv Post carried a commentary titled "Trojan Horse: How Chinese Cameras Put Ukraine at Risk," warning that hardware within a foreign government's sphere of influence could become a back door into Ukraine's surveillance network. That piece was closer to opinion. No investigative report technically confirming that a back door actually opened and that something went out through it appears in the secured list of sources, and warning and proof carry different weights.

Parliament also began preparing legislation to protect personal data. A personal data protection bill (draft no. 8153) following the standard of the European Union's General Data Protection Regulation (GDPR) was introduced in Ukraine's parliament in October 2022. The GDPR is the European law that sets who may keep personal data, for what purpose, and for how long, and gives citizens the right to demand access and deletion. The Council of Europe convened an expert discussion and made the point that when the state's data collection powers widen under the exceptional conditions of war, legal safeguards are needed to protect citizens.

The date of introduction is October 2022. Two and a half years had passed since Diia came into the world, and eight months since the full-scale invasion began. The speed of making convenience and the speed of making rules to govern that convenience were not the same. The app arrived within months; the law to govern the data that app handles began being discussed years later. This lag repeats itself in other countries too, but in Ukraine that lag overlapped with a war.

Questions outside the public record remain as well. We were unable to secure a primary report from Ukraine's human rights organizations or civil society groups investigating Diia's data handling directly. A substantial share of the criticism reaches us through foreign media summaries or rebuttals issued by the responsible ministry. A structure in which criticism is read only through rebuttals is dangerous. A rebuttal can pick from among many criticisms the ones easiest to refute and quote those, and can leave the awkward ones unmentioned. Writing that we could not fill the gap is better than writing as though there were no gap.

From 2019 to early 2022, Ukraine moved its administration into the smartphone at a speed matched by few countries in the world. Screen and plumbing and institution were built together, and citizens no

longer queued at a service window. In the same period, the data holding up that convenience was stitched more tightly together, the cameras in the cities multiplied, and the law to handle all of it only began to be discussed late. Achievement and concern are not separate events but two faces of the same event.

Before the war, convenience and security and surveillance were three forces pulling in different directions. What balance these three would settle into had not yet been decided, and deciding that balance was the work of law and politics. On 24 February 2022, one of them overwhelmed the other two, because the state's survival was placed ahead of every other discussion.

Other countries had already drawn a line over where the cameras came from. The United States Federal Communications Commission blocked imports of Hikvision and Dahua equipment on espionage concerns, and the European Parliament stripped out Hikvision devices citing human rights abuses. Ukraine's cities went on using these companies' cameras afterward. On why they kept using them, the public record stops here. There is no investigative record to distinguish whether it was because the price was low, or because there was no budget to buy replacement equipment, or because something else was going on in the procurement. Write what lies outside the public record as though it were confirmed and the sentence becomes an accusation, and an accusation requires evidence.

Facial recognition crosses over from administrative convenience into an instrument of war. Ukraine's government brought the American firm Clearview AI's facial recognition software into military operations. It was reported to have been used this way: photograph a fallen Russian soldier's face, match it against the heap of photographs floating around the internet to learn his identity, then notify that soldier's mother in Russia of his death. This company has been banned or fined in at least four European Union member states over the problem of having collected billions of face photographs from the internet without permission. Ukraine's Digital Security Lab noted that no legal framework governing such military use of the technology exists within Ukrainian law.

When the powers of the agency handling surveillance and security grow, the next question is who watches that agency. In July 2023 the Ukrainian League of Industrialists and Entrepreneurs criticized draft cyber security bill no. 8087 for concentrating too much authority in the State Service of Special Communications and Information Protection. Not long after, Ukraine's National Anti-Corruption Bureau announced that two senior figures at that agency, including its head Yurii Shchyhol, were suspected of siphoning off 62 million hryvnia in the course of buying software, and the two stepped down from their posts and faced investigation. The proposition from the first section — that removing the service window reduces corruption — comes back around here. The paper windows had shrunk, but the window for buying things was still standing.

In November 2023, Ukraine's government attended the AI Safety Summit held in Britain and signed the Bletchley Declaration. A signature is a promise, and a promise is not a rule. Turning a promise into a rule is the work of parliament and the courts, and as we have seen, that work started late.

Chapter 2. February 2022: E-Government Becomes Wartime Infrastructure

On 23 February 2022, a massive wave of connection attempts broke over Ukraine's government networks. Government portals and banking sites wobbled. Countless computers were trying to connect all at once in order to bring the servers to a halt — the method the security industry calls a DDoS attack. At the same hour, a different sort of program began running on several systems. It was malware built to erase files beyond any hope of recovery, and the security industry calls this kind a wiper. The specimens found that day were given the names HermeticWiper and FoxBlade. A number of analytical reports attributed the attack to Sandworm, a hacking group identified as tied to Russia's military intelligence service, the GRU. And at dawn the next day, ground forces crossed the border.

Ukraine's e-government came under attack in February 2022 and kept operating. Yet much of the public documentation supporting that account consists of announcements from the Ukrainian government itself. Only by separating government statements from verification by outside bodies can we see clearly what role Diia actually played in the war.

1. Digital Administration That Never Went Dark, Even on the First Day

A few days before the war began, Ukraine's parliament passed a law permitting the state's core data to be stored in foreign clouds.

Before that change, state records could not be kept outside Ukraine. Until then, Ukrainian law had bound national registries — land titles, residence records — to servers inside the country. The thinking was that data had to sit within the borders for the state to control it, and in peacetime that is a plausible logic. In wartime the meaning shifts. Saying a server sits inside the country also means that server becomes a coordinate on a map, and one bomb on one building can erase an entire nation's property records at a stroke.

The cloud means somebody else's data centers, scattered across the world. You place your documents on servers inside buildings run by companies like Amazon or Microsoft and pull them back over the internet. If one building is destroyed and an identical copy remains in another, the documents survive. What Ukraine changed on the eve of the invasion was the law. The technology already existed in the world; only permission had been missing, and once permission came, the moving remained to be done.

The sheer volume of data was a problem too. National records are measured in petabytes (PB). One petabyte is roughly a million gigabytes. A smartphone holds something like 128 gigabytes, so a petabyte would fill thousands of such phones to the brim. Sending that many documents up through the internet lines of a country where war had just begun was impossible from the start.

Amazon Web Services (AWS) brought a device called Snowball into Ukraine. It is a rugged, high-capacity storage unit that looks like a suitcase. Documents were loaded onto it, carried physically out across the border, and then uploaded to the cloud from a European data center. If the volume was

too great to send over the wire, the idea went, you put it on a truck and drive it across the border. Several reports record that this operation moved somewhere between 10 and 15 petabytes of documents out of the country in about ten weeks, including land registries, property titles, and banking records. Other sources described the same operation as rescuing more than ten million gigabytes of government and economic data. The two figures do not point to different events; they state the same magnitude in different units.

Microsoft made it possible to run Ukrainian government services on its own cloud, Azure, and announced that it had provided 400 million dollars' worth of cloud usage credits free of charge. The amount and the substance come from the company's own disclosure; no document independently verifying how the credits were actually spent appears in the material gathered here. Fedorov said of this work, "You cannot bomb the cloud." His point was that scattering the nation's records across servers on the territory of NATO member states was itself a deterrent.

That formulation deserves scrutiny about its scope rather than acceptance at face value. You may not be able to bomb the cloud, but you can bomb the communications and power networks that reach it, and if the servers live while the lines are cut, a citizen cannot open a single page of what is inside them. A longer shadow falls elsewhere. Placing a nation's records on the servers of foreign private companies also means placing the nation's memory atop those companies' terms of service and the laws of the countries they belong to. If the company changes its policy, where does the nation's memory then stand? Recall Starlink and this question comes back in a far sharper form.

An announcement that the documents were moved does not by itself settle how control over them was arranged, and no answer has emerged yet. No contract has been made public showing who held the encryption keys, whether staff at the foreign data centers could reach the originals, or whether Ukrainian institutions could delete the copies themselves. The achievement of data surviving and the question of who controls that data are separate matters. During the war the first was urgent; when the war ends, the second remains.

In the immediate aftermath of the invasion, the Ukrainian government shut several services down for a time. It severed outside access to a number of national registries by its own hand. To keep the enemy from extracting or erasing documents, locking the door was safer than leaving it open — and the price was that for a while many citizens could not open their electronic documents in Diia.

When the war began, the government suspended some existing services before it rolled out any new ones. A decision to protect the state's documents became an inconvenience for citizens at once, and within a single day the war laid bare the fact that safety and convenience do not move in the same direction.

According to public documents, basic administration continued through the war. Through weeks of power cuts and falling missiles, administrative operations were largely maintained, the banking system kept running, and payments of wages and pensions never stopped. That a considerable share of this assessment reproduces Fedorov's own statements belongs in the same place. The recollections of the minister in charge are testimony about events, and they carry a different weight than findings

confirmed by an outside audit.

The reason the Diia app itself was never breached is generally credited to its design. Diia stores citizens' personal data neither on the phone nor on the app's servers. Through Trembita, the data exchange channel between ministries, it pulls information from the original registries each time it is needed, displays it on the screen, and leaves nothing behind once the screen closes. The documents call this a "data in transition" architecture. It means that even if you break into the app, there is nothing inside to take.

This design was made in peacetime. Security was part of the thinking, but the larger aim was to avoid the old style of administration in which every ministry piled up its own documents separately. Once the war came, the same structure took on a different worth. An app with nothing to steal yields nothing when attacked. A peacetime design principle turned into a wartime line of defense, and a substantial share of what Ukraine accomplished in 2022 happened on the foundation of e-government built up over the years since 2019.

Some roles could not be pinned down. We could not establish documents showing what security checks Ukraine ran before the invasion, or how far it had mapped the weak points in government systems in advance. Nor does the material gathered here contain any externally verified audit report on how many attacks targeted Diia after the invasion, or whether personal data leaked. A structural explanation that the design reduces the risk of leakage and a claim that the number of leaks was in fact zero cannot be treated as equal in weight. The first sentence exists in public documents; the second does not.

Here is what can be confirmed about February 2022. Russia tried to paralyze the state by striking administrative buildings, communications, and power, and Ukraine moved its administration outside the buildings, onto servers beyond the border. A number of reports record that this response worked. That a large share of the voices those reports cite belong to the Ukrainian government itself belongs in the same place.

Behind the ability to move national records across the border in February 2022 lies a chronology stretching back several years. Ukraine's e-government did not grow at leisure in tranquil times. It began after the Maidan revolution of 2014 with the opening of Prozorro, a public procurement platform meant to fight corruption; then in 2019 the Ministry of Digital Transformation was created, bringing in Trembita and Vulyk, the channels connecting documents across ministries. In 2020 the Diia app and portal, Diia.Business for small and medium enterprises, and a system for disbursing COVID-19 relief payments opened one after another, and in early 2022, just before the invasion, Diia City, a tax regime for information technology companies, was launched. What met the war was not one hastily built app but plumbing that had already set hard.

Before the documents could be moved, a legal foundation was needed — the standing to say "move them." The e-government body created in 2014 could cooperate with individual ministries but had no authority to compel compliance. In 2019 that work passed to the newly created Ministry of Digital Transformation, which by 2023 had grown past 300 people. The ministry does not build other

ministries' services directly. It manages Trembita and Diia while standing in a supervisory position, coordinating digital projects across the whole of government. Parliament has a Committee on Digital Transformation that supports this work as well. The decision to move a nation's records wholesale onto servers beyond the border was a question of authority before it was one of technology, and the opening to give that order had already been made three years before the invasion.

Not much is known about the judgments made by the parties on the other side of the table. No document in the material reviewed here shows why Amazon and Microsoft decided to hand over equipment and credits, or what discussions inside those companies produced the decision. The two firms took the national records of a country at war into their own buildings, and those records are still there. We could not obtain documents confirming what contractual terms were attached, how long the storage would last, or where the documents were to be returned once the war ends. A company's goodwill is not a contract, and goodwill without a contract can be withdrawn at any time.

2. eVorog and Citizen Reporting: The War in Which Civilians Became Sensors

In March 2022, a month after the invasion, a chatbot appeared on Telegram, the messenger Ukrainians used every day. Its name was eVorog (єВорог) — eEnemy in English, "electronic enemy" if we render it plainly. A chatbot is a channel where a program handles the conversation automatically. If citizens spotted Russian troops, equipment, or convoys, they could send geotagged photos, video, and a short description to this channel, and what came in was passed along to military intelligence channels for analysis.

What Ukraine did was connect a device already in everyone's pocket to a single channel. No new weapon and no new unit were required. The hole in that connection shows immediately. If anyone can send, the enemy can send too. You could flood it with fake coordinates and make friendly artillery strike the wrong place; you could pour in useless reports and paralyze the people doing the verification. A system open wide to information is open just as wide to false information.

Even a report that passes authentication is not guaranteed to be accurate. A civilian's eyes and a military analyst's eyes are different. There is no reason the type and number of tanks glimpsed through smoke and noise and fear would be correct. A frightened person overcounts; someone watching from far off confuses one type with another. So there has to be a filtering procedure. The documents record that verified citizen reports flow, together with information from drones, satellites, and scouts, into a system called DELTA. DELTA is a battlefield awareness platform that layers information arriving from many places onto a single digital map and shows commanders a real-time picture of the situation. One fact is worth holding onto. In the spring of 2022, a circuit was built through which a civilian's smartphone could place a single dot on the army's map.

The decision-making process is hard to confirm from public documents alone. We could not establish public documentation of how reporters' identities were checked, what percentage of incoming reports proved usable, or how many stages the verification ran through and who made the calls. Traces exist of such figures being mentioned in interview form, but they were not established as citable sources, so they are not set down as fact. What the documents say — that a procedure existed — is

as far as we can go; how fine-meshed that procedure was lies beyond the range.

The scale was not small. One tally holds that as of the end of 2022, more than 433,000 Ukrainians had sent battlefield information through the eVorog chatbot. Over the same period, a Telegram channel called "STOP Russian War" gathered more than 100,000 reports of enemy movements. Those 433,000 are citizens who used a reporting channel, and the figure comes from a different system than the count of IT Army participants — a different number entirely. The two must not be read as overlapping.

What these numbers prove must also be stated carefully. The 433,000 is the number of people who sent a report. The number who produced a valid target is not contained in it. No public document within the range reviewed here independently establishes how many strikes citizen reports actually led to, or how much those strikes contributed to the shape of the front. The scale of participation is confirmed; as for results, the public record stops here. The moment that distinction is erased, the record becomes propaganda.

Abroad, Ukraine's speed of response drew high praise. The British daily The Guardian described Diia as an app you use to pay taxes and also to report Russian soldiers, and The Economist wrote that chatbots like this had turned Ukrainian civilians into a "digital resistance."

But there are problems that such praise does not explain away. One report assessed that Ukraine, through digital connection, had blurred the line that once stood between the contributions of combatants and non-combatants, and wrote that citizens had become "digital eyes" covering the whole territory, acting as a force multiplier. A force multiplier is a military term for something that magnifies the effect of troops or weapons several times over without increasing their number.

"Blurred the line" was used as a compliment, but it is a heavy phrase. The law of war has long divided those who wear a uniform from those who do not, and placed the latter under protection. That protection rests on the premise that non-combatants do not take direct part in hostilities. On which side of that premise does a citizen stand who photographs enemy positions with a smartphone and puts them on the army's map? The question does not end with Ukraine; it becomes the question of every citizen of every country holding a smartphone. The collision between volunteer cyber mobilization and international law is not something that can be answered now, so the question stays open rather than closed.

There are things we could not confirm. For citizens who remained in occupied territory, reporting enemy positions carried danger. Discovery meant risking your life, and the wider the reporting channel, the more people bear that risk. No independent document in the material reviewed here shows what the Ukrainian government did to protect informants, or whether citizens were harmed because of their reports. Since there is no foundation, this is left open rather than closed prematurely; writing down that it is blank is more honest than filling the blank in.

Where the reporting channel was placed also deserves a look. eVorog sat not inside a state-built app but on top of Telegram, a private messenger. One report describes the chatbot as a state project built to record Russian troop movements in real time and preserve them as documentation. If so, the

floor of this channel is the server of a company the Ukrainian government does not own. No document in the material gathered here shows what was agreed with Telegram, where the servers sit, or who can look inside them. That the state asked its citizens to send it enemy positions while not holding the conduit itself in its own hands is worth noting, quite apart from the results.

The information that comes in arrives at DELTA. The documents describe DELTA as a platform riding on the cloud. It layers information from drones, satellites, scouts, and civilians onto a single map and gives commanders a real-time picture. Layering is one method of filtering. When different eyes point at the same thing, confidence grows; when only one points, doubt remains. Even so, layering does not finish the verification. Many eyes can share the same illusion, and on an urgent front there may be no time to wait for the other eyes to arrive. The phrase "on the cloud" comes with a condition too. The map may be alive, but a command post whose line is cut cannot open it.

Praise from outside has to be read for what kind of thing it is. The sentences in The Guardian and The Economist are impressions from outside, not audits weighing how accurate this system was. The press writes down what stands out, and what stands out sometimes coincides with results and sometimes diverges from them.

Time is attached to the numbers as well. The tally of 433,000 is a figure from the end of 2022. We could not establish any later tally telling us whether the channel kept running at the same scale afterward, whether reports rose or fell, or whether people grew weary and let go. What we hold is a single photograph taken at the tail end of the war's first year, and there is no film after it.

3. Refugee Support and Damage Recovery: Diia's Two Faces in Wartime

When the war began, millions left the places they had lived. As of the end of 2023, roughly 14 million Ukrainians had left their homes.

People fleeing in haste sometimes could not gather their identity cards and other papers. Those who left paper passports and ID cards behind, those whose whole drawer of documents collapsed with the building, lined up at borders and stations and shelters. A state that cannot confirm who they are can do nothing for them. Support payments, shelter, passage through checkpoints — all of it begins with confirming identity. On top of that, because the government had cut access to the national registries by its own hand right after the invasion, even opening an electronic document in Diia was difficult for a while. It was a gap created by a measure taken for defense.

In early March 2022, e-Document (єДокумент) was added to Diia. It is an electronic document allowing people without a paper passport to prove their identity provisionally, and it carried passport information and a taxpayer number. With this single document a person could pass checkpoints, register at a shelter, and apply for support. What the state returned to its citizens through this document was less a sheet of paper than an identity.

Damage recovery was handled by e-Recovery (єВідновлення). It is a channel through which citizens whose homes were destroyed by shelling upload photographs and damage details via the app to claim compensation. By the Ukrainian government's tally, more than 108,000 citizens received a

total of 10.6 billion hryvnia for home repairs, and roughly 23,000 received digital housing vouchers to buy new homes, amounting to 33 billion hryvnia. These figures are a government tally reproduced by a report issued in November 2025.

Two things must be kept in mind together when reading the numbers. These sums are not the figures for the single month of February 2022 but cumulative totals built up over the years that followed. The stage is 2022, but to see what the channel opened then went on to carry, there is no choice but to bring in the later numbers. And the body that produced the tally is the government that paid the money out. No external audit document in the material reviewed here confirms whether the compensation actually reached the victims, how many people were rejected in screening and why, or how much fraudulent claiming was filtered out. The size of the sums disbursed and the fairness of the system are different questions, and for the second there is as yet no foundation for an answer.

Administrative services continued through the war. One report tallied that 63 percent of Ukrainian citizens use state electronic services, and wrote that between 130 and 150 digital public services were maintained without interruption in wartime.

During the war Diia became both a means of living support and a channel where government authority gathered.

One face is survival. It returned an identity to those who lost their ID cards, opened the road for money to reach those who lost their homes, and kept administration going in cities where the government buildings had collapsed. When Russia bombed the offices to create chaos, Ukraine moved the offices inside an app.

The other face is concentration. One and the same app is an identity card, a welfare counter, and a property damage claim form. Information about a single person gathers under a single authentication system, and the source of convenience and the source of danger run through the same thing. The explanation that Diia's architecture does not store personal data in the app means there is nothing to gain from breaking into it. Read as meaning the state cannot identify its citizens, it is wrong. The state can always identify them; that is the definition of an electronic ID.

So it matters who controls this technology and by what procedure. Who reaches this data, whether a record of the access remains, and if it does, who looks at that record; how far exceptions are permitted in wartime and when those exceptions end. A door opened during a war does not close by itself when the war ends. Someone has to close it, there must be voices demanding that it be closed, and for those demands to carry there must remain an opening in which to make them.

The public record does not contain enough of the citizens' own experience. Independent documents showing what Ukrainian civil society or human rights organizations objected to regarding Diia and surveillance in wartime administration, and how the government answered, are conspicuously absent from the material gathered here. The government's account exists; the original text of the criticism does not. When the foundation lies on only one side, balance is not something you can manufacture but something you must confess, and this gap remains unfilled.

One judgment remains to be set down about February 2022. Ukraine's e-government did not have its performance proven by meeting a war; its purpose changed. A tool built to abolish queues came to stand beside a conduit for finding targets. An authentication system built to collect taxes became the frame of wartime administration. A counter that had received welfare applications received photographs of ruined homes. This conversion was fast, and many documents record that it worked. Fast conversion skips deliberation. Skipped deliberation does not disappear; it piles up behind, and what piles up comes back one day as an invoice.

The channels opened in wartime did not spring from bare ground. When the Diia app and portal appeared in 2020, a system for paying COVID-19 relief to citizens opened alongside them. Ukraine first went through the experience of a state sending money by app to people struck by disaster during an epidemic. The e-Recovery of 2022 was less the cutting of a new road than the loading of a different burden onto a road already cut.

Diia was also used to send support payments to citizens. Into Diia went a function for displaced people to register a new place of residence and apply for monthly government support, and a function for buying war bonds — which raise money for the cost of the war — was attached as well. On one side the state's money goes out to citizens; on the other, citizens' money comes in to the state. A single screen became a wallet facing in two directions.

The tally that 63 percent use state electronic services has to be read the other way round. It means people who do not use them remain. There are people without smartphones, people who lived near the front with their lines cut, people too old to handle an app. No document in the material reviewed here shows where these people proved their identity in wartime or through which channel they claimed compensation. In a country that has moved its administration inside an app, where does the person standing outside the app go? We do not hold the foundation to answer that question, and writing that it is absent is more accurate than pretending it is there.

The form of oversight exists on paper. The Ministry of Digital Transformation manages Trembita and Diia and plays a coordinating role across the government's digital projects, and parliament's Committee on Digital Transformation supports this work. But no record in the material gathered here shows what that committee deliberated during the war, what judgment it reached about cutting access to the national registries or about wartime exceptions, or when it decided those exceptions would be withdrawn. That a supervising body exists and that supervision took place are two different statements. The first is confirmed; as for the second, the public record stops here.

Chapter 3. The IT Army, a Volunteer Corps in Cyberspace

On February 26, 2022, a short message appeared on the official Telegram channel of Mykhailo Fedorov, Ukraine's Minister of Digital Transformation. It was an appeal to anyone who knew how to handle digital technology to stand with Ukraine, regardless of nationality. It was the third day of the full-scale invasion, and the response came quickly. Before long the channel had grown to roughly 150,000 subscribers.

The organization was called the IT Army of Ukraine. The word army was attached to it, but there were no barracks and no insignia. The recruitment notice came from a digital minister's social media account, and applicants underwent no physical examination and swore no oath. You subscribed to the channel, pointed your own computer at the target on the screen, and that was enlistment. There was no need to collect a weapon, no need to be assigned to a unit. All it took was one device connected to the internet and the decision to follow a list.

Articles and lectures about this organization often say that participants numbered four hundred thousand. The figure that can be confirmed in the underlying literature is roughly 150,000 Telegram channel subscribers. The primary source of the four-hundred-thousand figure could not be found anywhere in the public record, so only the confirmed range is used here.

The number of subscribers and the number of people who actually took part in attacks were different quantities from the start. Someone who subscribed to the channel and never once ran the tools still counts as a subscriber. Conversely, someone who never subscribed but downloaded and ran the distributed programs falls out of the subscriber count. The headcount of this organization shifts enormously depending on how you count, and the size of the IT Army remains unknown even now.

1. A Mobilization Beyond the State, Begun on Telegram

The person who first proposed the IT Army was an entrepreneur outside government. Two analytical reports record that the starting point was a proposal from the Ukrainian IT entrepreneur Yegor Aushev to Minister Fedorov to create a cybersecurity volunteer group. One is a report issued by Romania's New Strategy Center in June 2024, the other a one-year retrospective on the war published in February 2023 by CERT-EU, the computer emergency response team for the European Union institutions.

The idea came from the private sector, and the minister was the one who posted that proposal on a channel the whole world could see and gathered people to it. What Fedorov did was closer to amplification than to founding. He lent the state's loudspeaker to a private proposal. The person who opened the channel for the call and the person who directed everything done by those who answered it are not the same, and this distinction will be used again when weighing his merits and faults.

The sources diverge even on the founding date. Some place the start of the IT Army on February 25, 2022, others on February 26. Rather than choosing one, both dates are left standing. A single day's difference may look small, but in the debate under international law over when the state began to be involved with this organization, that day serves as a foundation. The wobble in the date within the war

record reflects the circumstance that this organization was born from an urgent social media post.

To see what the assembled people actually did, you have to look at the tools. The IT Army's main instrument was the DDoS (distributed denial of service) attack. The term sounds difficult, but the principle is not. When a great many computers pour connection requests at a single website at once, the server exceeds the volume it can handle and stops. It resembles a narrow doorway crowded all at once, so that no one who actually has business there can get in or out.

This method accomplishes nothing with a single computer. Tens of thousands must move together to become a wall, and the headcount of volunteers is itself the firepower. So for the IT Army, lowering the threshold of participation led directly to increasing the organization's strength.

Volunteers offered up the communications bandwidth of their own computers to form an enormous botnet. A botnet means a herd of computers moving together at a single command. The automation tools this required were built and distributed by hackers themselves. Bohdan Ivashko (handle: Arriven), a Ukrainian-born engineer working at the American security company Cyberhaven, released a program called db1000n on GitHub. GitHub is a public repository where developers upload program code for anyone to download. A tool called disBalancer, which uses a Web 3.0 network, appeared, and an IT ARMY Kit bundling several tools into one was also distributed. They took a form in which even someone who knew nothing about programming could download them, press a run button, and join the ranks. This was a war in which individuals built the weapons, individuals distributed them, and individuals downloaded and used them.

The character of this mobilization was, as the name suggests, beyond the state. Participants did not have to be Ukrainian citizens; wherever in the world they lived, they only needed the internet. The people who built the tools, and the places those tools sat, were individuals and private platforms like GitHub. The very stage on which the organization operated was Telegram, a private messenger. The state was only a voice announcing targets, not the owner of the organization.

As people of varied nationalities, residences, and affiliations gathered, the locus of responsibility grew unclear. The question is how much responsibility the state must bear for a force organized beyond the state, joined by people beyond the state, and moved by tools beyond the state.

The inside of the organization was not flat throughout. The New Strategy Center report analyzes the IT Army as a structure mixing a horizontal volunteer network with a vertical chain of command. At the top were 25 to 30 IT specialists drawn from Ukraine's intelligence services and government ministries, and the report calls them the Generals. They directed a group of skilled hackers with genuine intrusion capabilities, the so-called Colonels, on a separate secure platform. The ordinary volunteers who received the target lists posted openly on Telegram were the outer layer of this structure.

It means that what is visible from outside is a single Telegram channel, but behind it lay two more invisible layers. A volunteer in the outer layer may have pressed the run button without knowing whose plan they were executing.

This structure matters for weighing Fedorov's personal merits and faults. That he posted on Telegram and gathered a subscriber base of some 150,000 is a confirmed fact. But what direction the

Generals received from the government, who made the final decisions on targets, and how roles were divided between the Ministry of Digital Transformation and the intelligence services — on these the public record does not yet permit a conclusion. It does not follow that the person who opened the door was the commander of everything that happened inside. Fedorov's share is clear as far as opening the door; what lies inside it remains blurred.

Fedorov could speak to the world's technical workforce on the third day of the invasion because that channel was not one hastily built when the war broke out. Ukraine's Ministry of Digital Transformation was established in 2019. It was the ministry charged with the pledge President Volodymyr Zelensky made in the 2019 election, the "state in a smartphone," and in 2020 the national mobile app Diia appeared. Before the invasion Diia had gathered users in the range of twenty-two million and was installed on 77 percent of Ukraine's smartphones. Diia.City, which grants tax benefits to IT firms, had thousands of companies inside it. A channel for speaking directly to citizens and to the technology industry had already been running for several years.

The Ministry of Digital Transformation also opened a channel for citizen reports early in the war. The eVorog chatbot, through which citizens reported Russian troop movements and positions with photographs and location data, ran alongside it. By the end of 2022 more than 433,000 citizens had sent military information through this chatbot, and that information passed through verification and entered Delta. Delta is a military system that gathers scattered reports and reconnaissance data onto a single screen to show what is where. The chatbot was designed to require identity verification through Diia, so as to block false reports planted by the enemy.

The two organizations differed in their mode of participation and their chain of command. eVorog admitted only people whose identity had been verified through a state app, and the information that came in was filtered through the military's systems. The IT Army was entered through a single Telegram subscribe button, and nowhere in the public record is any procedure for verifying a participant's identity written down. On one side, a record remains of who sent what; on the other, no record remains of who clicked what.

This distinction is needed when handling the numbers as well. The 433,000 is a figure recorded as the number of eVorog informants, and the figure that can be confirmed for the IT Army is roughly 150,000 Telegram subscribers. The public record does not connect the two figures. Where the four-hundred-thousand figure came from is a point at which the public record stops.

2. The Debate in International Law over Targets, Participants, and Command

The IT Army landed on the desks of international law scholars because it fit into none of the existing rulebook's slots. War, too, has rules. The bodies of rules called international humanitarian law (IHL) and the law of armed conflict (LOAC) set out who may fight, what may be struck, and who bears responsibility. The IT Army blurred the answer to all three questions.

First, the question of what may be struck.

Additional Protocol I to the Geneva Conventions of 1977 requires belligerents to attack only military objectives. A military objective is something whose destruction or neutralization offers a definite military advantage. And proportion must be kept between the military advantage gained and the harm suffered by civilians. This framework is applied again to the cyber domain in a report the Atlantic Council issued in November 2025. The International Committee of the Red Cross (ICRC) has put forward eight rules that civilian hackers taking part in wartime must observe: do not directly target civilian facilities; do not use malware that spreads indiscriminately across military objectives and civilian facilities alike; do not touch medical or humanitarian facilities; do not strike infrastructure essential to civilian survival; and so on.

It is hard to say the IT Army broke every one of these rules. The report notes that they were reluctant to target the health and social support sectors. It means they tried not to touch hospitals. The trouble comes next. The principal targets recorded in the same report were banks such as Sberbank, Gazprombank, and VTB; the video platform Rutube; the Moscow Exchange; and the Troika portal, which processes fare payments across 38 regions. These are the systems through which Russian citizens pay bus fares, receive their wages, and watch videos. Civilian infrastructure that keeps daily life running took up a large share of the target list.

The IT Army held out the aim of reducing Russia's economic resources and thereby degrading its capacity to wage war. But whether attacks on civilian services translated into military advantage is not clear. Is the inconvenience a Russian citizen suffers when a banking app stops for a few hours a definite military advantage in the sense international law means? How do you measure the causal link between shaking a payments network and the outcome of battles at the front? Even among Western policy research institutes this debate has not been settled. When the criteria for choosing targets are blurred, the price of that blurriness is paid by the civilians of the targeted country.

Next comes the question of whether the participants are soldiers or civilians. Whether they receive prisoner-of-war treatment when captured or stand trial as criminals turns on this, so it is a distinction on which people's lives and liberty depend.

There are conditions for becoming a combatant in the sense international law means. Under Article 4(A) of the Third Geneva Convention and Articles 43 and 44 of Additional Protocol I, one must belong to a belligerent's regular armed forces or to a militia or volunteer corps integrated into them, must be under the command of a superior, must wear a distinctive sign recognizable at a distance, must carry arms openly, and must observe international humanitarian law in operations. There is also an exception, the levée en masse, for inhabitants who spontaneously take up arms as an invading army bears down.

The IT Army satisfies none of these items. It was not incorporated into the regular armed forces, it has no uniform, and a laptop cannot be called a weapon carried openly. Scattered across the world, its members cannot be an uprising of the inhabitants of occupied territory either. So they are legally civilians, and while inflicting real damage in a war, their status classifies them as people unconnected to it.

When civilians lay hands on a war, the next question is whether it amounts to direct participation in hostilities (DPH). All three conditions must be cleared. The act must cause death, injury, or physical destruction, or have a substantial adverse effect on the enemy's military operations (the threshold of harm); there must be a direct causal link between the act and the harm; and the purpose must be to aid one belligerent and injure the other.

The report's judgment runs like this. The last condition is met. Their intent to help Ukraine is plain. But DDoS attacks and website defacement neither kill nor wound anyone, nor do they break objects. Defacement means replacing the front page of someone else's website with a message of your own. So the condition of the threshold of harm is not cleared.

Apply the law and their status becomes one that is hard to protect. The IT Army's volunteers fail the combatant requirements and so receive no prisoner-of-war protection. At the same time they fail the requirements of direct participation and so are not recognized as engaging in lawful acts of war either. If captured by Russia they can be punished as hacking criminals under Russian criminal law. Tens of thousands came to stand in a blank space in the law, with neither protection nor status. The lower the threshold of participation, the less visible the substance of the risk may have been even to the participants themselves.

State responsibility must also be examined.

There is a document setting out legal standards for cyber operations, the Tallinn Manual 2.0. It is a commentary produced by a gathering of NATO-affiliated experts. Rules 15 and 17 hold that when a non-state actor conducts operations under the instruction, direction, or control of a state, the act is attributed to that state. The problem is how strictly to read control, and two principles collide here.

One is the effective control doctrine (ECD). Emerging from the International Court of Justice's Nicaragua case, the standard recognizes responsibility only when it is proven beyond doubt that the state directly and thoroughly controlled the organization. The threshold is high. The other is the overall control doctrine (OCD). It emerged from the Tadić case at the International Criminal Tribunal for the former Yugoslavia (ICTY), and holds that a state can be held responsible even if it merely played the role of organizing, coordinating, and supporting the organization. The threshold is low. On the same set of facts, which yardstick you use flips the presence or absence of state responsibility.

Under the strict ECD standard the Ukrainian government has room to slip through. Proving that the government directly ordered individual attacks is not easy. Under the looser OCD standard the situation is different. So long as people were gathered through a minister's channel and there is a Telegram where target lists changed hands, traces of coordination and support are hard to deny.

The report offers a table laying out the degree of state responsibility across ten levels. Level 1 is the stage at which a state prohibits and prevents attacks by third parties, and level 10 is the stage at which a state's regular forces and third-party proxies are fully integrated. On this scale, the Ukrainian government's position early in the war was either state coordination (level 6), proposing operational details, or state encouragement (level 4), promoting attacks as a matter of policy. It is a role of having been involved without owning.

This legal position can change. Ukraine's parliament and the Ministry of Digital Transformation prepared a draft cybersecurity bill that would legalize volunteer hacker units as a cyber reserve of the regular armed forces and incorporate them. If this law passes, the IT Army enters the state's organization the way the Estonian Defence League's cyber defence unit has, and Ukraine's state responsibility rises to the highest step, state integration (level 10). It means the state would take on in full the international legal responsibility and reparation obligations arising from the hacking the volunteers carried out. The cyber reserve bill is a plan at the draft stage, and on its passage and implementation the public record stops here.

Embrace them in law and the volunteers gain protection while the state gains responsibility. Leave them outside and the state avoids responsibility while the volunteers lose protection. When Fedorov posted a single message to Telegram, this problem — costly whichever way it goes — was opened along with it.

It is worth noting what kind of documents the yardsticks used in this debate actually are. The Tallinn Manual 2.0 is not a treaty signed by states but a commentary written by a gathering of NATO-affiliated experts. The table laying out state responsibility across ten levels is not law either but a scale created for analysis by Romania's New Strategy Center. The ICRC's eight rules, likewise, are not provisions that impose punishment when broken but recommendations asking for compliance. There are several documents that speak of rules, yet no decision by an international tribunal applying those rules to the IT Army and rendering judgment exists in the public record. There are many yardsticks, and the courtroom has yet to open.

Hackers are not the only ones standing in the gray zone. A report on Ukraine's wartime cybersecurity system notes that this kind of citizen participation blurred the boundary between the contributions of combatants and non-combatants. The 433,000 citizens who photographed Russian troop movements and uploaded them to a chatbot stand before the same question. As to which is closer to the war — the person who ran a DDoS tool or the person who uploaded a photograph — international law's old slots hold no answer.

The model the incorporation bill measures itself against is also worth confirming. The model the report cites is the Estonian Defence League's cyber defence unit. It is a method of bringing volunteers inside the state's organization and placing them under a chain of command and discipline. Once inside, volunteers gain status and protection, and the state takes on alongside them the obligation to make reparation for what they did. To whom and through what procedure that reparation would be made, and what the people who used Sberbank or the Troika portal could claim, is not written in the public record.

Nor do the stakeholders end with the government and the volunteers. GitHub, where the tools sat, and Telegram, on which the organization operated, are both services of private companies. How these companies handled what happened on their platforms, and whether they could have taken down the tools or blocked the channel, is not in the public record. In the place where the rules of war are debated, the very parties that own the stage are absent.

3. What the Volunteer Network Achieved and the Blank Where Control Should Be

The signature strike recorded by the New Strategy Center report is the attack on Rutube timed to Russia's Victory Day, May 9, 2022. It states that administrator passwords were changed and data on the scale of a petabyte was erased. A petabyte is about a million times the size of a gigabyte. Cases in which the Moscow Exchange, Tinkoff Bank, and Troika, the public transit payment portal for 38 regions, were brought to a halt are recorded alongside it.

Without a single penny of regular military budget, without a single troop movement, they shook an adversary's everyday infrastructure for days at a time. With nothing but cheap laptops and volunteers' hours, they produced an upheaval comparable to a costly regular operation.

The problem that no one is measuring the size of the achievement follows immediately. The effect of a DDoS attack is generally temporary. A server stops for a few hours, at most a few days, and comes back. The absence of physical destruction is the very quality that made their legal status ambiguous. No document independently measuring how much these attacks actually cut into Russia's capacity to wage war can be confirmed in the public record; there are only announcements from the Ukrainian side and self-reports from participants. The principle of not placing announcements on the same scale as independent verification applies here just as it does elsewhere.

Control, too, is empty. As time passed the IT Army drifted away from the state. According to the report, government support shrank to the level of non-operational support, and the organization came to run on a distributed model, raising its own funds through crowdfunding. Crowdfunding is a method of gathering many small donations over the internet. An organization the state called into being slipped out of the state's hands; a single blast of the loudspeaker sufficed to call it, but for turning it around there is no such loudspeaker.

The circumstance that there are rules but no hand to enforce them appears at once as a practical problem. The ICRC made eight rules for civilian hackers, but there is no means of enforcing those rules on tens of thousands of people loosely linked by a Telegram channel. If someone strikes a hospital's computer network, who stops them? Who punishes them? An army without a commander has no military law either. What was this organization's strength, that anyone can join, becomes its weakness intact. To say that anyone can join travels together with saying that no one bears responsibility, and the openness that grew the organization and the openness that made it impossible to control were one and the same.

The numbers and facts, too, carry questions outside the public record. The widely cited scale of four hundred thousand is a point at which the public record stops. What can be confirmed is a single figure: roughly 150,000 Telegram subscribers. The founding date splits between February 25 and 26. What command relationship the 25 to 30 Generals of the leadership had with the government is likewise something on which a conclusion is still premature. It is hard to hope that the records of an organization created in the middle of a war would be intact. But recording the fact that records are absent is something that can be done, and leaving the blank as a blank rather than pretending to have filled it is how one handles this organization honestly.

Reports kept appearing even after the events had passed. CERT-EU summarized the first year of the war's cyber operations in February 2023. Romania's New Strategy Center issued a report on the eastern digital front in June 2024. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) published a document on the evolution of Ukraine's cyber defence in March 2026, and the Australian Army Research Centre released OP 35, a paper on the IT Army, on April 22, 2026. That military research institutes in various countries have held onto the same organization for years after the invasion means the conclusions have not come in.

What can be confirmed to his credit is speed. On the third day of the invasion he opened a channel reaching the world's technical workforce and drew a response on the scale of 150,000 people. Had the defense ministry organized a volunteer corps through proper procedure, it would have taken months. The person with the idea was the private entrepreneur Aushev, the people who built the tools were developers like Ivashko, and what the minister did was attach the state's loudspeaker to that current.

What came into view is the role that loudspeaker created. Tens of thousands gathered through a state channel came to stand in a position with neither the state's command nor the state's protection. Legally they are civilians; captured, they become criminals; and if they break the rules there is no one to stop them. There is no ground for saying that responsibility for this state of affairs lies entirely with Fedorov alone. But the fact that this state of affairs began with his Telegram post remains, and he was the designer of a rapid mobilization and, at the same time, the designer of a mobilization without control.

With a computer and the internet, one could take part in a war from beyond its borders. When the distance between a hand holding a smartphone and the front line disappears, the distance between combatant and civilian disappears with it. What remains on the erased line is a single subscriber figure of roughly 150,000 and a record that never settled whose command they followed, what they brought down, and how much.

The method of drawing volunteers into a war did not first appear in 2022. Ukraine had a volunteer drone reconnaissance group, Aerorozvidka, active since 2014. Civilians carried on experiments attaching smartphones, tablets, and commercially sold drones to military operations, and a military technology report notes that these experiments became the conceptual foundation of Delta, the Ukrainian military's battlefield situational awareness system, in 2017.

Aerorozvidka and the IT Army differed in how they verified information. Aerorozvidka's reconnaissance data, like the citizen reports coming in through the eVorog chatbot, passed through verification and flowed into Delta. Information had a filtering stage, and there was a system that received and used it. No such stage is recorded in the public record for the IT Army's DDoS attacks. Targets went down through Telegram, and whether they were acted on and with what result stayed on each person's laptop.

It is also worth looking at where the items listed as achievements came from. The sentence that Rutube's administrator passwords were changed and data on the scale of a petabyte was erased is a record from the New Strategy Center report. No document exists in the public record in which the

targeted Russian side confirmed that damage. A record left only by the attacking side and by reports analyzing that side must not be read as confirmed damage.

The observation that boundaries have blurred does not hang on the cyber front alone. The person flying a drone, the person photographing enemy troops and uploading it, and the person pouring connection requests at someone else's server have all entered the same gray zone. Whether Ukraine brings them inside the law or leaves them outside still hangs on a bill at the draft stage, and in the meantime the price is paid by the individual volunteer.

Chapter 4. Bargaining with Musk: Starlink

On 26 February 2022, Mykhailo Fedorov asked Elon Musk on X (then Twitter) to send Starlink terminals. It was a public request that passed through no diplomatic note and no embassy. Musk answered, and two days later, on 28 February, the first shipment of terminals arrived in Ukraine.

That post is often cited as the example that captures how Fedorov responded in the opening days of the war. The story goes that a young minister asked Elon Musk for help over social media and saved the country's communications. In truth, several governments and institutions took part in the supply effort.

The public post alone does not account for the whole chain of terminal supply. Why satellite internet was chosen, where the terminals were used, and what costs and conditions Ukraine bore have to be checked against other sources. A situation in which a private company's terms of service and the judgment of a single executive effectively set the range of communications available to a country at war was a problem this war produced for the first time. That is why the Stockholm International Peace Research Institute (SIPRI), in a report of June 2023, treated the war in Ukraine's effect on space governance as a subject in its own right.

These pages draw mainly on a report issued by the RAND Corporation in March 2025. The early supply routes for terminals, the installation in medical facilities, the Bucha and railway cases, and the pairing with drones all come from there. Where cross-checking was possible, the account is supplemented by the miltech report issued in February 2026 by the French Institute of International Relations (IFRI) and the Munich Security Conference, by a Ukrainian Ministry of Defence notice of February 2026, and by domestic press coverage. Where that was not possible, the sentence itself says that it rests on a single source. What one report conveys is likely to be true, but likely is not the same as established.

1. From a Public Request to the Arrival of the Terminals

Just before the full-scale invasion began, Ukraine's communications had already collapsed once. On the eve of the invasion, Russian hackers launched a large-scale attack against the KA-SAT network of the American satellite communications firm Viasat, and the satellite links that the Ukrainian military and several government bodies were relying on were paralysed, straining command and control in the war's first days.

How far the Viasat attack actually disabled Ukrainian command and control is judged differently from one analytical institution to the next. Some reports treat it as the decisive blow of the opening phase; others hold that the Ukrainian military already had other means of communication and that the effect was limited. Weighing the conflicting evidence and methodologies is a task for another place. The fact needed here narrows to one point. In late February 2022, having just learned how easily satellite communications can be severed, the Ukrainian government was looking for a substitute line.

Starlink is a service that delivers internet access through a dense swarm of small satellites that SpaceX has placed in low Earth orbit. The phrase is unfamiliar, so let us unpack it. Satellite internet

until then meant putting a handful of large, expensive satellites into a much higher orbit. Because a satellite sits high, one of them covers a wide area. In exchange, the signal travels a long way, so responses are slow, and if one of those few satellites is disabled, a whole broad region goes dark at once. That is what happened when Viasat was targeted. Low-orbit systems stand on the opposite side. Each satellite is small and short-lived, but there are so many of them that the loss of a few does not immediately stop the service. On the ground you need only a dish-shaped terminal and power — no fibre, no base stations, no switching centres.

In areas where shelling had erased the telecom facilities, that condition was decisive. Rebuilding a city's base stations takes materials, workers and time, and a rebuilt base station can be shelled again. A satellite terminal stands outside that cycle. A network with no ground installation to knock down — that was what Ukraine was looking for in the spring of 2022.

From the moment Fedorov's post went up, to Musk's answer, to the arrival on 28 February, less than three days passed. It is a speed no government's procurement process could imagine. Months just to publish a tender, set the specifications and sign a contract is the normal pace of peacetime administration.

Even so, to write that one man's tweet produced that speed is to cut the facts too narrowly. The early supply of Starlink involved not only SpaceX but the United States government, the United States Agency for International Development (USAID), Poland and France. It was these institutions and governments that bought thousands of terminals and hauled them to the border.

What negotiations actually took place after the tweet, and who decided what and when, cannot be reconstructed from published documents. On what passed between Fedorov and Musk, and at what point and in what manner the United States government stepped in, the primary record stops here. Conversations and decisions outside the public record have been left out of this text.

What is visible is the outcome. Between February and April 2022 roughly 5,000 Starlink terminals entered Ukraine, and in that period the continuity of the national chain of command was restored — so the IFRI and Munich Security Conference miltech report records. The phrase "continuity of the chain of command" is stiff, but its meaning is not hard. It means that instructions from the presidential office reach regional administrations, and orders from military headquarters reach subordinate units, without a break; and when that breaks, a state exists only on a map.

Users grew faster than supply. Five weeks after the service went live, daily Starlink users inside Ukraine reached 150,000, according to the RAND report. That figure has to be handled with care. Who compiled the 150,000 and how, and whether it comes from SpaceX connection logs or a Ukrainian government estimate, is where the public record stops in that report. The earlier 5,000 terminals and this 150,000 come from different sources and different reference dates. Dividing one by the other to say how many people shared each terminal can hardly be called an accurate method, and it is better to stop at the point where the temptation to do the arithmetic arises. What can be confirmed is this much. At a time when terminals numbered in the thousands, users had already climbed into the hundreds of thousands, and at that point Starlink had passed beyond the character of a piece of military

communications equipment.

The form of the request also set the nature of the relationship. Fedorov chose a public platform instead of a private diplomatic channel. The counterpart was a company rather than a state, and that company's chief executive was a man who reacted instantly on social media. A person named in public finds it hard to stay silent, because not answering is itself an answer. This pressure is a kind of force written into no treaty and no contract. That is less a fact contained in the public documents than the author's reading of them.

The choice worked, and at the same time it fixed the nature of the relationship. The request became a personal response rather than an agreement between states, and the response took the form of a favour. What begins as a favour can be withdrawn as a favour. The seed of the problem Ukraine would face from the autumn of 2022 lies here. Still, there is no basis for supposing that Ukraine in late February 2022 had other options comfortably at hand; in practice only one operator could supply satellite internet in bulk within a few days.

The character of the Viasat attack is worth noting too. No satellite was shot down. On the eve of the invasion, Russian hackers came in through several routes at once and brought the KA-SAT network to a halt, and satellite links were severed without a single bomb. That a network can go dark without being physically broken was confirmed on the first day of the war.

In the same period the country's data was moved beyond the borders through Amazon Web Services' Snowball devices and Microsoft's Azure cloud. The scale and the process were covered in Chapter 2. What matters here is that the dishes belonged to SpaceX and the servers to Amazon and Microsoft. The foundation on which the state stood had shifted onto the facilities of foreign private companies.

Under what conditions the civil servants and developers who did the work during those ten weeks of extracting data actually worked, and by what route the storage devices crossed the border, is not recorded in the public documents at hand.

2. A Private Satellite Network Links Hospitals, Government and the Front

Starlink terminals were installed not only at the front but in hospitals that had lost their connections. Ukraine's Ministry of Health stated that within a month of the service starting it had installed Starlink at 590 medical facilities. That figure is a Ukrainian ministry's own tally, and the RAND report is relaying that announcement. Whether the number installed matches the number actually working, and how long those connections held, is where the public record stops. Rather than transcribing a government announcement as fact, it is more accurate to state who announced it and what kind of announcement it was.

Why internet access matters in a hospital may need explaining. A modern hospital handles patient records, drug inventories, referrals and transfers, and the sharing of test results over a data network. When the line goes down, a doctor cannot see a patient's history and can neither send a patient elsewhere nor receive one. At a hospital near the front, a severed line goes beyond administrative

inconvenience and becomes a question of mortality.

Repair of civilian infrastructure began at once as well. In Bucha, outside Kyiv, the mobile operator Lifecell used Starlink to restore some of the destroyed mobile services. Executives of the state railway company Ukrzaliznytsia kept their connection over Starlink aboard moving trains and directed rail logistics and the movement of refugees from there. Both cases come from a single RAND report and have not been cross-checked against other sources.

Railways and mobile networks are civilian infrastructure, but in wartime they also carry military movement and communication. Still, in the spring of 2022, when millions were moving toward the western border, train schedules and telephone networks were a condition of survival. Knowing which stations trains were stopping at and which lines were still alive, as against not knowing, made an enormous difference. In the first weeks of the war, access to information bore directly on preventing public panic, the same report notes. Panic produces military consequences of its own, because when roads clog with columns of refugees, supply vehicles cannot get through either.

As time passed, Starlink's centre of gravity moved from the rear to the front. By early 2023 about 42,000 terminals were operating in Ukraine, more than an eightfold increase in a single year.

Dishes sat in trenches, in bunkers and in armoured vehicle shelters. Commanders coordinated operations over encrypted real-time links and passed enemy coordinates to artillery units. Whether passing coordinates to the guns takes several minutes or several dozen seconds decides whether the target is still there. Against a moving target, communication delay is another word for accuracy.

The pairing with drones went a step further. Starlink terminals were mounted directly on drone airframes. Exchanging live video and data over the satellite link, an operator could identify targets beyond line of sight and support precision strikes at night.

The size of the change shows up in operating radius. Until then a drone's radius was bound to the distance the control radio signal could reach — the limits of ground repeaters and antennas. If a single hill blocked the signal, that was the end of it. A satellite link routes around that limit by going upward, because the signal does not follow the terrain but comes back by way of the sky. People often say cheap drones changed the war; what carried those drones far was a satellite network that was not cheap.

Starlink arrived at first as a strategic safeguard — a reserve line to use when the existing networks collapsed. By 2023 Starlink had already outgrown the role of a reserve line and become a tactical dependency, something units structurally leaned on to direct artillery fire and fly drones. Losing a reserve line is merely inconvenient; when a dependency is cut, operations stop.

The weakness of a commercial consumer service is that anyone can buy it. As the war dragged on, Russian forces too began using Starlink terminals smuggled in through third countries on the battlefield. Starlink components were identified in the wreckage of Shahed loitering munitions based on Iranian designs and of Molniya drones. The network Ukraine had brought back to life returned as the link for drones striking Ukrainian cities.

The response came from both the technical and the administrative side. On the technical side, SpaceX applied geofencing — a function that automatically blocks service according to location and conditions. If an airframe carrying a Starlink terminal was detected flying faster than 75 to 90 kilometres an hour, that terminal's connection was cut. Russian drones heading for the rear lost their links and were neutralised, domestic reporting says. A terminal carried by a person or mounted in a vehicle rarely exceeds that speed; a loitering munition does. A single physical quantity — speed — separated civilian users from attacking weapons.

On the administrative side, Ukraine's Ministry of Defence introduced a whitelist system, a measure under which only certified and registered terminals work on Ukrainian territory. Users must check their terminal's KIT number and UTID identifier and complete registration; unregistered devices are cut off. Even approved terminals are restricted to working only when stationary or moving at low speed. The ministry announced this on 3 February 2026, and domestic outlets reported the same development on 5 February 2026.

The timing is worth marking. February 2026 falls after Fedorov took over the Ministry of Defence. But that he proposed or approved this system is where the public record stops in the documents at hand. A ministry notice will be left as a ministry notice. Transcribing everything a ministry did during a minister's tenure into that minister's personal record of achievement is a trap biography commonly falls into.

The direction of the system is clear. Equipment that anyone could buy and switch on now switches on only after it is entered in the defence ministry's register; convenience shrinks and control grows. This is roughly what war does to civilian technology.

As of the reference date of 13 July 2026, reporting confirms that Russian attempts at jamming and evasion, and Ukrainian and SpaceX countermeasures, are still alternating. The contest of spear and shield has not yet reached its full stop.

The sentence that a private satellite network linked hospitals, government and the front is true. The same sentence also reads in reverse. It also means that hospitals, government and the front were tied to a single private company's single service. What laid the network was not one tweet but thousands of hands, and yet the switch that turned that network on and off sat in one place.

It is worth looking a little more closely at what the whitelist demands of users. A terminal's owner must find the device's KIT number and UTID identifier and complete certification according to the ministry's instructions, and an uncertified device is cut off. Even a certified device works only when stationary or moving slowly. How registration is handled for non-military users such as hospitals or relief organisations, and whether there is any procedure for appeal when registration is refused, is not written in the notice.

There is a snag in dividing by speed. Starlink terminals were also mounted on Ukrainian drone airframes. How a rule that cuts the link of a fast-flying airframe runs alongside an operating practice that mounts terminals on fast-flying airframes appears neither in the ministry notice nor in the RAND report. Whether an exception is built in for military links, or whether a separate certification scheme

exists, is where the public record stops.

The Ukrainian government and a private company each shaped the scope of the service. One constraint SpaceX imposed through geofencing; the other the Ukrainian Ministry of Defence imposed through registration. What the company set, the company releases; what the ministry set, the ministry releases. As control grew, so did the number of hands doing the controlling. That a measure against Russian drones is also a measure for managing one's own citizens is a result of reading the two measures laid over each other, not a sentence any document wrote down.

3. The Crimea Cut-Off and the Cost Dispute: A Company's Terms Become Geopolitics

In the autumn of 2022, Ukrainian forces sent uncrewed surface vessels into the Black Sea. The target was the Russian Black Sea Fleet anchored off Sevastopol, in Crimea. Within the operating radius the Starlink connection did not come through; the drone boats, having lost communications, drifted ashore, and the operation failed.

The incident has since been told in conflicting versions. From the published documents alone, it is hard to establish which account is correct.

The RAND report and several news outlets say the Ukrainian government urgently asked for Starlink service to be opened as far as Sevastopol and that Musk refused. Musk himself, in a post on X, said that the Ukrainian intent was to sink the Russian fleet at anchor, and that had he granted the request SpaceX would have been complicit in a major act of war and in escalating the conflict. He cited concern that it might spill over into nuclear war.

"A service already switched on was switched off" and "a request to switch it on was refused" are different stories. If the first is right, a company halted an operation already under way; if the second is right, a company declined a demand to extend its service area. The moral weight and the legal implications are not the same. Musk himself claimed the latter, and there are records that put it as the former. Which is true, and in what way the United States government or other actors bore on that judgment, cannot be concluded from the published documents.

This account will not push on into Musk's inner motives. Claims circulate about whether he had commercial interests at stake, or what contacts there may have been with the Russian side, but on the documents at hand the public record stops here. The moment one writes what lies outside the public record as though it were confirmed, biography becomes fiction.

What is visible is the outcome and the structure. The outcome is a failed operation, and the structure is this. The range within which a belligerent state could conduct military operations was in practice set by a private company's service coverage. Baroness Martha Lane Fox, a member of the British House of Lords, criticised the arrangement, saying that control of Starlink rests with Elon Musk alone and that his judgment governs access to critical infrastructure.

Between states there are treaties, and treaties have procedures. If they are broken, there is room to contest it, and the way to contest it is laid down. A company's terms of service have nothing of the

kind. Which regions get service, which uses are permitted, when service is suspended — the company decides. In the world of commercial contracts, that is a natural authority. Which countries a video service operates in and which it does not is the company's decision, and no one calls that a violation of sovereignty.

When that service is the command-and-control link of a country at war, the same authority becomes a geopolitical decision and an act of drawing lines on a map. That is where SIPRI's June 2023 report located the war in Ukraine as a problem of space governance. There is as yet no agreement on how far international law and norms apply when a private space operator is deeply involved in armed conflict, or on whether such an operator can be regarded as a party to the conflict. No agreement means no room to render a judgment, and where there is no room to judge, the decision goes back to whoever is able to decide.

Alongside the dispute over control came a dispute over cost. In the early period SpaceX absorbed more than 80 million dollars itself. As users and terminals multiplied and the burden grew hard to carry, Musk asked the US Department of Defense for funding.

The costs were shared among several governments. USAID, Poland, France and others took on the purchase and delivery of thousands of terminals. The German government allocated 20 million euros to cover Ukraine's Starlink service fees. The US Department of Defense signed a six-month contract with SpaceX worth 14 million dollars, stabilising the supply of service.

The story that "Musk donated the internet to Ukraine" explains only parts of the first few months. A substantial share of Starlink's operation was sustained by Western governments' budgets, and beginning as a donation and shifting to a contract is closer to what happened. Nor did control pass to governments once governments began paying the bills. That the side paying and the side holding the switch were different is precisely the heart of this arrangement, and a contract in which the party paying cannot set the terms of use is not common. The condition of war produced that uncommon contract.

Ukraine was not sitting idle. Attempts to reduce dependence on a single company followed. The service of the satellite operator OneWeb was brought in, and with German government funding a plan was drawn up to deploy between 5,000 and as many as 10,000 OneWeb terminals in Ukraine. What can be confirmed goes as far as the plan and the funding allocation. Documents showing how many were actually deployed and how many worked are where the public record stops.

OneWeb cannot replace Starlink. Its terminals are large and are not tuned for military operations. Even so the direction is clear: to remove the single point of failure — the thing whose collapse brings everything down with it — and to recover political autonomy. It is an attempt to move toward a hybrid communications ecosystem mixing several orbits and several operators, as the IFRI report puts it. Efficiency falls and costs rise, and that is the price of autonomy.

So how should that post of 26 February 2022 be judged?

The credit is plain. In a country whose communications had collapsed, it compressed into a few days what government procurement would have taken months to do. It picked the right target for the request

and used a public platform as an instrument of pressure. The 590 medical facilities counted by the Ministry of Health and the 42,000 terminals of early 2023 are parts of a current that began with that choice.

The fault is plain too. Perhaps it is more accurate to call it a price than a fault. Build a nation's communications layer on a favour, and when the favour cools there is nothing to lean on. The drone boats drifting ashore off Crimea were the moment that price came due.

The two sentences have to be set side by side. There is no basis for holding that Fedorov personally designed the consequences as well. Nor is there any basis for holding that Ukraine in February 2022 had comfortable alternatives. The achievement that fast execution produced and the dependence that execution left behind are the front and back of one event. Looking at only one side and writing a hero's tale, or writing an indictment of error, are both easy and both inaccurate.

What it means to build a digital front on civilian infrastructure is a question policy institutions including the Atlantic Council are still asking, now that the war has entered its fourth year. The answer has not come yet. Many countries stand before the same question. Every country that has laid its administration and military communications on top of satellite internet, cloud services, mapping services and messengers is in the same position. In peacetime it is invisible, and by the time it becomes visible it is usually late.

Starlink is remembered in Fedorov's record as a method: pulling in quickly, from outside the state, what the state does not have. People, money, technology — all summoned from beyond the state. That the grammar worked in war, and what that grammar leaves behind in a state, are questions that have to be asked separately.

The cost of buying the terminals is on the record, but the process that set the service's coverage was never disclosed. The Pentagon's six-month, 14-million-dollar contract with SpaceX and the German government's 20 million euros are confirmed as amounts. But how those contracts defined the service area, permitted uses and conditions for suspension — or whether they defined them at all — is where the public record stops in the published documents. It means we cannot know whether the side paying the bill also helped set the terms, and the reason there is no room to contest the decision made off Sevastopol by way of documents lies in that same blank.

OneWeb is a satellite operator based in France, and the funding for deployment in Ukraine comes from the German government. Adding operators reduces the chance that an entire operation hangs on one company's single judgment. That is as far as the reduction goes. OneWeb is also a private company, and the side paying for the terminals is still a foreign government. Leaning on several companies and not leaning at all are different things.

The reason the versions of the Crimea incident diverge also lies in the shape of the documents. The primary statement that survives is a post Musk himself put on X, and no record left by SpaceX or the US government has been made public. When one party's after-the-fact statement is the only primary document, that is testimony, not a record. This chapter sets the two versions side by side and stops there not out of caution, but because there are no further documents to walk on.

Chapter 5. What Did Cyberwar Actually Change?

On 24 February 2022, Viasat's satellite internet service went dark in six European countries at once. Thousands of subscribers lost their connections in Germany, France, Hungary, Greece, Italy, and Poland. The damage spread even to countries hundreds of kilometres from the front.

More than 5,800 wind turbines managed by the German energy company Enercon also lost their remote communications. The satellite modems linking the turbines to their control rooms had been caught in the attack.

That same morning, Russian ground forces crossed the Ukrainian border. Several analytical reports put the interval between the two events at one hour. One hour before the ground forces crossed, the KA-SAT network of the American satellite communications company Viasat was hacked.

Everything Fedorov pushed through in that first week of the invasion rested on a single condition: what Russia could and could not do in cyberspace. Without a sense of the scale of that condition, it is impossible to gauge why he moved with such urgency — and even now it is too early to state that scale with confidence.

Before the war, cybersecurity experts around the world expected Russian attacks to bring Ukraine down within days. The expectation missed. Why it missed, and whether it truly missed at all, is still being argued over by analysts. The argument splits into three disputes: the scale of the first strike, the relationship between cyber operations and missiles, and the success or failure of Russian cyberwar.

1. The Clash over How Much Damage the Viasat Hack Did

The Viasat hack had a run-up. It is hard to see it as an ambush that sprang out of nowhere that morning. A research report on Ukraine's wartime cybersecurity (ARMG Publishing) includes a 'Viasat cyberattack timeline'. From early February 2022, as Russian troops moved toward the border and tension climbed, cyberattacks aimed at Ukraine's key infrastructure and government networks began to appear. On 23 February, the day before the invasion, distributed denial-of-service (DDoS) attacks struck banks and government websites. The method pours connection requests at a single website from many computers at once until the server stalls — closer to lining up tens of thousands of fake customers at a bank counter so that real customers cannot get in.

Then came 24 February. Malware called AcidRain rode the KA-SAT satellite network down into modems and routers on the ground. AcidRain is classed as a wiper, a tool that erases the data inside a device. Less a burglar choosing what to steal than an arsonist destroying whatever is left. The attack knocked thousands of modems and routers offline and severed one pillar of the communications network shared by Ukraine's military, government, and civilians.

The tool's name and identity emerged only a month after the event. In late March 2022, the security firm SentinelOne confirmed that the tool that had erased the devices' firmware and disabled them was AcidRain. Firmware is the software that sits at the very bottom of a machine, the layer it uses to switch itself on and move. Erase it and the machine becomes a shell: press the power button and it cannot

remember what it is for.

Why the damage leaked outside Ukraine is not difficult to explain. The internet does not observe borders. KA-SAT did not carry Ukrainian users alone. Subscribers from several European countries sat beneath the same satellite network, and so an attack aimed at Ukrainian military communications also stopped wind turbines in Germany. The reports call this 'international spillover'.

As the damage spread across countries, the incident turned into a diplomatic matter. On 10 May 2022, the European Union, the United States, the United Kingdom, and other states issued formal statements naming Russia's military intelligence service, the GRU, as the party behind the hack. Several governments called out the same culprit together.

Up to this point, the facts are broadly agreed. There is a timestamp, a name for the code, a count of broken devices, and a joint attribution by multiple governments. The dispute begins with what comes next: how large a blow this attack actually dealt to Ukraine. On that question the story divides into two readings.

Early coverage described the incident as an 'enormous loss of communications'. The headline of a Reuters report on 15 March 2022 stands for that reading. It said the satellite outage had caused an enormous loss of communications at the outbreak of the war, and its basis was a statement by a Ukrainian official. The article left the world with the impression that Russia's first strike had inflicted a mortal wound on Ukrainian military command and control.

One of those who lent weight to this reading was the analyst Jon Bateman. He pointed to the Viasat hack as a clear case of coordinated destructive action in the information domain. His grounds were three: the timing, one hour before ground forces crossed the border; the plain military purpose of degrading Ukraine's communications capacity; and the international spillover that shook connectivity in several European countries. Put those three together and it becomes hard to call it coincidence.

Half a year later, a different account appeared. On 26 September 2022, the reporter Kim Zetter published a piece in the investigative outlet Zero Day. An official, it reported, had said that the Viasat hack had 'not' had an enormous impact on Ukrainian military communications.

That official was Victor Zhora, a senior figure at Ukraine's State Service of Special Communications and Information Protection (SSSCIP). He acknowledged that communications had indeed been cut temporarily during the first hours of the invasion. But he said that thanks to the 'redundancy' already built into Ukraine's communications system, the incident was not as devastating as had been feared.

Redundancy means designing several layers in advance so that if one communications path is cut, traffic can move to another. A city with a single bridge is isolated when that bridge falls; a city with four still has a road left when one goes. Zhora's claim runs like this: even with the Viasat network wiped, the Ukrainian military moved onto other means, and so the paralysis of command and control that Russia had aimed for never happened.

Both statements came from the same Ukrainian government, and they described the scale of the damage differently. The person who spoke of an "enormous loss" in March was a Ukrainian official,

and so was the person who said in September that "it was not that bad".

The official words of a country at war are an act before they are a report of fact. At a moment when weapons support must be drawn in, and at a moment when national resilience must be shown, the size of the same event can be described differently. In March, Ukraine was a country asking the world for help. In September, it was a country holding on and preparing a counteroffensive.

That is as far as the public record goes. On what political adjustment lay between the two statements, or on what intention shaped how Zhora calibrated his wording, the public record stops here. On whether the two officials were at odds with each other, the public record stops here as well. What can be confirmed is the timing and content of the statements, and the fact that the two collide head-on. Anything beyond that would be fiction.

A CNA analysis frames this confusion as a familiar difficulty: assessments of the effect of a cyberattack diverge when conclusions are drawn while only incomplete, early-stage evidence is in hand. That is less a footnote attached to one incident than a warning label attached to the whole field of cyberwar analysis.

The warning label is there for a reason. The effect of a cyberattack cannot be counted in photographs the way a bombed building can. A collapsed apartment block has floors that can be counted; a destroyed tank leaves wreckage. But which unit lost communications for how many hours, and which orders failed to arrive in that time, are military secrets. Unless the victim discloses it, there is no ready way to verify from outside — and the victim is at war.

The Viasat hack shows the power and the limits of cyberattack together. Seen through a technical and operational lens, Russia demonstrated the ability to knock over civilian infrastructure in six countries across a border, in a chain, with one hour of precise timing. Seen through a strategic lens, that ability did nothing to bring about the swift fall of Kyiv. The same event is both a proof of capability and a failure to reach an objective, and all we are doing now is choosing which lens to name it by. We do not hold one settled answer.

Viasat is an American company. The network was not built by the Ukrainian government, nor owned by the Ukrainian military. Even before the war, Ukraine's military, government, and civilians used this company's satellite service together, and European households used the same service. A country's military communications, in other words, rode on a foreign company's commercial offering.

It is worth noting how the shape of the incident became known. The timing — one hour ahead of the ground forces — came from reporting by Patrick Howell O'Neill of Technology Review, the magazine published by the Massachusetts Institute of Technology. The assessment that the hack was an attack prepared along several routes came from Christian Vasquez and Elias Groll of CyberScoop, while Matt Burgess of Wired and the CyberPeace Institute called it a mysterious satellite hack that had claimed victims beyond Ukraine. What reconstructed the event was not an investigator's case file but the reporting of journalists and the after-the-fact analysis of security firms. The character of the available evidence was like that from the start.

It is also worth explaining what kind of instrument the 10 May joint statement was. The procedure by which the European Union, the United States, the United Kingdom, and the other Five Eyes countries named Russian military intelligence as the party behind the attack is called attribution in cybersecurity. It is a political act in which several countries speak the same name together to harden a fact — not a court's verdict of guilt. Who stood trial after that statement, and what punishment followed, does not appear in the public documents.

2. Did Cyberattacks and Missile Strikes Move Together?

The question Viasat leaves behind runs straight into a larger one. Did Russia's cyberattacks and missile strikes move together on a single timetable? Were the hackers and the artillery listening to the same commander?

The question matters because the defender's response changes with the answer. If the two are coordinated, a cyber alert is also a missile alert, and when servers shudder oddly the air defence units must tense up too. If they are not coordinated, they are separate wars turning at their own rhythms, and each must be blocked on its own.

There are several cases where the two appear to overlap. Viasat is counted as the first. One hour before the ground forces crossed the border is too precise a moment to call coincidence, and the precision is exactly why Bateman cited a 'clear military purpose'.

The Kyiv television transmission tower on 1 March 2022 leads to the same problem. The CNA report records that as the facility was struck by missiles, cyberattacks aimed at the networks of major broadcasters ran alongside. Two methods of cutting off broadcasting were used together on the same day. One breaks the tower, the other breaks the broadcaster's computers, and the intended result is identical: to keep the Ukrainian people from hearing the voice of their own government.

The same pairing appears in winter. After the front lines hardened, Russia used missile strikes and hacking together to cut Ukraine's heating and electricity, and the target was the survival conditions of civilians.

One number gives a sense of the scale. According to a tally cited in both the CNA and Henry Jackson Society reports, from the invasion through the end of April 2022 at least six distinct Russia-linked hacker groups carried out 237 cyber operations against Ukraine. Malware that wrecks networks, such as Whispergate and Foxblade, was deployed again and again. That is 237 operations in a little over two months — three or four a day. Cyberattacks were happening daily; they simply did not catch the world's eye.

That very number is also the trap in the coordination debate. Timetables overlapping and two attacks being coordinated under one chain of command are not the same statement. If cyberattacks are occurring three or four times a day and missile strikes occur nearly every day, then the fact that a hack also happened somewhere on a day a missile fell is not by itself surprising. The odds of two events landing on the same day near similar targets are not low on chance alone.

There is a long distance between picking out a few striking combinations and proving that cyber units and missile units shared a common target list. The first is case collection, the second is proof of causation, and no quantity of cases makes causation follow on its own.

Closing that distance would require Russian operational documents or chain-of-command documents — paper showing who instructed whom, when, to do what. No such documents are public now, and there is no sign that they will be.

The limits of the public record are left as they are. The reports relied on so far all come from the defending side: Western analytical institutions, American companies, Ukrainian authorities. No primary document in which the Russian defence ministry or its intelligence services explain their own methods of coordination appears in the list of public documents. This is watching a match from one set of stands. From there you can see where the ball went, but not what plays the coach called.

So on the question of whether they moved together, what can be said extends only to correlation observed from outside. Causation handed down from inside cannot be spoken to. The warning that analysis wobbles when conclusions are drawn from incomplete, early evidence applies not only to the Viasat dispute but equally to this synchronisation dispute.

Even if the question of coordination cannot be settled, one fact is certain: this war changed the nature of targets.

In traditional war, cutting an enemy's communications network meant bombing a transmission tower or severing a cable. That required a weapon to physically reach the problem. A bomber had to fly, a missile's range had to stretch, and along the way air defences had to be penetrated. The scope of war was set by the distance a weapon could reach.

AcidRain reached wind turbines in Germany. Without a bomber, without crossing a border, by way of a company's network management path. The very concept of range blurred. A weapon aimed at Ukraine arrived in homes in Poland and Greece, countries that had never consented to the attack and had never entered the war. That is why the European Union, the United States, and the United Kingdom felt compelled to issue a joint statement.

The Ministry of Digital Transformation that Fedorov led had to run a state under these conditions. The decision to move government data beyond the border and the decision to rush in satellite internet terminals were both answers to that condition. Why the hurry is explained by one fact: on the first day of the invasion, a satellite communications network had already been erased.

For a country that had prided itself on e-government, vigilance about network security grew after this incident. To say that a state is put inside a smartphone is to say that a state is placed on a network, and what is placed on a network can be erased along with it.

The question of coordination does not hang on the Russian side alone. It hangs equally on the Ukrainian side. Right after the invasion, hackers and citizens from around the world flocked to the 'IT Army of Ukraine' gathered on a Telegram channel, and the confirmed public scale was around 150,000 Telegram subscribers. Subscriber numbers and the number of people who actually took part in attacks

are different things, and on how many people attacked Russia's digital infrastructure, it is still too early to conclude from the public record. So claims divide over whether this was a unit commanded by the state or a gathering that citizens formed on their own.

The government's official position is that it was voluntary. Victor Zhora drew the line: he was grateful to the volunteer groups, but the activity was strictly voluntary and the state did not coordinate it. Fedorov, too, spoke forcefully of a moral right to protect citizens' lives while publicly and repeatedly denying the suspicion that the state had authorised or directed hacking against Russian civilian targets.

The circumstantial evidence pointing the other way is also plain. The IT Army began below the surface when the IT entrepreneur Yegor Aushev, at the request of a senior defence ministry official, gathered a thousand hackers, and Fedorov issued a public call to arms on his own Telegram channel on 26 February. There are records that the Ministry of Digital Transformation recruited for this crowdsourced hacking, and that a target list running from Russian media outlets to banks to government offices was regularly updated and passed down. Inside the organisation there were 25 to 30 'generals' believed to have come from intelligence services and government ministries, and beneath them 'colonels' who carried out the destructive attacks in practice. One figure who ran as a volunteer hacker before enlisting in the regular forces testified that coordination with government agencies existed even then.

This dispute does not stop at words. International law has two standards for binding civilian conduct to a state. Under the effective control test, responsibility attaches only if it is proven beyond doubt that the state exercised complete command. Under the overall control test, responsibility attaches if the state merely organised, coordinated, and supported. Ukraine can slip past the first standard, but not the second. On a ten-step scale devised in one report, this relationship in the early war sits between step four, 'state-encouraged', and step six, 'state-coordinated'. Ukraine's parliament and the Ministry of Digital Transformation drafted a bill to fold these hackers into the regular forces as a cyber reserve; if that law passes, the status rises to step ten, 'state-integrated', and all of their hacking becomes the state's responsibility.

3. The Failure Thesis and the Long-Attrition Thesis in Russian Cyberwar

Before the war began, Western cybersecurity experts were largely drawing the same picture, and that picture had grounds.

Russia had long been assessed as treating Ukraine like a proving ground for cyberwar. In 2015 and 2016 came the hacks of Ukraine's power grid. In the depth of winter the electricity went out in cities, and only later did it emerge that this had been a hack. In 2017, the NotPetya malware spread beyond Ukraine to 65 countries. Code aimed at Ukraine brought down the accounting and logistics systems of companies worldwide.

Looking at that record, experts expected a shock on the order of a so-called 'cyber Pearl Harbor' to arrive together with the full-scale invasion. It was a scenario in which the functions of a state stop within days. The picture was of electricity cut, banks halted, a government unable to say a word to its

people.

But the paralysis they feared, at that scale, did not come. In the spring of 2022, the British weekly The Economist reported a conspicuous absence of large-scale cyberattacks against Ukraine. The specialist outlet War on the Rocks carried an analysis pinpointing the failure of Russian cyber operations. The assessment was that cyberattacks had not managed to coercively change the course of the war. And so the 'Russian cyberwar failure thesis' took hold.

What was blamed for the failure? The analyst Justin Sherman set out five reasons why the effect of Russian cyber operations was suppressed: the difficulty of coordinating across domains, resource constraints, competition among intelligence services, deliberate strategic prioritisation, and Ukraine's defensive capability.

Among these, the item many analyses weighted most heavily is competition among intelligence services. Russia's cyber capability is not gathered in one organisation but scattered across several agencies. The military intelligence service named behind the Viasat hack is only one of them. The reading is that internal competition among these agencies over infrastructure and authority, together with the absence of coordination that would have aligned their operations, ate away at their own capability.

Yurii Shchyhol, head of Ukraine's State Service of Special Communications and Information Protection, offered a different explanation. Russia had not expected Ukraine to withstand the first wave of cyberattacks, and its plans for that contingency were not sufficient. So certain was it of a quick, decisive victory that it had not stockpiled the cyber volume and plans a long war would need.

It is a persuasive diagnosis. But it should be remembered alongside the fact that the speaker was the official responsible for the Ukrainian government's cyber defence. Words pointing to the enemy's lack of preparation are at the same time words explaining one's own organisation's performance. How the Russian side explains the situation lies outside the range of public documents. To write up victory and defeat from one side's testimony without the other's is closer to issuing a press release than to keeping a record.

The other half of the failure thesis is the response of Ukraine and the companies and governments standing behind it.

The AWS Snowball devices and the Microsoft cloud support seen in Chapter 2 show that the outcome of cyberwar was not decided by offensive technology alone. Backups, overseas storage, and allied threat detection limited what Russia's attacks achieved.

Beneath Ukraine's cyber resilience lay support from the United States government, American companies, and the United Kingdom. Speak of resilience only as one nation's virtue, and whose resources that virtue stood on is erased. When reading the sentence that Fedorov's digital state did not stop even on the first day of the invasion, this fact has to be set beside it for the scales to balance.

As the failure thesis spread, a rebuttal soon came. A piece by Cattler and Black in Foreign Affairs stands for it, and its title was 'The Myth of the Missing Cyberwar'. The argument runs like this: what

was absent was the cinematic collapse the public had imagined, not the attacks. Russia's attacks never let up.

The evidence is the numbers already seen. Six groups and 237 operations in a little over two months. The Viasat hack one hour before the invasion. Damage spreading to six European countries. The 5,800 wind turbines in Germany. To look at all that and say there were no cyberattacks, the rebuttal holds, is not Russian incompetence but observer failure.

The two camps were answering different questions. The failure thesis answered "did cyberattacks change who won the war?" The rebuttal answered "were there cyberattacks?" The answers are no and yes respectively, and both can be right.

The compromise the experts arrived at is this. Russia's cyber operations were not lacking in tactical volume of activity. If they failed, it was at the strategic level — the level that changes who wins a war. The cyber weapons worked diligently, but they did not end the war.

Once the quick victory collapsed and the front lines hardened, Russia's cyber operations changed character too. Clint Watts analysed that Russia's influence operations and cyber operations were adapting to a long war and boring into the West's 'war fatigue'. War fatigue means the state in which the publics of the supporting countries grow tired and start saying enough. It is a route by which support is cut off not because weapons run short but because the will is spent.

In this phase the target shifts from the command post at the front to the mind in the rear. The CNA report records that Russia put its weight behind information operations that widen divisions inside Western societies. Manipulated claims spread — that the inflow of Ukrainian refugees was lowering Europeans' standard of living — and propaganda chipping away at international trust in Ukraine followed. At the same time the targets of cyberattack broadened to energy grids and logistics. Missiles and hacking were used together to cut winter heating and electricity, and the intended result was civilian exhaustion.

This is the 'long-attrition thesis'. It reassesses cyberwar as a technique less for landing a single decisive blow than for grinding away at an opponent's infrastructure and patience over time — not dramatic collapse but tedious bleeding.

Lay the two discourses over each other and this picture emerges. Cyberattacks were not as dramatic as expected, but neither did they vanish. They did not end the war, but they were used to make the war long.

The lesson this picture gives the defender comes back to redundancy. If one satellite network is erased and another path remains, command continues. Data held on a single server inside the border disappears with one missile; data scattered across the clouds of several countries does not. The redundancy Victor Zhora spoke of was a design principle before it was an after-the-fact excuse.

This conclusion also explains where Fedorov and his ministry staked their resources afterward. It became clear within 2022 that defence and counterattack in cyberspace alone could not push back Russian ground forces. The outcome of the war was being decided in the trenches, on the roads, in

the sky, and among the cheap machines flying there.

If asked what cyberwar changed, one can answer this way. Cyberwar did not change how the war ends. It changed how far a war can reach, and it changed what a state must scatter in advance, in many layers, if it wants to survive.

The remaining questions stay open. How large a blow was the Viasat hack? Were the hackers and the artillery reading the same order? Is Russia's cyberwar a failure, or a different kind of success still under way? On these three, what we hold is evidence observed from the defender's side, statements from officials that contradict one another, and reports that declare themselves incomplete. Knowing precisely what we do not know helps in understanding this war more than pretending to know the answers.

The source of the figure 237 deserves stating. The tally came from a Microsoft report. The same company was also the party that supplied cloud services to the Ukrainian government. Clint Watts, who analysed that Russian cyber operations were adapting to a long war and boring into Western war fatigue, is likewise with Microsoft. That the side counting and the side defending are the same does not make the number wrong. But it is more honest to note alongside it that the cyber record of this war was made largely in the hands of the companies that took part in the defence.

The tone in which the failure thesis spread survives in the titles. The Economist spoke of a conspicuous absence of large-scale attacks, and the piece in War on the Rocks was titled 'Why Russia's Cyber Dogs Have Mostly Failed to Bark'. Justin Sherman's analysis was titled 'Untangling Russia's Cyber Matryoshka'. A matryoshka is the Russian wooden doll with smaller dolls nested inside, layer upon layer. The title carried the meaning that Russia's cyber capability is not one mass but divided into many layers.

The names of those layers are the military intelligence service (GRU), the foreign intelligence service (SVR), and the federal security service (FSB). The one named behind the Viasat hack was only one of them. Internal competition among these agencies over cyber infrastructure and authority, and the absence of coordination that would have aligned their operations, cut away at their own capability — that is the diagnosis of several analyses.

On the Ukrainian side, the opposite happened. American and British support did not rush in after the invasion began; it was already in place on the eve of the war. Resilience is a name given to a result, and mixed into that result are other people's resources that had arrived ahead of time.

Chapter 6. From Crowdfunding to the Army of Drones

1. The Circuit That Turns UNITED24 Donations into Drones

In June 2022, on the stage of the Cannes Lions International Festival of Creativity in Cannes, France, the Ukrainian government's fundraising platform UNITED24 was introduced. A festival where people who make their living in advertising and marketing hand one another awards, and there a wartime country's national fund was being unveiled: the pairing was strange in itself. Two months later, at the Ukraine Recovery Conference in Lugano, Switzerland, UNITED24 presented its first report card. Donations gathered in the platform's first two months had passed 75 million dollars. At the same venue, the platform recruited participants for the Army of Drones (Армія дронів). Within three days, the amount raised reached roughly 200 million hryvnias.

Collecting donations and using that money to buy weapons and deliver them to units are two different jobs. That the second is far harder than the first was written nowhere in that summer's announcements.

In any country in the world, the money that buys weapons comes out of the defense budget. Parliament approves the budget, a procurement agency opens a tender, a contract is signed, and the goods pass through a warehouse and arrive at the unit. This route is slow. There is a reason it is slow. Buying weapons with tax money must carry oversight and records along with it. Only if there is a record of who bought what and for how much can questions be asked later, and only if questions can be asked does the money stop leaking. Procurement is slow because slowness was designed into it from the start.

Ukraine in 2022 was in no position to bear that designed slowness. Units at the front needed drones they could fly today, and the normal procedure would deliver them months later. Mykhailo Fedorov, the Minister of Digital Transformation, built a separate channel that connected card payments from citizens around the world to drone purchases for the Ukrainian military. This circuit did not abolish the Ministry of Defense's procurement line. It was a second track laid alongside it, and the difference in speed between the two tracks would reshape the terrain of Ukraine's defense industry over the years that followed.

The donations began on smartphones. From the earliest days of the war, Fedorov posted the government's cryptocurrency wallet addresses on social media and asked for contributions. He saw this method as both a way of raising funds and a way of holding the world's attention. His judgment was that even a small donation creates a relationship between an individual somewhere in the world and Ukraine, and keeps the war inside people's screens. Someone who gives five dollars will keep looking for news from Ukraine afterward. Fedorov believed that fundraising could gather money and the world's attention at the same time.

This judgment carried into Diia, the state administrative app. Diia added functions for donating to UNITED24 and buying war bonds. On the same screen where they had been looking at their ID cards and driver's licenses, citizens could now add to the defense budget. Research reports described this

combination as an administrative app changing its character into a fintech tool for war financing. In the first three months after the invasion began, more than 166 million dollars was gathered for military and humanitarian needs. The support categories available through Diia included fundraising for drones, and tens of millions of hryvnias came in through this route for the Ukrainian military and the Army of Drones.

Securing a budget does not mean drones are immediately deployed to the front. Ukraine in 2022 had small companies and workshops scattered across the country that could build drones, but most of them had never delivered anything to the military. To supply the military, you must pass the Ministry of Defense's tests and receive an official code. A code is the registration number that puts an item on the military's supply list. Without that number, no matter how well an item flies, the military cannot pay money for it. To get the number you need test reports and technical documents, and you need someone who has written such documents before. A company with twenty employees has no such person. A technician who had been shaping propellers in a warehouse could not suddenly start writing military administrative paperwork.

The Army of Drones project focused on shortening the delay between purchase, testing, and deployment. The Ukrainian government substantially loosened the profit margin cap on drone manufacturers through "Decree No. 256." Analytical reports record that the Army of Drones project was created immediately afterward. A profit margin cap is the ceiling on the profit a company may keep when selling to the state. If the ceiling is too low, the company loses money the more it makes, and no one enters a market where they lose money. The project's aim was to use the funds gathered through UNITED24 to draw new companies into the market and get them supplying drones to the military. It did not stop at buying finished products. It cut down the stages of testing and quality certification paperwork, and it attached dedicated staff to help entrepreneurs pass the tests. Once a manufacturer received its Ministry of Defense code, the Army of Drones paid the production costs of the drones destined for the Ukrainian military directly, out of UNITED24 funds.

The government gave companies funding, testing opportunities, and a procurement channel. It rewrote the rules so they could make a profit, pushed their paperwork through for them, and bought their first products. In the world of startups, this role is called an accelerator: an organization that attaches money, advice, and a first customer to a newly born company all at once. The fundraising platform became both an institution supporting fledgling defense firms and their first buyer. This approach later led to the defense technology cluster called Brave1. Donations passed through deregulation and paperwork assistance and landed in the production costs of new companies.

On 30 October 2022, Fedorov announced that he would reinforce the Army of Drones with Ukrainian-made attack drones, and that cooperation agreements had been concluded with four companies. It was a Ministry of Digital Transformation announcement, and its center of gravity rested on the words "Ukrainian-made." It was a declaration of direction: a country that had relied on goods bought from abroad would move toward being a country that buys what its own companies make. A supply line that leans on imports hangs by someone else's decisions. A single export restriction, a single change in a manufacturer's policy, can close the front's eyes. That said, how many aircraft the

four contracts produced does not appear in the announcement. The contract unit prices were not disclosed either. What the announcement confirms extends as far as the project's direction; the actual results remain unanswered.

This circuit cannot be read as mere self-congratulation by the Ukrainian government. Analysis from outside the government confirms the same function. One policy research report assessed that the Ministry of Digital Transformation's points system and UNITED24 had created a sustainable procurement and development channel. Behind it, the report saw government procurement slowed by bureaucracy and a shortage of capability at the front line. It is a structure in which a fundraising platform created by the government fills what the government cannot deliver on time. Written out in a sentence it sounds bizarre, but at the front it was an answer you could hold in your hand.

The scale of citizen fundraising was not small either. According to a Forbes analysis, donations to the top 50 charities plus public fundraising amounted to 2 to 2.5 percent of Ukraine's gross domestic product in 2023. Gross domestic product is the sum of the wealth a country produces in a year. It means that roughly one-fiftieth of it flowed toward defense under the name of voluntary citizen donations. When money on this scale moves outside budget deliberation, whoever stands at the junctions it passes through holds power that never went through a parliamentary vote.

But the detailed record of how the funds were used was not sufficiently disclosed from the beginning. The amounts raised are made public. How much went to which model from which company is not. Whether the contract unit prices were appropriate, and why the companies that lost out were rejected, also remain unanswered. No independent audit document confirming these things could be obtained. The published figures are, for the most part, values announced by UNITED24, the Ministry of Digital Transformation, and the Ministry of Defense. A structure remains in which the same government that built the system evaluates that system's results.

The Ministry of Digital Transformation built a channel connecting donations to drone purchases. These two sentences from 2022 became the first stretch of the road that, some years later, would take Fedorov into the Ministry of Defense building.

Fedorov had already pulled in outside resources in a similar way in the field of communications. In February 2022, just before the invasion, Russian hackers attacked the American company Viasat's KA-SAT network. Thousands of satellite communication modems used by the Ukrainian military and government were knocked out. Several reports and official statements hold that the attack left a major communications loss in the command-and-control network, though the scale of its impact is assessed differently across the literature. On 26 February, Fedorov asked Elon Musk for Starlink terminals on X. The answer came in under twelve hours. Two days later the first shipment arrived. The method of pulling in resources from outside the government through social media rather than through an approval chain had, by then, already been through one trial run. Four months later, UNITED24 taking the stage at Cannes was that same method transposed onto money.

When you lean on a private company's service, that company's decisions can also cut the service off. When the Ukrainian military ran an unmanned surface vessel operation in the waters off

Sevastopol, the Starlink connection did not come through. Whether a service already switched on was blocked, or whether Musk refused Ukraine's request for an expansion of coverage, differs across the literature. What is confirmed is that the operation of the unmanned vessels that lost communications failed, and that the extent of use of a major communications network was decided by SpaceX, a company. The evidence for and the limits of both versions are set side by side in Chapter 4.

The donations that came in through UNITED24 were spent on drone procurement alongside the state budget. It was one of the three sources from which Ukraine has funded drone purchases since 2014. Money from large private foundations such as Come Back Alive and the Serhiy Prytula Foundation flowed in the same direction. It means that no small share of the money holding up national defense hangs on donors' decisions rather than on budget deliberation. What the plan is for a situation in which donations decline — in the public documents collected, the public record stops here.

2. A National Project Binding Together Pilot Training, Repair, and Replacement

Sending one drone to the front is not like sending one parcel. A drone has to be flown by a person, repaired when it breaks, and replaced with a new one when it cannot be repaired. If even one of these three is missing, the other two collapse. A drone with no pilot is a box in a warehouse. A unit with no repair personnel runs out of airframes within a month. When replacement is late, the better a unit fights the sooner it is left empty-handed, because the more you use, the more you lose. What Ukraine built after 2022 did not stop at a program that bought drones; it grew into a national project that bound training, repair, and replacement into one.

Pilot training in the early war was in the hands of volunteers and private drone schools. People who had flown drones as a hobby rented warehouses and opened courses, teaching neighbors headed for the army how to hold the controls. What the state did was draw this civilian energy into the military's personnel system. The Ukrainian Ministry of Defense created a procedure for officially certifying civilian nongovernmental organizations and private schools, and certified more than 30 drone pilot schools. Graduates of certified schools became eligible for the qualification "Military Occupational Specialty Number 216: External Crew Member of Unmanned Aerial Vehicles."

An occupational specialty number is the number tag by which an army classifies people. Only with a number does a person exist as a "drone pilot" within the military's personnel records. Only with a number is he assigned to that post, and when that post empties, it is filled by someone with the same number. Without a number, no matter how well he flies, on paper he is an infantryman, and if he is killed, one infantryman is subtracted; a pilot is not counted as lost. Losses that are not counted are not caught in replacement planning either. The state certified civilian drone schools and attached a number to them. A skill learned as a hobby began to be recognized as a military specialty. This change later led to the founding of the Unmanned Systems Forces.

The names of the certified schools are themselves a map of this ecosystem's terrain. Borvibiter and Kruk are certified schools teaching the military specialties of the Unmanned Systems Forces. Borvibiter divided its courses by aircraft type — multirotor, fixed-wing, FPV multirotor. FPV means "first-person view," a method in which the pilot watches the feed from a camera mounted on the aircraft

through goggles and flies as if he were sitting inside it. Killhouse Academy taught civilians and soldiers the practical operation of FPV drones. ProFPV UA Drone ran courses on handling commercial airframes such as the DJI Mavic and the Autel EVO in combat. UA Drone School kept a four-day intensive course for units that had to send people out in a hurry.

The civilian training institutions, including these schools, stated that they had trained more than 250,000 people since 2022. The fields of instruction included FPV piloting, maintenance, mission planning, and deep strike. This 250,000 is a figure the training institutions tallied and put out themselves. How many of the graduates actually took the controls at the front — the public record stops here. Whether a four-day course and a several-week course were counted as the same "completion" also remains unanswered. No external evaluation document comparing training quality across schools could be found either. It is more accurate to read it not as proof of achievement but as an indicator of scale, showing how many people this country pushed into this work.

Nor does it mean the training was free. Consider the case of one foreign top-tier manufacturer. Training four pilots for intelligence, surveillance, and reconnaissance drones cost roughly 30,000 euros. The equipment they would use cost roughly 100,000 euros. Intelligence, surveillance, and reconnaissance is the collective name for the missions of finding, watching, and learning about the enemy. Because nothing explodes in these missions they rarely appear in the news, but without them the question of where to strike goes unanswered. The arithmetic is that putting four people into that post cost 130,000 euros, and the phrase "cheap drone" is already starting to slip in front of these training and equipment costs.

Repair was harder still. Drones on the battlefield are shot down, crash, or lose control to electronic jamming. Even the airframes that come home need their propellers, cameras, and batteries swapped out before they can fly again. In automotive terms, it is like crashing every day and going into the shop every day. The reality was not smooth. Because manufacturers' after-sales support was lacking, combat unit members had to assemble their own teams to handle modification, repair, and performance improvement of the equipment. Frontline drone pilots received an allowance of roughly 3,000 dollars a month. There are records that they spent 5 to 30 percent of it out of their own pockets on equipment repair and upgrades.

There were cases of soldiers repairing state-issued drones with their own money. This burden on the ground has to be seen together with the large-scale fundraising results. At the far end of the very circuit where the world's donations filled 200 million hryvnias in three days, a pilot was putting parts on his own card. Procurement grew faster, but that did not mean the necessary support reached every soldier.

The state responded by pulling repair into the training curriculum. Prometheus, a Ukrainian provider of open online courses, opened a course called "FPV for the People" teaching assembly and maintenance. Kyiv Drone Pilot ran an engineering course covering both piloting and maintenance skills. Dronarnia offered hands-on training specializing in the assembly, maintenance, and repair of tactical attack drones and small-batch production. At the front, the pilot and the mechanic are often the same person. The soldier who launched the airframe in the morning picks up a soldering iron in the

evening. That is why piloting and maintenance instruction went into the same program.

What handled replacement was the "Army of Drones Bonus," which converted strike footage into points and let units choose the drones they needed with those points. The system's scoring and verification procedures are covered in Chapter 10. In this chapter we look at the fact that supply authority moved from the central warehouse toward brigades and frontline units.

In a fast procurement process, inspection and accountability checks can be pushed to the back. Distributing equipment by points also means that missions good at generating points gain an advantage over missions that generate points poorly. How reconnaissance, communications relay, mine clearance, and rescue of friendly troops — missions with no explosion in them — are calculated has not been disclosed. The authority and procedure for setting the coefficients: the public record stops here. Who filters out inflation in performance reports also remains unanswered. Independent documents answering these questions: within the range of public records collected, the public record stops here. There is no basis for saying the system's designers were unaware of this problem, and none for saying they solved it; only the questions remain open.

It is worth noting who actually ran this training network. Most of the more than thirty certified schools were not government agencies but civilian nongovernmental organizations and private schools. The state did not build new schools itself. It certified private schools that were already operating. The actual instruction was handled by organizations outside the government. Where the schools' operating funds came from: the public record stops here. Who sets instructor qualifications and by what standard also remains unanswered. The criteria for revoking certification could not be found in the published public documents either.

The record that units assembled their own teams for modification, repair, and performance improvement also means that combat units came to double as small factories. It is a state in which the after-sales responsibility that should fall on the company that made the weapon has been passed to the person using it. As for what line item the 5 to 30 percent taken out of a soldier's allowance is entered under in the country's defense spending statistics — or whether it is entered at all — no document within the range obtained tells us.

Once replacement authority moved downward, the buyers themselves became many. From 2024, budget execution by local governments and direct purchasing by brigades were permitted. Goods arrive quickly. But the procedure for gathering in one place and comparing who bought what at what price: the public record stops here. The audit method for inspecting the purchase records of brigades and local governments could not be found in the published public documents either. As the circuit grew faster, the windows for looking into the circuit should have grown in number too, and where those windows are is still not visible.

3. The Myth of the Cheap Drone and the Reality of Production, Munitions, and Electronic Warfare

Articles on Ukraine's drone war have a favorite contrast: one kamikaze drone costing a few hundred dollars destroys a tank worth millions. The numbers are vivid and the picture is satisfying. This contrast

holds one fragment of the truth, but looking only at that fragment leads you to read the economics of the war backward.

Look at the training costs and the soldier's out-of-pocket burden and you can see the costs left on the ground. Putting four pilots into intelligence, surveillance, and reconnaissance work cost 130,000 euros in training and equipment. The pilots stood up that way were putting part of their own allowance back into maintaining equipment. Not one of these items appears on the airframe's price tag. It is not that drones are cheap; it is that the drone's real cost is scattered outside the airframe. So it goes with training people, maintenance personnel, communications networks, batteries, video transmission and reception gear — and attrition rates.

The attrition rate is the axis of this calculation. Once you fix how many you lose in a month, the cheap airframe changes from a one-time consumable into a recurring monthly expense. If one unit loses 100 drones at 500 dollars each in a month, that unit's drone cost is 50,000 dollars every month. Watching only the video of the single drone that destroyed a tank leaves the question of cost unanswered. The price of the dozens that fell short of their targets has to be counted too. That cost, all of it, is the real price that went into one success. How much the supply of warheads and explosives carried by kamikaze drones adds to that price cannot be given a number from the public record, so it is left blank.

Industry tells the same story in a different language. The Kyiv School of Economics Institute and Brave1 published "Ukraine's Drone Industry: Investment and Product Innovation" on 4 October 2024. The report analyzes the drone industry with investment and revenue at its center. It carried the 15-million-dollar investment raised by the Ukrainian startup Swarmer and its revenue indicators. Swarmer is a company building autonomous flight swarm technology. The source of that chart is listed as UNITED24.

The source of the drone industry statistics is largely a government platform. The drone industry's money passes through a government platform, and even the data used to analyze that industry leans on the same platform's tallies. While the circuit turns well, it is efficiency. Money and information sit in one place, so decisions are fast. When external verification documents are scarce, it becomes hard to find the cause once something goes wrong — because the institution that built the system also evaluated its own results.

The reality of production was not as smooth as the announcements either. New companies entered the market only after the government eased the profit margin cap. After that, the state also trimmed the testing and certification paperwork. It attached dedicated staff to help companies get registered with a Ministry of Defense code. The record that manufacturers' after-sales service could not keep up, forcing units to assemble their own repair teams, is part of the same picture. Building factories was not enough. For the drones produced to keep moving at the front, training, repair, and parts supply had to follow. Ukraine ran into serious difficulty in this operational stretch.

In front of electronic warfare, what we know and what we do not must be kept apart. What actually determines a cheap drone's lifespan is not the enemy's tank but the enemy's jamming. This

technology, called jamming, works by laying heavy noise over the radio waves passing between the drone and the pilot until the signal breaks. When the satellite navigation signal is cut along with it, the airframe no longer knows where it is, and even a well-built drone falls out of that spot. Drones that send control signals over fiber-optic cable emerged to evade jamming. Guidance technology that flies the final stretch to the target without human control also appeared.

But within the documents used as a foundation here, figures supporting jamming success rates, the share of fiber-optic drones, and the scale of adoption of automatic guidance — the public record stops here. What lies outside the public record cannot be written as if confirmed, so this blank is left as it is. That jamming is a central variable of the drone war, and that we cannot yet speak of the size of that variable in numbers, must both be written down together.

What can be recorded instead is where this debate is taking place. The Australian Army Research Centre published "Drones in Modern Warfare: Lessons Learned from the War in Ukraine" on 22 October 2024. The American Irregular Warfare Center released "Six Lessons from Ukraine's Drone War" on 20 May 2026. The very fact that the armies of various countries are organizing this war's drones under the heading of "lessons" is itself an event. Among the things Ukraine has produced, along with weapons, is a textbook that other countries open when they redesign their own militaries. Whether the two reports arrive at the same conclusions as the Ukrainian government's announcements is a question that can only be answered after a document-by-document comparison.

One boundary needs to be laid out. The Army of Drones is not a military formation. It is a procurement and mobilization program that buys drones with donations and state budget money and sends them to units, trains pilots, and converts results into points to support replacement. Brave1 is an organization that supports defense technology startups. The Unmanned Systems Forces is a formal branch grouping the soldiers who operate drones, and it was created later than Brave1. The three are often introduced in the news as one lump, but the time they were created, their authority, and the people accountable for them are all different. Miss this distinction and one person's achievements get inflated, or another person's responsibility gets erased.

The story that began on the Cannes stage in the summer of 2022 therefore ends as neither a success story nor a failure story. The world's donations turned into 200 million hryvnias' worth of orders in three days. Contracts were signed with Ukrainian manufacturers. A pilot training network and a performance-based equipment replacement system were built afterward. The same circuit left a hole that sucked soldiers' pay into repair bills, and left a blank in verification where the maker of the results grades its own results.

Fedorov played a central role in building this procurement channel. Whether what he built was an auxiliary line assisting the Ministry of Defense, or a main line headed toward replacing it, remains a question still unanswered.

The costs scattered outside the airframe's price tag include the communications network. What ran Kropyva and Delta, the Ukrainian military's command-and-control and situational awareness software, was Starlink satellite internet, and a terminal could be set up at the front in fifteen minutes. One

analytical report recorded that thanks to this connectivity, the time from a drone spotting the enemy to artillery or an FPV drone striking dropped below five minutes. The number of terminals grew from roughly 42,000 in early 2023 to roughly 200,000 by around October 2025. For a 500-dollar airframe to hit its target, a satellite communications network on this scale has to be laid out behind it.

The cheap combination was not used by one side only. The Russian military mounted Starlink terminals smuggled through third countries onto Iranian-made Shahed kamikaze drones. Airframes modified this way exchanged documents in real time from as far as 2,000 kilometers away. It meant they could strike deep into Ukraine's rear. The combination Ukraine found first was also used in the opposite direction.

So what makes the phrase "cheap drone" wobble is not the price of the airframe. The real cost of one drone includes the pilot's training and the repair bills the unit paid. The cost of satellite terminals at the front is hard to subtract either. No document was obtained that also calculates the risk that the enemy can use the same terminals. What we know is the names of the line items, not their sum.

Chapter 7. Brave1, a Defense Silicon Valley Inside a War

Brave1 is a defense technology support organization created by the Ukrainian government. According to its official website, as of 13 July 2026 it counted 2,500 member companies and more than 5,000 registered products. Manufacturers of unmanned aerial vehicles numbered more than 500, and makers of artificial intelligence and unmanned ground vehicles more than 200 each. Brave1 serves as the window that connects companies with the military, the government, and investors.

These figures are Brave1's own tally, published by Brave1 itself. Nowhere on the site is there any sign that an outside accounting firm or audit body verified them. The public record stops here.

1. Gathering Startups, the Military, the Government, and Investors in One Place

Ukraine's defense technology market in 2022 was hot, but it was scattered. More and more people were assembling drones in garages and apartments, and software companies that had made apps and games in peacetime began writing programs for the battlefield. The trouble came at the next step. There was no official window for showing what you had built to the military, and what linked frontline units with developers was mostly a personal introduction or a post on social media.

Without an official channel between developers and the military, even testing a product is hard. Suppose a developer builds a communications module that can withstand enemy jamming. He has no way of knowing whether his device is any good. Only a unit at the front can judge that, and he has no way of learning where that unit is or whom to contact. The other side faces the same wall. A company commander at the front fights his battles without knowing that the very equipment he needs today already exists as a finished prototype in the corner of some workshop. The technology and the demand were inside the same country, yet they could not find each other, and the price of that mismatch was paid at the front.

Brave1 was the arrangement built so that developers and the military would meet at a single window. In April 2023, the Ukrainian government launched the defense technology cluster. The government's introductory documents state that six ministries took part. Yet only five participating institutions can be identified by name: the Ministry of Digital Transformation, the Ministry of Defense, the General Staff, the National Security and Defense Council, and the Ministry of Economy. Of these, the General Staff and the National Security and Defense Council are military and security bodies that do not hold the status of a government ministry. Which institution the sixth is, and whether the government's "six" counts ministries and other bodies together, cannot be confirmed in the public documents this account rests on. Rather than copying a single number across as it stands, we mark what lies outside the public record as lying outside the public record.

What can be confirmed lies beneath that. Brave1 is a national program created jointly by several government institutions, and the breadth of that participation makes it a stretch to call it the creation of Mykhailo Fedorov alone. The Ministry of Digital Transformation stood at the center of operations, but the Ministry of Defense, the General Staff, the National Security and Defense Council, and the Ministry of Economy interlock with it on questions of procurement and regulation. The moment this organization

is called by one person's name, the responsibility that several institutions divided among themselves is also heaped onto that one person. Credit shared is blame that can be shared, and in wartime administration this distinction is where any later audit begins.

Consider its legal form. Brave1 does not hold the status of a separate, independent legal entity. It is a national program and a marketplace that runs inside the Innovation Development Fund under the Ministry of Digital Transformation. It occupies the in-between role of a platform inside a government body, and that in-betweenness becomes a problem again later on. A company has shareholders and auditors who examine its books. A military unit has a chain of command and military inspectors on its heels. A platform inside the government falls cleanly into neither net, and by that much it grows unclear where the duty to audit resides.

The platform took on the intake and testing of products and the provision of funding. Its work was to build an entry point, to supply early money, and to draw in private capital.

Start with the entry point. An analysis by the French Institute of International Relations (IFRI) describes Brave1 as the primary entry point through which more than 2,000 private startups and small and medium-sized firms pass in search of government support and investors. Where a developer once had no idea which door of the Ministry of Defense to knock on, now there is one door to knock on. That there is only one door is a convenience and at the same time a danger, because the judgment of those who guard that door comes to decide the fate of the whole market. No method was put in place to determine later whether a technology rejected in review was in fact poor, or whether the reviewer's eye was narrow.

A state supplying early money is a different matter in kind. Hardware startups have trouble getting bank loans. At the stage where nobody knows whether the prototype will fly or explode — that is, a company at technology readiness level 1 through 5 — banks willing to lend are rare in wartime and in peacetime alike. Technology readiness level is a scale that divides the distance from an idea to battlefield deployment into nine steps. One is a principle on paper; nine is a finished product proven in actual combat. Levels 1 through 5 mean that nothing has been proven yet. That is the stretch capital fears most, and so it is the stretch that stands empty everywhere in the world. This is why founders call it the valley of death. The idea is alive but there is no money, so it dies in front of the prototype, and technology that dies that way never even appears in the statistics.

Brave1 filled that role with non-repayable support, that is, with grants. A grant is money given with no obligation to pay it back. If the company fails, the money is not recovered; if the company succeeds, no equity is taken. In exchange comes a condition: a prototype of specified performance must be delivered within a specified period. As of September 2024, 329 grants had been paid out, totaling five million dollars. In 2025 the scale changes. Grant financing passed sixty million dollars and spread to more than 600 companies, and the 2025 national budget set aside roughly 71.6 million dollars for Brave1 grants. Developers could apply for between about 12,000 dollars and a maximum of 192,000 dollars, depending on the importance of the project. From five million dollars to sixty million: more than a tenfold increase in a single year.

In September 2025, in an interview with a Ukrainian military channel, Mykhailo Fedorov called Brave1 "Ukraine's largest angel investor." An angel investor is an individual who puts personal money into a company at its earliest stage, when it has neither revenue nor a product. In Silicon Valley, successful founders and retired executives take that role. They operate on the arithmetic that if you back ten companies, nine may fail so long as one succeeds enormously. Fedorov's declaration is that the state has taken over that role. It sounds like a boast, but it also means that risk private capital will not carry is being carried by taxes. An angel investor pays for nine failures out of his own pocket. When the state calls itself an angel investor, the citizens pay for the nine failures, and the bill is absorbed into the budget without ever arriving on anyone's desk.

The last task was drawing in private capital. Brave1 maintains a database of more than 150 venture funds and regularly held demo days where companies could present directly to investors. Oleksandr Bornyakov, deputy minister of digital transformation, testified to how bleak the early days were. In early 2023, he said, nobody wanted to invest in defense technology, so they had to travel through Europe and the United States explaining it in person. By his account, the Ukrainian government went abroad to vouch for the creditworthiness of its own founders. The cluster set itself up as a guide through Ukraine's complicated administration, and it vetted founders' backgrounds so that trustworthy teams could be connected to foreign investors.

As time passed, the roster filled in. Funds such as D3 Venture Capital, in which former Google chief executive Eric Schmidt took part as a partner, along with MITS Capital, Green Flag Ventures, and Nezlamni, created by the ride-hailing company Uklon, entered this ecosystem. Ukraine, in the third year of the war, had been plotted as a coordinate on the map of international venture capital.

Report cards for individual companies came in as well. Swarmer, which builds artificial intelligence for drone swarms, received grants of 50,000 dollars and then 200,000 dollars from Brave1, proved out its technology, then raised 2.7 million dollars in seed investment, and in 2025 raised a Series A round of 15 million dollars. Seed investment is the first money at the stage of sowing the seed; a Series A is the money for widening the field once that seed has sprouted. The road Swarmer walked — building a prototype with a state grant, then standing before private capital with the result in hand — is the model specimen of the circuit Brave1 designed. Osavul, an artificial intelligence company countering disinformation, raised three million dollars, and Farsight Vision, a battlefield intelligence platform, raised 600,000 euros. Bornyakov said an ecosystem of several hundred angel investors had formed, and looked ahead past ninety million dollars to venture investment on the order of 150 to 200 million. That last figure is his forecast, not a result.

The numbers offered so far are inward-facing numbers of "money that went in" and "companies that gathered": grant amounts, company counts, product counts, investment raised. They say nothing about what was destroyed at the front, or how much. Investment raised is an indicator of how the market prices this country's technology, and proof that the technology actually worked has to come from somewhere else. The companies that documents on Brave1 hold up as success stories are, for the most part, described as successful on the basis of their funding rounds. That an investor placed a bet and that a soldier's life was saved are two different sentences, and the distinction cannot be erased

on the way past.

The names of the companies that received grants remain in public documents. DeepState, Swarmer, Skylab, Mantis Analytics, and Frontline spent this money on early product development and performance testing. The side whose names remain is the side that survived. The name of a company that took a grant and then stopped in front of its prototype appears on no list, and whether such a list was ever compiled at all — the public record stops here.

Comparing the grants with private investment shows the scale of the early money the state took on. D3 Venture Capital, with a fund of 19 to 30 million dollars, puts 125,000 to 750,000 dollars into a single company. MITS Capital, at a scale of 50 million dollars, puts in 100,000 to 500,000. The Brave1 grant ceiling of 192,000 dollars is comparable in size to a single one of these private early investments. The state sat down with money of roughly the same size as a private investor's, and the only difference is that it takes no equity.

Swarmer's seed round drew in the American defense firm R-G.AI, along with Radius Capital, Green Flag Ventures, and D3, and in February 2026 the company filed for a Nasdaq listing, the first Ukrainian defense technology firm to do so. A company primed by 50,000 and 200,000 dollars from the state is knocking on the door of the American securities market. If the listing goes through, the gains go to shareholders. How the Ukrainian treasury, which carried the early risk, gets its share of those gains back — or whether it gets anything back at all — does not appear in the public documents.

The vetting Bornyakov described is also worth a second look. The cluster checked founders' backgrounds and connected only trustworthy teams to foreign investors. For an investor, this amounted to having the risk of an unfamiliar country filtered by that country's own government. Turned around, it also means that nothing has been settled about where responsibility goes if a team the government picked later causes trouble. When a state stands as guarantor, the state's credit rises and falls together with the company's.

2. An Institutional Experiment That Changed the Speed of Testing, Certification, and Contracts

The cluster set out to shorten the time it takes for a product to reach a unit. For a single weapon to enter an army, it must ordinarily pass through a long procedure. It passes testing, is checked against specifications, is entered on a register, has a contract signed, and has budget disbursed. Each stage exists for a reason. If unverified equipment is put in a soldier's hands, that soldier dies. If budget goes to an unvetted supplier, that money disappears. Procedures are slow in order to prevent accidents, and in peacetime it would not be strange for this road to take several years.

The lifespan of technology on a drone battlefield is far shorter than that. If the other side changes the frequency of its electronic warfare equipment, an airframe that flew perfectly yesterday falls today. Electronic warfare means a fight in which radio waves are the weapon. It jams the radio signal linking a drone to its pilot, or feeds it false position data to bring the airframe down. The board of this game changes on a scale of weeks. When the speed of procedure and the speed of the battlefield fall out of step, a weapon that passes the procedure loses its usefulness while passing it. On the day a drone

verified perfectly over three regulation years is deployed, that drone is already an obsolete object.

It was this mismatch that Brave1 laid hands on, and it laid hands on two tasks.

First, it seated the military at the review table. Applications submitted to the cluster are examined jointly by representatives of the defense forces. Products are screened against the demands of the front, and the selected products are then supported through testing and NATO equipment codification. Codification is the work of assigning each piece of equipment a unique number that conforms to international standards. Think of the barcodes on the goods around us and it becomes easy to grasp. Without a number, an item cannot ride on allied supply systems, and it has trouble getting onto official procurement lists. It looks like trivial paperwork, but this number is what lets an object rise onto a contract. Invention is the business of engineering and the number is the business of bureaucracy, and when the two do not meet, the invention stays in the warehouse.

Next came the marketplace. On 28 April 2025, Brave1 Market opened. It is an online catalog and procurement channel through which Ukrainian military units can search for and order defense technology products directly. A structure in which a unit orders straight from a manufacturer means skipping several rungs of approval in between. Instead of an application climbing from brigade to division, from division to some directorate of the Ministry of Defense and on to some department, collecting stamps along the way, a company picks its equipment off a screen. What is worth noting is that Brave1 tried to thread review, testing, codification, and ordering onto a single line.

That is how the system was designed, but the actual results have to be confirmed separately. What can be confirmed is that a new procedure was created; whether that procedure actually turned months into days is another matter. Nowhere in the documents underlying this account is there an independent measurement showing how many days it took to reach a contract before Brave1 stepped in and how many days it took afterward. There is only the cluster's own announcement that things got faster, and analytical reports that cite the government's announcements. To confirm an improvement in speed with numbers, one would need the procurement agency's statistics on contract processing times, and a considerable share of wartime procurement information is withheld on grounds of security.

Nor is there any ground for calling the sentence "it got faster" false. It means the claim is unverified; the first sentence is a rebuttal and the second is a reservation. When a government at war reports on the results of its own policy, the report generally points in the direction of the truth without pointing precisely at the size of it. Readers have the right to read direction and size separately.

Outside eyes were not entirely absent. In October 2023, the Center for Security and Emerging Technology (CSET) at Georgetown University issued a report on a drone conference that the U.S. Defense Innovation Unit (DIU) and Brave1 held jointly in Warsaw. It means that six months after the cluster launched, a Western policy research institution had begun taking Ukraine's drone ecosystem as a direct object of observation. Ukraine's institutional experiment proceeded from the start before internationally watching eyes. Observation is not audit, but it is better than no one looking at all.

There is one more fact that must be set alongside any judgment of this experiment's worth. Brave1 did not replace the procurement system. It is a channel that exists separately from the Ministry of

Defense's formal procurement, closer to a forecourt leading into formal procurement. So no matter how fast the cluster runs, if the door of budget and contract is blocked at the final stage, the goods do not reach the front. Analyses of drone production capacity have pointed out that Ukraine's bottleneck has shifted from whether it can build to whether it has money to buy. That bottleneck lies outside Brave1's design. Even after the government raised the speed of making, the speed of buying remained a budget problem, and the cluster alone cannot untangle a situation in which the factories are running but the orders do not come.

Brave1 turned the path by which a developer meets the military into an institution, and as for how much that path shortened overall procurement time, with the documents public today, the public record stops here.

The volume arriving at the review table is not small. Documents on the cluster record that more than 900 applications were processed in a single year. The reviewers are representatives of the defense forces. The principle that the people who will use a weapon choose the weapon is close to common sense, and for a developer the demands of the front become the specification sheet itself. In exchange, this standard has a narrow span of time. When what the front wants today differs from what will be needed two years from now, no method was put in place for confirming from the record which of the two gets pushed back.

Open up the phrase "units order directly" and inside it sits a points system. Frontline units accumulate points for confirmed strike results, and with those points they order drones and equipment directly from manufacturers on Brave1 Market. It means a unit picks its equipment off a screen without riding the Ministry of Defense's approval chain. Some of the power to decide procurement came down from the top of the chain of command to the bottom.

A method that increases supply according to battlefield results has side effects too. Points accumulate through strikes. A unit assigned to reconnaissance, communications relay, casualty evacuation, or the defense of positions — missions that do not convert into a count of strikes — stands before the same screen holding fewer points. As for documents showing how this structure actually changed the distribution of equipment among units, the public record stops here. The blueprint is public, and the distribution that blueprint produced still cannot be counted from outside.

The Ukrainian government announced that more than 80 percent of enemy targets are destroyed by drones, and analytical reports citing Reuters coverage carry that announcement across unchanged. Here too, the side making the announcement and the side the announcement points at do not come apart. The distance between the sentence that the system got faster and proof that the system worked remains, from the start of this section to its end, uncrossed.

3. Performance Indicators and the Blank Where an External Audit Would Be

To evaluate Brave1, two questions have to be put separately. What did this cluster announce? And who verified that announcement?

Lay out the indicators Brave1 has offered once more. 2,500 companies, more than 5,000 products, more than 500 unmanned aircraft manufacturers. These values are Brave1's own postings. Grants from 329 totaling five million dollars to more than sixty million. A budget allocation of 71.6 million dollars. 150 venture funds. It is an eye-catching list, and every one of these values counts how much gathered and how much went out.

These are input indicators. In a school, they correspond to how many teachers were hired and how many books were bought. Whether the students' grades rose is something other numbers must answer, and the numbers that would answer the following questions are not in the public documents. Of the roughly 600 companies that received grants, how many actually delivered to a unit? What proportion took a grant and produced no product? Of the 5,000 registered products, how many passed testing, how many made it to codification, and how many led to a contract? Was there any difference in battlefield performance between technologies the cluster supported and those it did not?

Venture investors who do not disclose their failure rates are common. It is private money, and private judgment may keep it hidden. But the money Brave1 spends is the national budget. If the state calls itself an angel investor, it must bear a public institution's duties along with an angel investor's freedom. The public documents contain no accounting report or audit-body report independently auditing Brave1's grant disbursements. This blank may be a limit of the document collection, or it may be that no such document yet exists. Which of the two it is, we do not close hastily; we leave standing only the fact that the blank exists.

To gauge the size of that blank, a point of comparison is needed. Within the same Ukraine, in the same wartime, there is a domain equipped with far denser audit machinery: the reconstruction sector, into which international money flows.

The Ukraine Relief, Recovery, Reconstruction and Reform Trust Fund (URTF), led by the World Bank, publishes its results framework as a document. As of 2025 it had raised a cumulative 2.52 billion dollars and disbursed 1.5 billion, and its financial indicators are laid out in terms such as an additional 4.2 billion dollars unlocked on the strength of that support. All approved projects — 100 percent — are to use third-party monitoring, and 100 percent are to have a beneficiary grievance mechanism in place.

Start by unpacking the phrase third-party monitoring. It is a procedure in which a third institution, outside both the side that gave the money and the side that received it, goes to the site, confirms with its own eyes that the work actually happened, and records it in a document. If the paperwork says thirty hospitals were repaired but only twenty actually were, catching that gap is the third party's job. The grievance mechanism is a device pointing the other way. When residents who ought to benefit from a project feel the money leaked somewhere else, a window for filing complaints has been set up in advance. In the URTF, UDA Consulting handles third-party monitoring across the portfolio, visiting sites and recording progress, while logistics and energy recovery projects in areas that are difficult or dangerous to reach are supervised by the United Nations Office for Project Services (UNOPS) as trustee agent.

There are domestic mechanisms as well. Independent audit of public spending falls to the Accounting Chamber and the State Audit Service, and high-level corruption cases are handled by a chain running through the National Anti-Corruption Bureau (NABU), the Specialized Anti-Corruption Prosecutor's Office (SAPO), and the High Anti-Corruption Court. The DREAM platform, which publishes reconstruction project data from budget allocation through procurement and progress rates, lets donors and civil society see the same documents the government sees. Oversight does not hold if the information sits on one side only, and accountability begins with looking at the same screen together.

Civil society has not been sitting on its hands either. In 2025 alone, the Anti-Corruption Action Center (ANTAC) analyzed 1,526 public procurement cases and filed legal challenges against ten procurement procedures in which corruption risk was confirmed. This watch network has in fact changed a course of events. After a scandal broke over inflated prices for goods such as eggs and jackets in Ministry of Defense procurement, the law was amended to return defense procurement to the open electronic procurement platform ProZorro. ProZorro is a system that puts who is buying what at what price straight onto the internet. It was a measure in which the government itself admitted that corruption had grown while that door was kept shut on grounds of wartime secrecy, and while the argument that secrecy is necessary may be correct, secrecy bills you for itself.

Around Brave1, machinery on this scale — the public record stops here. Not the name of a third-party monitoring body, not an Accounting Chamber audit report on grant disbursement, not a civil society document analyzing the cluster's budget; none of it is in the public documents.

The objection that defense technology sits under conditions different from reconstruction projects is legitimate. The moment you reveal which company is making an interceptor drone with what performance, that becomes information handed to the enemy. Reports on the reconstruction sector point to the same dilemma. Donors demand maximum transparency, and the government must keep the maximum secrecy that operations require. The two demands collide head-on.

Colliding does not mean one of them must be discarded. The road DREAM took is the proof. It is tiered access control: restricting access to sensitive location data while publishing totals and progress information. What is being built and where is masked; how much was spent and how far it has come is shown. Carry the same logic over to defense technology and it comes out like this. Even while masking which company is making what, it is possible to publish aggregate figures for how many applications entered grant review, how many passed, and how many of those reached delivery. The specifications of an individual product and the total volume of disbursement are different kinds of information, and as far as can be confirmed, Brave1 did not open even the latter to outside verification.

The same report on reconstruction points to a more painful problem. The places where accountability machinery is weakest are precisely the places where the risk of corruption and misallocation is greatest: the areas adjacent to the front, where oversight capacity is exhausted. This paradox, in which controls loosen exactly where the risk is high, repeats outside reconstruction sites as well. A structure that spends money fast, contracts fast, and sends fast to the front is by definition a structure that cuts verification steps. The moment speed becomes a virtue, every procedure that slows

things down begins to look like an obstruction, and a procedure that has come to look like an obstruction does not survive long.

Brave1's record can be divided into confirmed facts and questions still outside the public record. What has been confirmed from the sources is this. A single door was opened between developers and the military, who had been scattered. State money went into the dangerous early stage, and foreign venture capital followed behind it. A channel running from testing and codification through to direct ordering by units was designed as an institution. A country in the third year of an invasion won a coordinate on the international venture map.

What lies outside the public record is this. How much this system actually shortened procurement time. What the success and failure rates are for the grants the state scattered. How many of the 5,000 registered products reached the front. And who, outside the government, looked into that money.

The nickname "a defense Silicon Valley inside a war" captures the energy of investment and founding well. Only, Silicon Valley's investors lose their own money, while Brave1's investors are the citizens. What fills that difference is audit, and that channel is empty right now. Writing down the missing audit as missing is the best courtesy that can be paid to Brave1 today.

Look a little further into the reconstruction sector's indicators and the shape of the empty column in Brave1's list grows distinct. The URTF's results framework does not record only sums of money. It records that a cumulative 40.7 million services were provided to beneficiaries, that 330 medical facilities were repaired through the HEAL project, that 3,130 public sector personnel were trained for relief work. How much went in and what got fixed, and how much of it, are counted separately. Brave1's published list has no column corresponding to the latter.

The layers of audit run several deep as well. The World Bank does not stop at entrusting on-site verification to outside bodies such as UDA Consulting and the United Nations Office for Project Services; it also keeps an inspection panel that investigates policy violations and an internal audit organization within itself. It is a structure in which the side that gave the money suspects even itself. The Anti-Corruption Action Center issued 339 publications in 2025 and submitted opinions on eleven bills concerning anti-corruption bodies, carrying six of them through. Oversight does not run on good intentions alone. It runs when documents to read, a window to complain through, and legal means to contest are all present together.

Reconstruction money came from abroad, so donors could demand audits, and that is how the condition of attaching third-party monitoring to every approved project came to be attached. Brave1's grants come out of Ukraine's national budget. The explanation that no audit machinery was attached because there is no outside donor to impose conditions grasps the structure of the facts well. And that explanation does not make the problem go away. To say there is no outside donor is to say the owner of that money is the Ukrainian people, and it does not mean there is no one to set conditions; it means the people who would set them are inside the country.

Chapter 8. Unmanned Systems Become a Service Branch, and the DELTA Lineage

On 23 January 2026, a single order appeared in the official news feed of Ukraine's Ministry of Defence. It bore the signature of the new defence minister, Mykhailo Fedorov, and it had nothing to do with buying weapons or moving units. It directed that a drone command-and-control system called Mission Control be brought into operation inside a combat system named DELTA. The signature came on his ninth day as master of the ministry building.

An order creating a new service branch does not, by itself, change anything on the ground. For a sentence on paper to reach the trenches at the front, training and communications and supply have to follow, and months usually sit in between. Yet the story changes once you look at what this document was resting on. Mission Control was not a system raised on empty ground; it is described as a function laid on top of DELTA, which had already been running for several years. DELTA's development and operation had been handled by organisations within the defence ministry's orbit, and long before Fedorov arrived there, DELTA was already serving as the Ukrainian military's map.

Before he became defence minister, two things were moving forward side by side inside the Ukrainian armed forces. One was the rise of the drone from an auxiliary piece of equipment attached to other units into an independent service branch with a name of its own. The other was the work of overlaying what those drones saw with what every other means of surveillance saw, all on a single screen. You could just as well call it building a new hand and gathering the eyes into one. Both currents took root before he arrived, and that is precisely where what he inherited parts company with what he signed himself.

1. From Aerorozvidka to the DELTA Combat System

On a battlefield, information does not arrive from one place. Video shot by a reconnaissance drone, radio calls from ground observers, satellite imagery, tracks caught by radar, tips sent in by residents — all of it pours in at once. The trouble is that these arrive through different channels, in different formats, at different units. When the enemy position known to an artillery battery does not match the one known to the infantry battalion beside it, the same target gets hit twice while another is missed entirely. If there are several maps, there are several wars, and those several wars get in each other's way.

DELTA is a situational-awareness system that gathers these scattered records, layers them onto a single map, and lets many units look at that map at the same time. Ukraine's defence ministry presents DELTA as a combat system used across the defence forces, and describes its function as integrating multiple surveillance sources and unit reports into a real-time picture of the battlefield.

Even real-time information guarantees no accurate judgement if the incoming records are late or wrong. What makes it work is the tedious labour of standardising the channels through which records arrive, settling on one convention for writing coordinates, and deciding in advance who has the right to see what. If the coordinates sent by a drone operator and the coordinates read by an artillery crew do not follow the same rule, then however dazzling the display, that map cannot simply be trusted as it

stands. Most of the work of making a battlefield map is administrative: agreeing on rules and getting people to keep to them.

When the lineage is traced, the name most often given as the starting point is Aerorozvidka. It was a group of civilian engineers and volunteers who came together amid the Donbas war in 2014 and built reconnaissance drones and battlefield information software with their own hands, and the widely accepted account holds that their work was later absorbed into the defence ministry's innovation arm and became the root of DELTA.

That is as far as verification goes. Within the set of documents compared here, no primary source records that early period down to dates and names; the public record stops there. So the workshop of Aerorozvidka and the scene of the first meeting are not reconstructed here. There is no public document telling us who said what on which night. What can be confirmed is only the direction of the lineage. DELTA looks less like a thing born out of a ministry's planning paper than like a tool built by people who felt a need close to the fighting, a tool that travelled upward and became a national system.

Confuse who did what, and the whole lineage bends out of shape. DELTA's development and operation belonged to organisations in the defence ministry's orbit, and Fedorov issuing orders over DELTA is a matter of 2026. Reading DELTA as "the battlefield app the digital minister built" is a common error, and the more favourably a piece treats him, the more often it commits that error.

The moment DELTA drew international notice was news of a test passed. On 17 July 2024, Ukraine's defence ministry announced that DELTA had passed a NATO audit.

What does it mean to say a system passed a NATO audit? For the armies of several countries to fight together, everything from radio frequencies to map coordinate conventions to the data formats of targeting information has to be readable by all sides. If a coordinate sent by one side is interpreted by the other side's system as something else entirely, you get not cooperation but a friendly-fire accident. This compatibility is called interoperability. A NATO audit is the procedure for checking whether a system can exchange information in line with NATO standards, and passing it means, roughly, that DELTA had taken a form that could be slotted into a NATO-style command-and-control picture. For Ukraine, the announcement was technical news and political news at once. It was a declaration that our system speaks the same language as the West.

The achievement and its limits have to be looked at together.

The party making the announcement was Ukraine's defence ministry. A separate verification report issued by NATO is not in the public record. There is no cause to brand a wartime government's announcement false on its face. But a document in which a body reports its own success cannot be weighed the same as a document independently verified by an outside institution. A considerable share of the established facts about DELTA rests on ministry announcements, and that circumstance will not be hidden here. Please do give the attributions at the ends of the sentences a glance. Whose mouth a sentence came out of matters as much here as what it says.

Passing a standard and performing in combat are also separate matters. An audit looks at whether the form is correct. How many brigades use DELTA at the front, how often, and how accurately is not written into an audit report. In automotive terms, it is the equivalent of type approval, which is a different thing from a record of driving rough roads.

Here is what to remember about DELTA's lineage. DELTA is an accumulation that passed through many hands. There is a received account that it began in a volunteer engineering group; defence ministry organisations took over its development and operation; it is presented as a combat system for the defence forces as a whole; and in July 2024 a ministry announcement of a passed NATO audit was attached to it. On top of that accumulation, the new defence minister of 2026 laid his own signature — and only by looking at the lineage first can one avoid either inflating or shrinking the size of that signature.

For a map like DELTA to be of use, there have to be people down below building the machines that send records up to it. The framework in which Ukraine bound that lower layer together is a defence technology cluster called Brave1. Some 2,500 startups and companies belong to the cluster and have registered more than 5,000 products, among them over 500 makers of unmanned aerial vehicles, over 200 makers of unmanned ground vehicles, and over 200 makers of artificial intelligence products. Submitted products are reviewed by representatives of Ukraine's defence forces, who pick out what is genuinely needed at the front and then connect them to field trials and NATO codification.

NATO codification is the procedure of attaching to a piece of equipment the common number and specification data NATO uses, so that other countries' military supply systems recognise it as the same object. It runs in a direction similar to the NATO audit DELTA passed, but it is a different door. One door aligns the format in which information is exchanged; the other aligns the label on the object.

A caution, left here deliberately. Brave1 is not the organisation that built DELTA. DELTA's development and operation were handled by defence ministry organisations, and within the set of documents compared here the public record stops short of showing how the machines of Brave1-nurtured companies feed records onto the map called DELTA, or what institutional paperwork ties the two axes together. What can be attached to the lineage is the fact that the two currents grew side by side, and no more than that can be said with the documents at hand.

2. The Founding of the Unmanned Systems Forces and the Institutionalisation of the Drone

If DELTA was the work of gathering scattered eyes into one, then over the same period the Ukrainian military was reorganising the very hand that holds the drone.

Militaries have a concept called the service branch. It means a large military category with its own independent structure, chain of command, budget and doctrine — like the army, the navy, the air force. For a weapon to become a service branch means it becomes an organisation that recruits, trains and writes doctrine under its own name. It gets its own line in the budget table, its own promotion ladder, and a commander who answers for failure. Ukraine gave the drone that standing, and the branch that resulted is named the Unmanned Systems Forces (USF).

The founding date is written differently from source to source. One report says the Ukrainian government officially established the Unmanned Systems Forces in early 2024. Another writes that as of 16 September 2024 the Unmanned Systems Forces were separated out and elevated to an independent branch of the Ukrainian armed forces. It looks like the gap between a declaration and the completion of the structure, but rather than nailing it to one date, both records are set down side by side. A new branch is not born the way a birthday cake is cut, and reading it as a process spanning the whole of 2024 fits the public documents better.

There is a question here that sits outside the public record. The founding of the Unmanned Systems Forces happened long before Fedorov became defence minister. He took over the ministry in January 2026. A fair number of accounts, in Ukraine and abroad, transcribe the decision to make the drone a service branch into his column of achievements, and the documents do not support that. This is the temptation to guard against most carefully when writing a life. The temptation, that is, to arrange things that were already doing their work before the protagonist arrived as though he had brought them with him.

The standing of the Unmanned Systems Forces shows up in the organisation chart. The branch was placed on equal footing with the Special Operations Forces and the Territorial Defence Forces. Colonel Vadym Sukharevskyi was appointed its first commander, and in becoming commander of the Unmanned Systems Forces he simultaneously held the post of deputy to the commander-in-chief, Oleksandr Syrskyi.

For a single commander to hold a post directly beneath the commander-in-chief means moving the drone question from the bottom of the general staff's agenda list into the middle of the command group. This is generally how something becomes important inside an organisation. The seating changes before the slogans do. The moment it is settled who sits where in the meeting room and who can report directly to the commander-in-chief, that field actually acquires power. An organisation chart is a document that shows, without saying a word, what an organisation holds to be important.

Once a branch exists, the shape of its units changes. In 2025, the existing 14th Regiment was expanded and reorganised into the 1st Center under the Unmanned Systems Forces. Going from regiment to center was a step far beyond swapping a sign. Borys, an officer connected with the unit, explained it as a deliberate strategic choice and put it this way: "Our goal is not to fight longer, but to fight smarter. Through precision, structure, and engineering thinking, we can exhaust the enemy faster than the enemy can adapt."

A regiment fights. A center fights while also experimenting, teaching and revising doctrine. According to the same report, the 1st Center was designed as an integrated hub binding combat operations together with experimentation, training and doctrinal improvement, and given the role of a channel through which inventions at the front line pass into practice the whole branch can use. Suppose some battalion works out a trick for evading enemy jamming. If that trick stays inside the battalion's radio chatter, it never becomes an asset of the army. The center is the organisation that turns it into a document, folds it into a training course, and carries it to the unit next door — and knowledge from the front spreads only when someone is there to carry it.

The same report states that the 1st Center produces 80 to 90 per cent of the drones it uses in operations inside Ukraine itself, and possesses the ability to strike targets as deep as 1,000 km into Russian territory. These figures rest on statements from the unit and people connected to it, and within the accessible documents there is no independent cross-verification. The numbers are carried over but not confirmed. A unit's own wartime tally, even when it is true, cannot be filed in the same column as a verified fact.

The role of drone units themselves changed in this period as well. One study assesses that unmanned systems units have moved beyond their old auxiliary reconnaissance role and evolved into multidomain combat enablers spanning air, ground and sea, becoming a structural element of modern combined-arms warfare. The phrasing is heavy, so let it be unpacked. The drone of the past was an eye that saw for the infantry what the infantry could not see. The drone of today is an eye and a hand both, and it no longer stays only in the sky.

Change at sea is often cited as the proof. Across 2024 and 2025 the Ukrainian military reached the point of managing dozens of naval drone boats with differing functions simultaneously. A naval drone boat is a small vessel that carries no crew and is steered remotely. By this period, naval drone operations had evolved beyond suicide attacks that ram a single target into multi-axis strikes binding together unmanned aircraft, underwater drones, cruise missiles and electronic warfare capability. There are recorded cases of turrets or small-calibre missiles mounted on the boats, and even of a boat used as a launch platform for a counter-drone system belonging to the Special Operations Forces.

It is a structure in which a drone carries a drone out to catch a drone. Combinations like this do not come together on an idea alone. It has to be settled in advance which unit drives the boat, which unit flies the drone riding on it, and whose judgement prevails when communications drop. The substance of saying a branch has been created lies in this: it has been settled who is responsible for designing such combinations, and only once there is someone responsible does a single success harden into a repeatable operation.

The assessment that drones have become the dominant feature of modern war is repeated by military research institutions outside Ukraine as well. It is a diagnosis that survives even after the Ukrainian government's own announcements are stripped away, and its foundation is comparatively thick.

But institutionalisation does not amount to victory. The warnings the cited report leaves behind are set down here as they stand.

One is organisational drift. The report on the Unmanned Systems Forces names institutional drift as the branch's great worry heading into 2026, and states flatly that the 1st Center must not become cut off from the reality of combat. The moment an innovating unit becomes an institution, paperwork and meetings multiply, and the trap of losing the feel of the front opens up. The story of yesterday's insurgents becoming today's bureaucrats is common enough outside the military too.

The other is a diagnosis of what is lacking. The same report defines their immediate task as transformation into an expanded command capable of producing sustained strategic effect across the

whole battlefield, and leaves technological shortfalls and the generation of sortie capacity off that list. The conditions it names are command and control, battle damage assessment, and the capacity for continuous experimentation. Battle damage assessment is the procedure of confirming, after a strike, what was actually destroyed and how much, and feeding that into the next decision. The centre of gravity has shifted from the problem of building many drones to the problem of commanding the information and the strikes that drones generate — and the gap in which DELTA and Mission Control stand is exactly that role of command and control, battle damage assessment, and experimentation.

The equipment the new branch would use comes from private companies and the state procurement system. On 28 April 2025 Ukraine opened an online marketplace called Brave1 Market. It was a channel for getting things like short-range electronic warfare gear, interceptor drones that stop enemy drones, AI-equipped drones and fibre-optic drones to the front quickly. A fibre-optic drone exchanges signals along a strand of glass as fine as a hair, unspooled behind it instead of using radio waves. Because the line is physically connected, control does not drop even when the enemy suppresses the radio spectrum.

This is how the marketplace runs. When a front-line unit strikes the enemy and certifies the moment with video, it receives combat points according to coefficients the government has set in advance. Rather than waiting on approval papers from the ministry or the general staff, the unit uses those points to order directly from a manufacturer the drone in the specification it needs right now. Once a contract is struck, the ministry pays the manufacturer in cash.

In this process, the military's requirements and companies' interests collide. The reason the documents give for founding the Unmanned Systems Forces was a demand to pull the operational deployment of scattered drone units together in one place. The marketplace, by contrast, pushes purchasing authority down to the units. The public record stops short of any document clarifying how the force pulling upward and the force releasing downward are reconciled, or how far the branch headquarters involves itself in each unit's orders. Who sets and revises the coefficients that decide how many points a given target is worth, and whether a unit can contest a certification ruling, are likewise where the public record stops.

Money from outside settled into place in this period as well. On 22 July 2025, Ukraine and the European Union launched a defence technology alliance worth 100 million euros. By the EU's account, BraveTech EU, which is bound up with this alliance, is a scheme to tie the European Defence Fund, the EU Defence Innovation Scheme and Brave1 into a single framework for joint development, testing and deployment, its stated rationale being to carry the knowledge Ukraine has won on the battlefield back into Europe. That the announcing body is the European Commission is noted here.

3. Mission Control, AI Targeting, and the Joining of Field Feedback

Suppose the drones of several units are aloft over one stretch of sky at once. While A Battalion's scout aircraft finds a target and reports it, B Brigade's strike drone flies toward the same target. C Unit, knowing nothing of this, sends its own drone up into the same airspace. There is one target but three assets are spent on it, the airspace tangles, and friendly electronic warfare gear ends up suppressing

friendly drones' communications along with everything else.

Back when drones were scarce, this congestion did not exist. The more drones there are, the cheaper they get, and the more every brigade runs a team of its own, the worse the congestion — and the problem created by success comes back as a new burden. Command and control is the function of sorting out, in one place, who does what, when and where, and Mission Control, which the order Fedorov signed on 23 January 2026 directed into operation, is a design for doing that sorting on top of the existing map called DELTA. Rather than drawing yet another map, it lays a layer onto the map already there.

There are not many public documents on this. On Mission Control, the public documentation amounts to a single announcement from Ukraine's defence ministry. The fact that the order was signed, the explanation that the system handles drone command and control inside DELTA, and the signing date of 23 January 2026 — that is the extent of what can be confirmed. How many units it was actually deployed to, how much target duplication fell where it was deployed, and how combat outcomes changed as a result: the public record stops there. A signature on the ninth day in office is large as a symbol, but a symbol cannot be transcribed as a result. The reason that signature opens this chapter is that it shows where the new minister laid his hand.

In this same period DELTA also came down into the individual soldier's hand. On 10 March 2026, Ukraine's defence ministry announced that soldiers would receive aerial threat alerts through the DELTA Mobile app. As of the announcement this was a stated plan, and how far the actual rollout went is where the public record stops. The direction alone is unmistakable. Track information that used to appear on the big screen on a command post wall was to be pushed onto personal devices in trenches and in moving vehicles.

In the military, one more thing hangs on this. Communications at the front drop often, and the enemy's electronic warfare hunts for signals. How well a design that pushes information down to personal devices holds up in that environment is not something the announcement answers.

The ministry's own announcements record both the achievements and the tasks left over. On 2 February 2026, the ministry published a summary of which training courses soldiers were taking in the Army+ app. That drone-related courses were out in front while DELTA remained an outstanding problem was both the headline and the substance of that announcement.

Building a system and getting people to use it are different jobs. A combat system that had passed a NATO audit, even after the branch was formally established, was still lagging on the study lists of the very soldiers who were supposed to handle it every day. There was a distance between the feature list in the documents introducing DELTA and the screen a squad leader at the front actually switches on and uses. It is worth recording that the body which disclosed this fact was Ukraine's defence ministry itself. An announcement in which a body writes down its own weakness is rare among the documents of a wartime government.

Closing that distance was the task Fedorov faced at the ministry. With a civilian service, if usage is low you fix the screen and buy advertising. In an army, low adoption of a system is a problem in which

orders, training, communications conditions and soldiers' trust are all tangled together at once. A squad leader who does not switch the app on usually has a reason. The battery is low, or there is no signal, or the few seconds spent looking at a screen are dangerous, or there is a memory of trusting that screen once and coming to grief. Usage statistics do not tell you the reason.

What can be said about AI targeting is narrow. There is analysis holding that a trend toward autonomy is appearing on Ukraine's battlefields, in which drones find their way to targets on their own even where satellite navigation signals are cut, and multiple aircraft cooperate in swarms. An environment with satellite navigation cut means a state in which the enemy has suppressed the spectrum so that GPS coordinates cannot be received. That the battlefield records DELTA accumulates become material for such automation is also, structurally, an intelligible claim.

But on which algorithms handle which targets at what degree of autonomy, and at what stage human approval intervenes, there is no confirmed primary document. The question of who bears responsibility when a target identification is wrong is likewise left open. Where documents are absent, writing down that the documents are absent is more honest to the reader than filling the space with imagination.

The organisation, the equipment and the information system of the unmanned forces move interlocked with one another. DELTA was a tool that climbed from the bottom upward. There is a received account that it began in the hands of volunteers and engineers; defence ministry organisations took over its development and operation; and in July 2024 a ministry announcement of a passed NATO audit was attached to it. Unmanned systems rose from equipment to a service branch. Across 2024 the Unmanned Systems Forces were established, their commander doubled as deputy to the commander-in-chief, and in 2025 the 14th Regiment was reorganised into the 1st Center, creating an organisation that learns while it fights. Both these currents had already grown before Fedorov became defence minister.

What he did was sign a document laying a command-and-control layer on top of them. Whether that signature changed the front cannot be said from the documents of the first half of 2026 alone. What is clear is that the system he inherited already had problems bearing its own name. The ministry's own diagnosis that DELTA was lagging on soldiers' training lists is one; the report's diagnosis naming command and control and battle damage assessment as the Unmanned Systems Forces' next task is the other. The two point to the same place. The tools are there; the way to use the tools together has not yet been fully settled.

Making the drone a service branch takes one order. Making that branch actually look at one map and move on one judgement takes many orders and far more time than that. The document signed on 23 January 2026 sat at the starting point of that time.

In the story of artificial intelligence handling targets, the one company the documents actually name is Swarmer. This company's Styx is a swarming technology that lets up to 25 drones keep their positions aligned with one another and move together even where satellite navigation signals are cut. The company's path to grants and investment was described in Chapter 7, on the Brave1 industrial

ecosystem. What matters here is the fact that there is no evidence that technology is linked to DELTA or Mission Control.

The connection to Mission Control is left open as well. There is analysis holding that a trend is appearing on the battlefield in which drones find their targets on their own where satellite navigation is blocked and multiple aircraft move together in swarms. But on whether Swarmer's swarming technology is in fact linked to DELTA or Mission Control, and at what stage a human confirms a target the swarm has chosen, the public record stops. The distance between the picture one infers from structure and the picture confirmed by documents is left here as it is, uncloseed.

Chapter 9. From Digital Minister to Defence Minister

1. January 2026: Zelensky's Nomination and the Parliamentary Vote

In the legislative database of Ukraine's Verkhovna Rada there sits a single document dated 14 January 2026. The Verkhovna Rada is Ukraine's parliament. The document is a resolution, numbered 4756-IX, and its title reads: "On the Appointment of Mykhailo Albertovych Fedorov as Minister of Defence of Ukraine." Its contents are brief. The president made a nomination, parliament voted, the appointment was confirmed. A record of procedure, and nothing more.

The official trace left by the moment when the man we have been following moved into the Ministry of Defence is one page long. The social media post pleading for satellite internet is not on that page. Neither is the assembly line of a drone factory, nor the demonstration stand at a startup exhibition. What a state leaves behind when it vests a person with authority is a single sheet of paper bearing a number, and whoever writes a life must begin from that sheet without dressing up what the paper does not say as though the paper had said it.

In Ukraine the president cannot appoint a defence minister alone. The president puts a candidate before parliament, and parliament must approve by vote before the appointment is complete. So ministerial appointments always leave two records behind: the nomination on the president's side and the resolution on parliament's side. In Fedorov's case those two records came a single day apart.

The process began with a public nomination by the president. On 13 January 2026, President Volodymyr Zelensky posted an address on the official website of the Office of the President. It was titled "Today We Have Begun a Genuine Reboot," with a subtitle describing internal changes meant to make Ukraine more resilient. In form it was a speech, but line after line was filled with names and roles, which made it closer to a personnel announcement.

The address laid out a plan to rework the defence establishment. Kyrylo Budanov, who had led the military intelligence directorate, would take over as head of the Office of the President. The military intelligence directorate belongs to the Ministry of Defence and exists to uncover the enemy's movements; in Ukraine it is commonly known by the abbreviation HUR. The post Budanov vacated would pass to Oleh Ivashchenko, who had been running the foreign intelligence service. The address also announced changes to the command structure and leadership of the border guard service, along with a promise to send parliament a bill overhauling the State Bureau of Investigation, the body that investigates crimes by senior officials and law enforcement agencies. It further mentioned a measure putting a deputy head of the Office of the President with combat command experience in direct contact with the brigades.

A restructuring of the Ministry of Defence was part of that plan. The president said he would change the ministry's "format of work," and disclosed that he had offered the post of defence minister to Mykhailo Fedorov. He added that the outgoing defence minister, Denys Shmyhal, would remain on the team and take on other state duties.

This address is a document the Office of the President issued about itself. A document in which a government explains its own personnel decisions does confirm the facts of those decisions. Who was nominated, when, and to which post is settled by this text. But the same document does not confirm the judgment attached to those decisions. The word "reboot" in the address is the government's own framing, and it sits on a different level from the diagnosis of an independent body. No government ever calls its own personnel shake-up damage control; it always calls it a leap forward. So the two levels must be read apart. Dates, names, and titles are fixed by the document; why these appointments were necessary remains a matter of interpretation.

The next day, 14 January, parliament voted. The Ministry of Defence of Ukraine issued an English-language press release the same day announcing that Fedorov had been appointed the new defence minister. The vote carried with 277 in favour.

To say precisely what the number 277 means, one must first say what it does not mean. The document consulted reports only that there were 277 votes in favour. How many voted against, how many abstained, how many deputies took no part in the vote at all — the public record stops here. So no verdict of "overwhelming support" or "passed by a hair" can be pinned to this number on its own. What is confirmed is that the appointment carried with 277 votes in favour, and a number only begins to speak once the denominator and the context around it are confirmed alongside it.

There is one more blank in the record. Before Fedorov could become defence minister, he had to leave the post of First Deputy Prime Minister and Minister of Digital Transformation. That resignation, or dismissal, would also have passed through a parliamentary procedure. But the primary document obtained — the appointment resolution — covers only the appointment to the Ministry of Defence. A primary document means an original record left by the parties to the event itself: parliament's resolution, the presidential address, a ministry's press release. No separate primary document giving the date a resignation letter was filed or the vote count on a dismissal was available for comparison. Secondary summaries in the public domain carry sentences about a resignation letter submitted in early January and a dismissal carried by 270 votes. They are plausible, and they may well be true. But numbers whose sources could not be checked were kept out of this text. Once a number is set in type, it hardens into something that looks like a verified fact and travels on into the next book and the article after that.

One sentence Fedorov spoke in the chamber was carried by several outlets. Before Russia's full-scale invasion, he said in substance, there had not been a single private company in Ukraine building missiles or robots; now there were dozens.

In his inaugural remarks Fedorov pointed to the work he had done at the Ministry of Digital Transformation as the foundation for defence reform. He had not risen through the corridors of the Ministry of Defence, and he had never worn a uniform. What he could set before the deputies was the circuitry he had built behind the defence industry over the past several years. The circuit that turned citizens' donations into drone contracts; the circuit that carried a startup's prototype onto the army's test range; the circuit that cut the waiting time for certification and contracts from months to weeks. Holding the products of the circuitry we have already watched him build, he now opened the door of

the ministry that buys those products.

Foreign journalists and analysts read the appointment in various ways. A policy analysis podcast released on 28 January 2026 characterised the reshuffle as the launch of a "war cabinet." Its panellists argued that authority had been concentrated in the hands of the head of the Office of the President, Andriy Yermak, and that information reaching the president had been filtered; they read the elevation of Budanov and Fedorov as a dispersal of power.

It is a persuasive reading, but it must be kept separate from confirmed fact. Those podcast panellists cannot possibly have had access to the minutes of the Office of the President. Why the president chose an information technology official in his mid-thirties as a wartime defence minister, and how the internal deliberations around that choice unfolded — no primary document showing this lies within the range of what was obtained. Zelensky's reasoning, the objections or endorsements of his advisers, what Fedorov weighed when the offer came. The more a reader wants to know about a given part of the story, the thinner the ground beneath it tends to be, and the only way to avoid filling that thin ground with imagination is to leave the blanks blank.

This much can be established. On 13 January 2026 the president publicly announced that he would change the Ministry of Defence's format of work and named Fedorov; on 14 January parliament adopted resolution 4756-IX with 277 votes in favour; and the Ministry of Defence announced it officially the same day.

Other items in the address also reveal the character of the reshuffle. The president said that Pavlo Palisa, a deputy head of the Office of the President with a record of combat command, would communicate directly with the brigades, and that the military education system would be reworked to match the realities of the battlefield. As for the departing defence minister Denys Shmyhal, he explained that Shmyhal would stay on the team because he had worked systematically — ordering, among other things, the production of more than a thousand interceptor drones a day. That assessment and that number are the president's own words about his own government, and they could not be checked against separate production statistics.

The stories circulating outside about the reasons for the reshuffle are far more specific. The panellists on that late-January podcast claimed that Andriy Yermak, the head of the Office of the President, not only held the levers of power but filtered the information that reached the president himself, and that because bad news was blocked, the true state of recruitment and the energy crisis became known only belatedly. The same broadcast said that only after his meeting with President Trump in Florida did Zelensky face the gravity of the situation. There was also a line about corruption cases coinciding with attempts to undermine the anti-corruption agencies.

Every one of these accounts presumes knowledge of what happened inside the Office of the President. Yet there is no basis for saying that the people on the broadcast had any channel for verifying that interior. Even the name "war cabinet" is not one the government gave; it is one the analysts gave. The primary documents obtained are only the president's address, parliament's resolution, and the Ministry of Defence's press release, and none of them contains a roll call showing

how the factions moved in the vote.

2. A Ministry at War, Inherited by a Thirty-Five-Year-Old

Articles at the time of his appointment gave his age variously as thirty-four and thirty-five. Some called him thirty-four; some sources called him thirty-five. Yonhap News, in an article dated 21 January 2026, described him as the "34-year-old Ukrainian defence minister," while a piece published in an English-language outlet in the spring of 2026, discussing the youth of Ukraine's leadership, introduced him as thirty-five. Neither is wrong. Fedorov's birthday is 21 January.

It should be stated, though, that this date of birth does not rest on solid ground. Among the documents consulted, the only one specifying 21 January 1991 as his birth date is the Chinese-language Wikipedia entry. Wikipedia is a tertiary source. That means a summary compiled by citing other sources, and on items such as a person's date of birth, errors from the editing process may survive. So when speaking of his age, two levels must be kept distinct. That the appointment date was 14 January 2026 is a fact fixed by a parliamentary resolution; that he was thirty-four years old on that day is a calculation resting on a tertiary public source.

The arithmetic itself is easy. If he was born on 21 January 1991, then on 14 January 2026 he was thirty-four, a week short of his thirty-fifth birthday, and turned thirty-five a week later on 21 January. The Yonhap article ran on that very 21 January, but it gave his age as thirty-four as of the appointment. The spring source that said thirty-five is correct for the same reason. Where the numbers differ, the difference is one of reference date, and so this book gives him as thirty-four at the time of appointment and thirty-five from just afterward.

The reason for pinning down the age precisely is that his youth is so often the emphasis in coverage of him. In writing about Fedorov, the age always arrives first, as a modifier. The twenty-eight-year-old youngest minister; the thirty-four-year-old wartime defence minister. Age makes a story fast, but it does not make it accurate. The moment age comes first, the reader reads the man's youth rather than the man's competence, and slides past as though that youth were itself the proof of reform. What matters more than his age is the organisation and the problems he took over at the Ministry of Defence.

In wartime Ukraine, the Ministry of Defence is where the money flows heaviest. It buys weapons, buys shells, buys food and clothing, and pays the salaries of hundreds of thousands. This business of a government buying goods and services is called procurement. Where money flows heavily, procurement problems always follow. Contracts with padded prices, supplies never delivered, warehouses that exist only on paper — these are the shadows that have hung over this ministry for a long time.

That analysis podcast of January 2026 depicted the Ministry of Defence as an institution wrecked by procurement corruption and inefficiency, and set out Fedorov's mission in two parts: one, to put procurement and internal management right; two, to shift the conduct of the war onto a technological footing. This diagnosis is the view of outside analysts. It carries a different weight from an audit body's conclusion or a prosecutor's indictment. Still, given that the president himself singled out the ministry's

format of work for change in his address, it is at least confirmed that inside the government, too, this ministry was counted among the things needing repair. When a government's self-diagnosis and outside criticism point the same way, the likelihood that the direction is real goes up — but between a raised likelihood and an established fact there is still a distance.

Some accounts of his earlier career are simply misreported. Sentences suggesting that Fedorov created the drone forces upon becoming defence minister turn up now and then, but the order of events is reversed.

The Unmanned Systems Forces (USF) are a separate branch of Ukraine's armed forces. A branch means one of the large military divisions such as the army, the navy, or the air force. So the units handling drones were formally elevated into a branch of that kind. Records of when it was founded differ from source to source. One research report puts its elevation to an independent branch in September 2024 and records that its first commander concurrently served as a deputy to the commander-in-chief. Another source records its founding in early 2024. Rather than choose between them, this book sets the two records side by side and shows the discrepancy as a discrepancy.

Whichever date one takes, the conclusion is the same. These events precede his appointment as defence minister by more than a year. As we saw earlier, the DELTA battlefield system was likewise not a product his ministry built. Its lineage runs back to Aerorozvidka, and the centre of its development and operation lay within the defence establishment.

During his time as Minister of Digital Transformation, he handled drone purchasing and production and the linking of startups to the military. Creating units and appointing commanders lay outside his remit, and the authority to change the army's order of battle was not in his hands. By the time he moved to the Ministry of Defence, the procurement system he had helped shape was already in operation. Reverse this order and two things happen at once: his achievements grow larger than they were, and the share of reform built up over years inside the military is erased. Once a biography starts erasing institutions in order to enlarge a man, it stops being a biography and becomes a promotional pamphlet.

On the direction he took immediately after taking office, there is one Korean-language report. Yonhap News, in its article of 21 January 2026, reported that Fedorov had set about replacing Chinese-made drones — over which security concerns had been raised — with Ukrainian-built airframes, and had ordered the development of artificial intelligence–based weapons and defence systems drawing on the battlefield data accumulated so far. For Korean readers this is a rare window. But the origin of the information is the Ukrainian government and local reporting. It is an article relaying a Ukrainian announcement at one remove, which means the distance between the announced direction and the results actually executed can only be narrowed by setting the procurement ledgers and battlefield outcomes side by side.

There are several items left deliberately blank. Secondary sources repeat sentences claiming that in various interviews after taking office, Fedorov cited internal audit findings and gave figures for the ministry's budget deficit, the number of men who failed to report for conscription, and the number of

troops absent without leave. A provocative figure said to be a target for Russian casualties is quoted alongside them. Those numbers were kept out of this text.

There are two reasons. One is that the original wording and dates of those remarks could not be checked against primary documents. Numbers passed along through video summaries easily shift in unit and in baseline as they travel. The other is that even if the remarks are genuine, they are a new minister assessing his own ministry's past, and that has a different standing from figures confirmed by an independent audit body. The larger a predecessor's failures are painted, the larger a successor's reform appears, and a new minister's opening remarks are born inside that structure. This is exactly the kind of place where the principle of not weighing government announcements the same as independent verification must apply, and until the ground is firm it is better to leave the space empty.

Written only within the confirmed range, what he inherited was this: a ministry handling a large share of the national budget while losing trust over procurement problems; an unmanned force already institutionalised as an independent branch and running; an organisation the president publicly singled out for a change of format; and a war that had by then been going on for nearly four years since the full-scale invasion of February 2022. What lay before him was not a blank page but a manuscript already half written, and some of that manuscript he had written himself, from the outside.

The weight of saying the Unmanned Systems Forces became an independent branch has to be measured in institutional terms. According to one research report, the force gained a standing equal to that of the Special Operations Forces and the Territorial Defence Forces. Its first commander, Vadym Sukharevskyi, concurrently served as a deputy to Commander-in-Chief Oleksandr Syrskyi. Creating a branch, seating a commander, and fitting it into the chain of command are powers belonging to the military leadership and the president. A minister of digital transformation had no such powers.

On the ministry's size, too, what is confirmed and what lies outside the public record diverge. The late-January podcast panellists said the Ministry of Defence handles half of Ukraine's state funds. That is a figure that could not be checked against budget documents, so it was left out of the main text as it stands. What the president's address and outside analysis both point to, however, is at least the direction: that this ministry is where the country's money gathers in bulk.

The policy of replacing Chinese-made drones with Ukrainian ones also needs unpacking. A great many of the airframes widely used at the front were originally commercial drones sold by Chinese companies for hobby and photography use. They were cheap and easy to obtain, but the worry followed them that the companies that made the parts and software could look in on an airframe's position or its control signals. There is also the problem that if the supply of parts is cut off, the whole force wobbles. The new minister's declaration that he would switch to Ukrainian airframes is an answer to that worry. But the policy comes to us as reporting that relayed a Ukrainian announcement, and how much of the replacement actually took place must be confirmed in the procurement ledgers.

3. Can the Ministry of Digital Transformation's Success Survive Without Its Founder?

On 29 August 2019, at twenty-eight, Fedorov became Minister of Digital Transformation. He held the post for more than six years and four months, until his move to the Ministry of Defence in January 2026, becoming one of the longest-serving members of Ukraine's cabinet. In that time the Diia app his ministry built became a state service used by more than 23 million Ukrainians.

Whether the existing programmes have been run the same way since he left the Ministry of Digital Transformation — here, too, the public record stops. Were the circuits of Diia, Brave1, and drone procurement institutions, or were they one man and the team he brought with him?

A government programme can be considered to have settled into an institution only if it continues after the person in charge changes. Successes inside a government are made in one of two ways. One is carved into law, budget, and organisational charts, so that it keeps turning when the officeholder changes. The other is driven through at speed by a small group with the power to route around the rules. For the first few years the two are outwardly indistinguishable. The app ships, the contracts are signed, the indicators climb. The difference always shows up later, after the people have gone.

As we have seen, a considerable share of the reason Ukraine's digital administration was fast lay in the second way. Quick decisions, a shortened chain of approvals, close proximity to the Office of the President. That was the force that saved the state's data in the first year of the war and rewrote the rules of drone procurement in a matter of months. When a founder leaves an organisation like that, what remains is either an institution hardened into regulation or the empty shell of a role whose person has vanished.

The present public record yields no answer. Among the public documents consulted there is no primary source confirming who succeeded Fedorov as Minister of Digital Transformation or how that person ran the ministry. There are no independent statistics showing how Diia's usage figures moved after his departure. There is no external audit document verifying whether Brave1's evaluations and contracts turn at the same speed in his absence. Fill groundless space with conjecture and you get plausible sentences; it is precisely such sentences that bring biographies down. So only the shape of the question is set here, precisely. The answer belongs to someone else, working from other sources, after the cut-off date of 13 July 2026.

The fact that the man himself moved is a clue of its own. The things Fedorov said he would do at the Ministry of Defence lie on the same line as the work he had done at the Ministry of Digital Transformation. Measuring results with data, treating procurement like an online marketplace, linking startups directly to the military. What he held up in the chamber as his own record was likewise the number of private companies building missiles and robots. If the method crosses from one ministry to another following the man, that is also evidence the method was attached to the man rather than the organisation. Conversely, if the Ministry of Digital Transformation keeps turning without him, then his six years were six years spent successfully making himself replaceable. Both possibilities are still open, and to lean the writing one way or the other now would be a matter of taste, not of evidence.

The political calendar overlaps this question too. That analysis podcast of late January 2026 described Fedorov's political capital this way: his name has not appeared in a corruption scandal, he is not entangled with the new oligarchs, and public trust in him is high. The same panellists identified him and Budanov as potential successors who could aim for the post-Zelensky era, and judged that sending such a figure into a ministry as prone to corruption as Defence was a risky gamble from the president's point of view. An English-language piece published in the spring of 2026 also introduces him as a highly regarded defence minister. But that outlet is a platform closer in character to investment promotion and external publicity for Ukraine. Favourable sentences must not be read as independent assessment.

These assessments are political analysis and impression, and cannot be placed on the same footing as verified fact. Yet the structure the analysis points to is worth noting. A man who made a reputation for cleanliness into political capital has taken charge of the ministry where, in Ukraine, money and suspicion gather together. Whether that reputation will withstand the Ministry of Defence's procurement ledgers and survive, or be burned up there, is too early to judge on the evidence available as of 13 July 2026. Writing that a judgment cannot be made is also part of a biography's work.

Looking at the confirmed facts: at the moment he changed roles, two powers — Ukraine's digital state project and its national defence — met on one man's résumé. The man who built Diia, who wired the circuits of drone procurement, who launched Brave1, is now the minister of the ministry that buys all of it. There are rules he made from the outside, there are companies that grew up on those rules, and now he stands on the side that signs contracts with those companies. It also means he has come close to the place where a reformer grades the results of his own reform. Whether to see this as reform completed or as power concentrated is disputed within Ukraine as well, and to relay that argument honestly one must first establish who is doing the criticising, before the content of the criticism.

Resolution 4756-IX of 14 January 2026 is a short document. Behind that short document lie six and a half years of one man, beginning with a smartphone app and passing through satellite internet, crowdfunding, and drone factories to arrive at the Ministry of Defence building. Whether he can hold the same speed at the ministry, though — here, too, the public record stops. That technology made the government fast has been confirmed. Whether that speed can be sustained inside an organisation as heavy as national defence, and if so at what cost, can only be answered once more evidence has accumulated.

The test of whether something has survived as an institution is not especially mysterious. It is whether it was carved into law, budget, and the organisational chart. If Brave1's evaluation criteria and contracting procedures have hardened into regulation, the same speed should come out no matter who the minister is. If they were attached only to a person, the approval chain grows long again. The documents needed for that determination are the successor minister's operating records, Diia's usage statistics, and the results of an external audit of Brave1's contracts — and none of the three lies within the range obtained.

The role he has crossed into is also one where interests collide. The man who made the rules from outside now stands on the side that signs contracts with the companies that grew up under those rules. What checks a structure like this is not a minister's conscience but audit bodies and anti-corruption agencies. And a claim that there had been attempts to undermine those very anti-corruption agencies came out of the late-January podcast. Whether that claim is true could not be confirmed. If it is, the problem of a man grading his own reform grows larger still.

Assessments of him carry different weight depending on their origin. The sentence saying he is clean and highly trusted comes from the panellists on a policy podcast. The description of him as a highly regarded defence minister is a contributed piece in a publication closer to investment promotion and external publicity for Ukraine. The Korean-language report on his direction just after taking office relays a Ukrainian government announcement at one remove. All three are worth reading, and none of the three is an independent audit. The answer to whether his six and a half years were an institution or a man will come not from these three kinds of writing but from the ledgers of the Ministry of Digital Transformation without him and the Ministry of Defence with him.

Chapter 10. An Army Commanded by Data and AI

1. The Circuit of Strike Points, Equipment Orders, and Procurement Data

On 26 January 2026, Ukraine's Ministry of Defense announced that over the course of 2025 its forces had struck roughly 820,000 Russian targets. The figure came from Minister Mykhailo Fedorov and was the ministry's own tally, calculated on the basis of a points system that the ministry itself operates.

To understand the number, one has to look first at how it is counted. The system is called the Army of Drones Bonus, and inside Ukraine people usually call it e-points. When a unit hits enemy equipment or a fortified position, a drone films the moment, and the unit uploads that footage as evidence. Results confirmed on video are assigned a score, and the score accumulates in the unit's account. The unit then takes those points into a state-run online marketplace, picks the drones and equipment it actually wants to use, and the state pays the manufacturer.

A soldier's record of destroying the enemy is converted into purchasing power over the weapon that soldier will hold next. In an army where the people who buy weapons and the people who use them had long gone without ever meeting one another, this system is an attempt to force the two together. The method Fedorov repeated during his years as minister of digital transformation shows through again: turn behavior into data, then turn that data into the criterion by which money and matériel are distributed.

Once points become orders, orders leave a procurement record behind. According to a ministry announcement on 11 March 2026, combat brigades received 500,000 items — drones and ground robotic systems among them — through DOT-Chain Defence, the digital procurement channel run by the rear-services procurement agency. This too is the ministry's own tally. Ground robotic systems are unmanned vehicles that travel over land on wheels or tracks, used to drag out the wounded or haul ammunition. On the same day, the ministry announced that it had contracted for multirotor drones on a record scale. A multirotor is an aircraft that flies on several propellers; the four-bladed drone familiar from photographs belongs to this family.

That the two announcements came on the same day does not look like coincidence. One concerns what the front took, and how much of it. The other concerns what the state newly bought, and how much. The first number holds up the second. What a unit chooses becomes a demand signal, and that signal becomes the basis of the next contract. It is the market principle that goods which sell well get produced in greater quantity, transplanted into the army's procurement procedures; what Fedorov's ministry calls the data cycle is a pair of arrows pointing in opposite directions — performance data rising from the front to the rear, matériel descending from the rear to the front.

Mission Control is the attempt to add the axes of time and people to this circuit. On 23 January 2026, Fedorov signed the order launching this drone command-and-control system within the DELTA combat digital ecosystem, declaring that every drone operation would be bound into a single digital system. The ambit the minister described in the ministry's announcement is wide. Which mission was carried

out at what intensity, what each crew did, how long a particular individual stayed at the very front, how many logistics operations moved on that individual's behalf — all of it to be read as data.

This description is the minister's own account and a plan stated at the moment of launch. No document exists in the public record in which a researcher or audit body outside the ministry has examined and confirmed what Mission Control actually processes. A statement about what one intends to do and a report about what one is doing sit at different levels, yet in government announcements the two often appear inside the same sentence, leaving the reader no choice but to separate them.

DELTA's roots lie in a situational-awareness tool built after 2014 by Aerorozvidka, a civilian volunteer organization. To call DELTA Fedorov's creation is to depart from the facts. It had already settled in as a state system long before he became defense minister, and the signature of January 2026 was the addition of one module to a system already turning. Miss this distinction and twelve years of a nation's accumulated work gets read as one man's achievement.

The larger the circuit grows, the further the human eye falls behind. One analytical report noted that between 2024 and 2025 DELTA came to process intelligence, surveillance, and reconnaissance (ISR) data amounting to tens of terabytes a day. Intelligence, surveillance, and reconnaissance is the military term covering the whole activity of finding out where the enemy has placed what, and what it is doing there; drone footage, artillery observation, and scout reports all fall under it. A terabyte holds several hundred high-definition films, and that volume piles up daily.

So the commander's problem moved from seeing more to choosing faster. If human eyes cannot get through tens of terabytes, the filtering falls to machines. Software takes on the work of narrowing candidate targets, deleting duplicates of the same scene, and ranking what should be struck first. DELTA, running in the cloud, sends this filtered picture down to senior command and subordinate units alike. One report observed that the design gives even frontline units and junior officers the situational awareness of a senior commander. It is a structure meant to let the field judge for itself without passing through several links in a reporting chain.

The faster judgment becomes, the greater the room for its basis to pass by without human verification. Which rules produced a given screen, who audits that algorithm, where responsibility rests when a target assessment is wrong — none of this appears in the ministry's announcements. The same was true on 9 April 2026, when the ministry issued a release introducing the Drone Line as the execution of a new doctrine of war. The wording was ambitious, but no independent assessment of what the Drone Line actually produced at the front has yet been obtained. The moment a government announcement is handled with the same weight as a verified fact, biography slides into promotional copy.

It took years for DELTA to become a state system. It was tested as a military coordination tool from 2017, but institutional backing was thin at first; with support from a NATO trust fund it began earning interoperability credentials around 2019. Interoperability means that the equipment and document formats of different national armies mesh and function together. With official ministry approval in 2023,

DELTA changed character from a program that displayed a map into an integrating format that stitches many systems into one.

DELTA is less a single program than an umbrella holding several modules. Under it sit Monitor, which follows NATO's common operational picture standard; Vezha, which streams drone footage in real time; Element, which carries encrypted messages; and Target Hub, which manages the history of a target from discovery to disposal. A common operational picture is the agreement that lets many units see the same map with the same symbols. Mission Control, which Fedorov launched in January 2026, is one new compartment hung beneath this umbrella; he did not raise the umbrella itself.

DELTA's 2024 information security audit is covered in Chapter 8. That audit addressed the system's security and its NATO standards certification; it did not verify the strike numbers DELTA counts.

2. Air Defense, Interceptor Drones, Digital Officers, and the After-Action Review

The fight in Ukraine's night sky in 2026 is a fight of firepower and also a fight of arithmetic. One analytical report noted that a cost gap of roughly 26 to 1 had opened between the attacking side and the defending one. To bring down a single cheap suicide drone, the defender must expend an asset some twenty-six times more expensive. Leave it alone and power plants and apartment blocks are wrecked; try to stop it and precious air-defense missiles disappear. The report called this dilemma the cost of inaction. In a situation where either choice exacts a price, the defending country grows a little poorer even as it wins.

Russia's calculation moved in the direction of widening that gap. According to the same report, Russia signed a production contract with Iran worth 1.75 billion dollars at the Alabuga special economic zone in Tatarstan, agreeing to build some 6,000 drones by 2025. The airframes changed too. The so-called Black Shahed line was fielded, coated in radar-absorbing material and black paint so that radar and the human eye catch it less easily, and fitted with adaptive antennas that filter out jamming. To burn through Ukraine's air defenses to no purpose, a cheap decoy drone called the Gerbera appeared, made of expanded polystyrene — styrofoam. The unit price the report gives for the Gerbera is around 1,000 dollars apiece. When firing a missile worth hundreds of thousands of dollars at a fake target worth 1,000 is repeated night after night, the defender collapses while boasting of its interception rate. This was the shape of the problem Ukrainian air defense had to solve.

Ukraine built a system linking field units, procurement agencies, and the ministry. The design of redundancy — laying things down in layers so that when one gives way another holds — repeats itself in the sky as well.

The bottom layer is the resurrection of old weapons. The Gepard self-propelled anti-aircraft gun, handed over by Germany, became a pillar of drone interception. A self-propelled anti-aircraft gun is a tank hull with a cannon mounted on top pointed at the sky, and its shells cost far less than missiles. Soviet-era short-range air-defense equipment — the ZU-23-2, the ZSU-23-4 Shilka, the 2S6 Tunguska — turned skyward again. In early 2022, a captured Russian Pantsir-S1 air-defense system was repaired, put into action, and credited with kills. For all the talk of a war of advanced technology, what held up the floor of air defense was old autocannon.

Above that lies a net that listens. Ukraine strung thousands of passive acoustic sensors on communications towers and utility poles in a network called Zvook. A passive sensor emits nothing of its own; it only takes down sound. An algorithm trained on the signature of a Shahed drone's engine picks out the airframe from that sound alone. Because it emits no radio waves as a radar does, the sensor's own position is never revealed. The detections gathered this way feed into command systems such as Virazh and Safe Sky, and targets are assigned to mobile firing teams armed with searchlights and heavy machine guns. In 2024, sighting equipment with thermal imaging cameras was added, allowing range and altitude to be fixed precisely. A Dutch radar deployed in Ukraine distinguished birds from drones through processing that reads minute vibration components. It is a method of spreading cheap sensors widely and binding their signals together with software; what Zvook did with sound data is exactly what DELTA did with target data.

The top layer is the interceptor drone. Instead of a missile, a drone catches a drone. The STING family of interceptors named in the report runs about 2,500 dollars apiece and carries a module that chases and aims at a Shahed on its own. If a 2,500-dollar airframe takes over the work of a missile costing hundreds of thousands, the sign in front of that 26-to-1 cost gap flips. The report wrote that this change is rewriting the rules of air combat.

The same report also noted where the net is torn: Russia's guided glide bombs, the KAB and FAB. These are old bombs fitted with wings and guidance kits and thrown from a distance. They are hard to jam, hard to intercept, and they bring down positions and buildings near the front whole. The report argued that production of smaller, cheaper European missiles capable of downing Shahed-class drones must be increased, and that contingency planning to move European defense-industrial facilities underground should be considered against the worst case. The domain where the economics of interceptor drones work beautifully and the domain where there is still no answer share the same sky, so to speak only of air defense's successes is to tell half the story.

There is no record in the public archive that a post called "digital officer" was newly created in the Ukrainian armed forces. Nor is there a primary document setting out how the after-action review — the procedure in which a unit gathers after an operation to trace back what went wrong — has changed in the Ukrainian military. That post and that meeting have therefore been left out of this text. What the documents actually show is only the circumstantial evidence that the role is migrating from people to software, and that is as far as confirmation goes.

One military journal took up how the work of the joint terminal attack controller (JTAC) is changing. A JTAC is an officer who goes forward and guides friendly aircraft onto their strikes. Once the job meant calling out coordinates by voice over a radio and controlling the bombing sequence; now small unmanned aircraft and laser target designators fill that role. The journal advanced the idea a step further, to what it called an Artificial RTO — artificial radio-telephone operator. The conception is of artificial intelligence software seated inside the communications system, processing voice traffic, geographic information, and doctrinal literature in real time and taking over target calculation, leaving the human with nothing but final approval authority.

This conception is a proposal published in a journal, not a system the Ukrainian military already runs, and that distinction will not be blurred here. But the direction of the proposal is the same direction DELTA and Mission Control are heading. It is a design that hands the sorting and calculating a person used to do over to a machine and leaves the person only the final decision. Whether that final decision is genuinely a human judgment, or a procedure for stamping a list the machine has already narrowed, is a question the blueprint alone does not answer.

With the after-action review, the situation is somewhat different. A report on DELTA singled out as a feature of the system its fast feedback loop running from operator to developer. A problem a soldier at the front encounters reaches a developer in short order, and the corrected software goes back down to the front. Lay Mission Control on top of that, and which mission succeeded and what which crew did remain as data during the operation or immediately after it.

Reports are preserved as computerized records, and the people responsible check progress on a dashboard. One can call this a digital after-action review. Something slips away the moment one calls it that. The traditional after-action review is where people argue out loud about why they failed. The log tells you what happened; it does not tell you why the commander judged as he did at that moment. Whether the circuit Fedorov's ministry has built can stand in for the first question, or quietly erases the second, is not something today's documents can answer.

One thing remains clear. When Mission Control proposes to read even an individual soldier's hours at the very front and the volume of logistics that moved for his sake, that system becomes a tool for watching one's own side as much as a tool for watching the enemy. An apparatus that measures performance is always also an apparatus that measures people, and the two functions run together on the same data.

The provenance of the equipment holding up the floor of air defense makes the character of this fight plainer still. The Gepard was designed in West Germany, built by KNDS by mounting an anti-aircraft gun on the hull of a Leopard 1 tank. The targets Zvook catches by sound are passed to mobile firing teams armed with searchlights, DShK heavy machine guns, and twin-mounted Maxim guns. The Maxim is a machine gun from the First World War, and the Skylark sighting unit fitted to it in 2024 uses a thermal camera to fix its range and altitude. A gun from a century ago and an AI acoustic classifier stand in the same position.

The evolution of the Russian airframes will be described only as far as the report records it. The Black Shahed line was fitted with 4G/LTE modems and Starlink communications, and the adaptive antenna that filters out jamming is called Kometa. The Gerbera decoy is not merely cheap; it was built to imitate the radar return that the real strike drone, the Geran-2, leaves behind. Making it impossible to tell the false from the real on a screen is this airframe's purpose. The micro-Doppler processing used by the Dutch radar deployed in Ukraine reads the fine vibrations made by a spinning propeller to separate birds from aircraft.

A caution is in order here. The 26-to-1 cost ratio, the 2,500-dollar figure for the STING, the 1,000-dollar figure for the Gerbera — all of these are numbers written down by a single analytical

report. They are not procurement unit prices published by the Ukrainian government or official manufacturer price lists, and no independent statistics exist in the public record on what percentage of Shaheds interceptor drones actually bring down. The same goes for the Artificial RTO conception: in a design that leaves the human only final approval authority, what that human bases the approval on, and what procedure it would take to overturn the list the machine has narrowed, is not written down in that journal either.

3. Procurement Reform and the Problem of Verifying Battlefield Results

Ukraine's Ministry of Defense drew heavy criticism over corruption in food and uniform procurement. Contracts buying military rations and clothing at absurd prices came to light, and the entire procurement system was put on the block. That shells were short at the front while the price of eggs was inflated in the rear was received as a species of betrayal the public found hard to bear.

Two specialized procurement agencies were created afterward. The Defence Procurement Agency (DPA) handles lethal equipment such as weapons and ammunition; the State Rear Operator (DOT) handles non-lethal supplies such as food and clothing. Supervisory boards staffed with domestic and foreign experts were attached, and contracts were posted on open procurement platforms such as ProZorro. ProZorro is Ukraine's public procurement window, built so that citizens can look up over the internet who bought what for how much. Up to this point it follows the textbook sequence of reform exactly.

Under the new system, the old problems reappeared. To keep defective goods from reaching the front, the DPA established multiple stages of quality inspection and a system of contractual penalties. The trouble was time. Months passed while inspection and standards-compliance procedures were worked through, and the technology cycle of the drone war is shorter than those months. By the time a flawlessly verified drone finally reached the front, there were cases where Russia's new electronic warfare equipment had already blocked the frequency that drone used. Electronic warfare is the fight to jam or intercept radio signals and cut an opponent's communications and control. It is the paradox of a weapon verified perfectly on paper losing its usefulness in the field. The tighter the verification, the later the weapon arrives; the later it arrives, the more the verification's meaning evaporates.

The shortfall in equipment and the burden of repair costs came back onto the soldiers. One report criticized this structure as reactive procurement. The ministry buys weapons in bulk to keep production lines turning and stacks them in warehouses, but by the time they reach the end user they are already obsolete and have to be sent back to the rear for work. When price competition pushes manufacturers to cut costs, the burden of testing, fixing, and modifying passes to frontline units. Cases were reported in which a considerable share of delivered drones could only be flown after units had taken them apart and reworked them, and the situation hardened in which a pilot doubles as mechanic and developer.

The relevant figures show how heavy the burden in the field was. According to a procurement report, frontline drone pilots were spending 5 to 30 percent of a monthly salary of around 3,000 dollars out of their own pockets on modifying and improving their equipment. While the state announced that it had successfully executed procurement in the billions, soldiers' pay was making up for the weapons'

shortfalls. The success of the procurement paperwork and the success of the battlefield were being entered in two different ledgers.

There were walls on the side that watches the money too. A report on the management of international aid funds points out that in wartime procurement, what is harder to handle than outright embezzlement is indirect fiduciary risk: inflating unit prices, trading quality for quantity, pressure to certify deliveries quickly. Even when the quantity specified on paper is certified as delivered exactly, whether the goods possess the quality the battlefield demands is difficult to establish through ex post control alone. So Ukraine and World Bank–affiliated funds brought in standardized procedures and third-party monitoring. Third-party monitoring is when an outside body — neither the giver of the money nor its receiver — goes into the field and checks the goods against the books. At the very front, where no one can enter, there is no way to conduct an on-site inspection; so the place that most needs verification remains the place where verification is hardest.

The answer from Fedorov's camp did not run toward more audits. It ran toward moving the standard of verification itself, and the e-points system already described is that move. Instead of a bureaucrat reviewing paperwork and approving it, the destruction footage a unit films becomes the evidence of performance. Performance becomes points, points become purchasing power, and units choose drones from the manufacturers they have tried themselves and come to trust. The logic is that defective goods get filtered out because the people who use them do the choosing. The procurement report noted that a DeCenter approach is also being tested, devolving to brigades the authority to buy drones and electronic warfare equipment directly from manufacturers with state budget funds. Units that spend their budget well get a larger allocation the next month; money left unspent is clawed back. Counted in hryvnia, Ukraine's currency, one Territorial Defense brigade executed 1 billion hryvnia — about 25 million dollars — in a single year, far beyond the 1 to 1.5 million dollars of an average brigade budget.

The architecture of the system has clear virtues. At the same time, this design did not eliminate the problem of verification so much as move it into a different role.

One role it moved into is the scoring table. The moment the state decides how many points a given target is worth, units chase the high-scoring targets, and the scoring table becomes tactical doctrine. No document has been obtained on who sets and revises this table, by what procedure, or whether that process can be seen from outside.

The reliability of video adjudication leads to the same problem. Deciding destruction from footage has been an old point of contention in every war. No independent document could be found on who makes this determination, how objections are raised, or how many misjudgments there are. The ministry's own tally of 820,000 targets in 2025 is a sum built on top of this adjudication procedure, so if the procedure is unverified, so is the sum.

Treating the speed of spending funds as performance carries its own risk. A rule that gives more money to units that spend money quickly breaks up sluggish administration. It also leaves room for spending fast and spending well to be counted as the same thing. A metric that measures speed

measures only speed.

But questions remain whose results have not been made public. No external audit report examining this entire circuit has been obtained. There is no document independently verifying the Army of Drones Bonus, DOT-Chain Defence, or the procurement results stacked on top of them. The 500,000 items and the record-scale drone contract announced on 11 March 2026 are figures the ministry issued itself, self-reporting as of the date of the announcement.

One policy report summed up the lesson of this war as follows: technology does not become combat power by itself, and only when policy, procurement, and doctrine move together does technology turn into military strength. Fedorov's ministry tried to translate that sentence into institutions. It built a circuit in which a strike becomes points, points become an order, an order becomes contract data, and contract data becomes matériel again and goes down to the front. From the procedure for buying a single component to the way a single brigade executes a budget, this circuit has tied the army's hands and feet to data.

How much faster that circuit actually became, and whether it was accurate in proportion to its speed, has yet to be answered. The documents that would produce an answer still exist on only one side. As of 13 July 2026, six months into his tenure as defense minister, the substance of the documents describing this circuit comes from the ministry that runs it. This is not an accusation but a description of a state of affairs. In a country at war, it is common for outside audits to lag. But if the delay stretches on, the condition in which the party claiming results and the party confirming them are the same person hardens, and an army commanded by data turns into an army commanded by the people who make the data.

Consider again the main substance of the reform. Procurement was taken out of the hands of ministry headquarters and moved to separate agencies; supervisory boards of domestic and foreign experts were seated above those agencies; contracts were posted on ProZorro for citizens to inspect. What this design aimed at was preventing a recurrence of the corruption of eggs and jackets, not getting weapons to the front faster. The two aims gnawed at each other on the same set of procedures, and the paradox in which tighter inspection means later arrival came from here.

The marketplace e-points opened is called Brave1 Market. A unit receives points in proportion to results certified on video, and when it uses those points to choose drones from a manufacturer it has tried itself and come to trust, the ministry pays the manufacturer. In this structure the manufacturer's customer is the unit, not the procurement bureaucrat. It is a market where the reputation circulating among units becomes revenue, and this is where a well-made company's power to survive comes from. It also leaves compartments that a list of what units want to buy cannot fill. For guided glide bombs — hard to intercept, capable of collapsing a position whole — the report noted there is no answer a unit can buy no matter how many points it accumulates.

The verification methods on the funding side carry limits of their own. Ukraine and World Bank–affiliated funds brought in third-party monitoring and standardized procedures because, as the scale of support grew, ad hoc checks and reliance on individual consultants could no longer bear the

weight. Ex post control means reconciling the books after the goods have arrived, so even when the quantities match, it cannot establish whether those goods possess the quality the battlefield demands.

The procurement report also records that pilots spend 5 to 30 percent of a 3,000-dollar monthly salary on modifying equipment. But no document has been obtained showing whether that share fell or held steady after e-points and DeCenter began to turn. Whether the new system has actually lightened the old problem will be answered only when someone looks into the soldiers' wallets again.

Chapter 11. The Other Side of Reform: Concentrated Power and Accountability

On 30 April 2026, an interview with Pavlo Yelizarov, deputy commander of the Ukrainian Air Force, went up on the YouTube channel of Ukrainska Pravda. The title carried three phrases: "Fedorov's 100 days," "the anti-drone dome," and "the chaos of short-range air defense." Yelizarov compares the mixing of the new team brought into the Ministry of Defense with the General Staff to "oil and water." Put them in one bowl and they still will not blend. His example is a count of radars. Work the terrain out on paper and four are enough to cover a city, yet eleven are demanded, for no reason other than that the establishment table says eleven.

An establishment table is a document written in advance, setting down which unit is to hold which equipment and how many people, and in what numbers. It is usually drawn up long before a war begins, and once drawn up it is rarely amended. Yelizarov's charge is that the document outranks the terrain. The document fixes the answer before the calculation is made, and custom sits in the seat where need ought to be weighed.

Where the charge came from deserves attention too. Yelizarov was a guest on a broadcast. How the General Staff answered on the same matter, and which page of which document actually carried the figure of eleven, are nowhere in the public record. Criticism and defense of Fedorov mostly circulate in this form. They are raised on a broadcast, rebutted on a broadcast, and leave no documentary trace.

Beyond the substance of the reform, the character of the documents supporting it must also be examined. Before asking where power is gathering, one asks first whether there is material with which to answer. The reference date is 13 July 2026, and between what the documents and broadcasts secured by that day confirm and what lies outside the public record there is a wide gap.

1. Whose Words Are the "Digital Mafia" Charge?

Fedorov was appointed defense minister in January 2026. A little over a month later, on 16 February 2026, the YouTube channel Dana Yarova posted a broadcast titled "Fedorov Is Zelensky's Mirror." The program took issue with signs that soldiers were being pulled in for questioning, and floated the suspicion that the government meant to run elections through the Diia app as well.

The phrase already carries the writer's verdict inside it. Mirror reads as a claim that Fedorov reflects back the same manner of governing as Zelensky. Running the state through apps and screens and announcements, putting speed ahead of procedure, and seeking to manage criticism rather than endure it — all of that is packed into the single word.

Around this time the phrase "digital mafia" began circulating on several Ukrainian political YouTube channels. It compresses into two words the suspicion that people who had worked alongside Fedorov since his days at the Ministry of Digital Transformation had divided the key posts of the Ministry of Defense among themselves, and that weapons procurement, battlefield data, and citizen-facing platforms had all gathered into the hands of one team. A figure from the military-technology industry is

named as the source of the phrase, but the public record holds no primary record of that person saying it.

Within the public record, "digital mafia" appears only as a quotation on YouTube broadcasts. There is no primary record — no text written by that person, no original transcript of an interview they gave, no minutes of a meeting — by which one could confirm when, where, or in what context the words were spoken.

"Mafia" likens a person to a criminal organization. The more gravely a word can wound someone's name, the firmer the ground must be beneath whoever repeats it. So the phrase is not treated here as a finding of fact, only as the name of a criticism now in circulation. That the phrase circulates is confirmed. Whether what it alleges is true — here the public record stops.

The condition of criticism living only on broadcasts holds just as firmly on the opposite side. On 10 July 2026, the YouTube channel Fabrika Novyn (Фабрика новин), covering the mass resignation of the cabinet, called Fedorov "the cabinet's only bright spot." The program's framing is stark. The military leadership, Commander-in-Chief Syrskyi among them, is trapped in an outdated doctrine that treats soldiers as consumables to be pushed into trenches; Fedorov is a man trying to fight the war with technology; and unless the President's Office replaces the old leadership, there is only so much he can do alone.

Fabrika Novyn is a single YouTube channel that publishes political commentary under provocative headlines. No reporting by another outlet, no internal military document, no independent verification exists in the public record to support or refute this program's charge that the military leadership holds a "consumables" doctrine. In wartime Ukraine's public sphere, the political intent of building one figure up and tearing another down seeps into the language of broadcasts, and this quotation stays on the page marked as a document of that character.

The same media ecosystem calls Fedorov's team a "mafia" on one side and "the only hope" on the other. Both statements are broadcast claims, and neither is backed by documents. The two frames are set side by side here because most of the information a Korean reader will encounter about Ukraine's defense reform has exactly this character. Heroic tales and conspiracy theories are made of the same material, and both spread fast without ever being checked.

Fedorov himself did not sidestep the controversy. On 17 June 2026, the title of his interview with the YouTube channel PRESSING carried, plainly, the three things he had to answer for: his relationship with Syrskyi, the rumors of his resignation, and the corruption clans in the defense sector.

That a country's defense minister fielded these three questions in one sitting, six months into the job, is itself a piece of information. It means three suspicions had grown around him at once. That he was at war with the commander-in-chief. That he was about to step down. And that the interest groups surrounding defense procurement were swallowing his reform, or else that his reform was creating a new interest group of its own.

The form of his answers is much the same from interview to interview. He answers with systems and data. A brigade-by-brigade combat-effectiveness rating, scored across multiple categories and used

as the basis for allocating resources and selecting commanders. Polygraph tests — lie-detector tests — meant to screen out leakers inside the ministry and the procurement bodies, along with lobbyists for suppliers. And shell procurement, where a range requirement was written into the tender so that the bidding conditions themselves changed. Those are the examples he returns to. Among them, he said, one measure — distributing a predictable quantity of equipment to each brigade — took three months to push through.

Numbers always accompany these examples. How many rating categories there are, what percentage of the budget the first tender saved, how far the price of a single shell fell. Those numbers are not reproduced here. All of them are the minister's own account, given in broadcast interviews, and within the public record no primary document — no tender notice, no contract, no audit report — could be found to support them.

Numbers that live outside the public record have been left out of the text. But when the actor carrying out the reform tallies the reform's results, announces that tally on a broadcast, and no external audit document exists, copying the numbers over puts publicity in the seat where verification should sit. Anyone trying to assess Fedorov's Ministry of Defense as of July 2026 stands on that condition.

Whether these changes amounted to a concentration of power also has to be weighed. It is neither asserted that power concentrated nor that it did not. What remains instead are the structural conditions that make concentration a reasonable suspicion. One ministry handles weapons procurement, battlefield data, and citizen-facing platforms together. That same ministry tallies the figures for its own performance and announces them itself. And no independent audit or investigative reporting exists in the public record by which that tally could be checked.

When those three overlap, it is hard to stop critics from reaching for an ugly word like "mafia." That does not mean the word is right. It means there is nothing with which to refute it except the ministry's own explanations. Whether power is in fact being abused, and whether any mechanism exists to confirm or deny the abuse, are different questions, and only the second can be gripped through the public record.

Trace criticism back to its source and the critic sometimes turns out to have an interest of their own. The person named as the source of the phrase works in the military-technology industry. The tender rules and procurement procedures Fedorov reached into touch that industry's revenue directly. Still, no primary record has been secured showing the context in which that person actually spoke the words. So this biography does not attribute the phrase to any individual as an established statement.

The character of his answers is worth noting as well. Brigade ratings, polygraph tests, changed tender conditions — these are all mechanisms by which a ministry looks inside itself. What is absent from the public record is how bodies standing outside the ministry and looking in — audit institutions, anti-corruption investigators — mesh with this reform. Organizations that examine themselves usually pass themselves.

How long it takes new rules to set is another limit. His remark that a single measure — distributing predictable quantities to each brigade — took three months shows the speed at which one decision

settles inside the Ministry of Defense. Any attempt to render a verdict on this dispute six months into his tenure is made with material still short.

2. The Clash of Rights in Conscription, Surveillance, and Rooting Out Corruption

TCC is the abbreviation for Ukraine's territorial recruitment centers. They are the bodies that find and summon those subject to mobilization. As the war has dragged on, the name has become one of the most hated in Ukrainian society.

On 24 April 2026, a Radio NV broadcast covering the overhaul Fedorov was drafting put in its headline his intention to change the entire mobilization system that runs through the TCCs. The grain of the reform is the same as the work he had done at the Ministry of Digital Transformation. One part is digitizing records: moving into data the files of soldiers who had been classified as absent without leave because a paper document went missing or never made it from one unit to another. Absence without leave is abbreviated in Ukrainian as СЗЧ, meaning the state of having left one's unit without permission. It has actually happened that a single vanished sheet of paper branded a soldier this way. The other part is introducing a contract model: writing into a document how long the term of service runs, and under what conditions a soldier may transfer to another unit or be discharged.

Grabbing people off the street and loading them into vans could not go on, was his diagnosis, and in an interview he criticized that method in terms close to human trafficking.

As of the reference date of 13 July 2026, this mobilization overhaul is confirmed as the minister's plan and as the direction he stated on broadcasts. When it was written into law, how far it was put into effect, and whether mobilization actually changed as a result — here the public record stops. Plans are not transcribed as outcomes.

On the ground, clashes were already happening. In its 10 July 2026 broadcast, Fabrika Novyn reported a physical confrontation between TCC staff and young men in Lviv, charging that TCC staff had become a privileged group that never goes to the front and instead commits violence against civilians in the rear with impunity. As noted, this channel is a single political-commentary YouTube outlet, and no investigative file or court document exists in the public record by which the course of events could be confirmed.

Responsibility is tangled too. Where the TCCs' chain of command connects to the Ministry of Defense — here the public record stops. What is confirmed is that the anger surrounding mobilization is aimed at the defense minister, and that Fedorov, rather than retreating behind a question of jurisdiction, chose to take the problem on. That choice is dangerous in two directions. Fail, and he wears someone else's failure. Succeed, and the data of troop mobilization gathers into his ministry.

Moving mobilization records into digital form makes administration faster, but it also raises the risk to citizens' rights. Fewer people will be branded deserters because one sheet of paper went missing. When a discharge date is fixed in a document, a soldier can foresee their own time, and service one can foresee is itself a right. Yet the same system creates a state that knows each citizen's location, service history, and movements far more finely than before. The device that grants convenience and

the device that enables surveillance are often the same object, and to say the app tells a soldier their discharge date is the front half of a sentence whose back half is that the state knows that soldier's status in real time.

Pressure to reduce rights shows up in blunter forms as well. Yelizarov, who appeared earlier, argued in his Ukrainska Pravda interview that people who did not go to defend the country may remain citizens but should not be allowed to vote in elections for the next ten years. He himself acknowledged that this draws criticism as the stripping of a constitutional right, and did not back down.

This is one guest's argument, and no ground exists in the public record for calling it government policy. Yet the fact that such an argument surfaces without hesitation in an interview with a major outlet shows that the wartime public sphere has begun putting basic rights like universal suffrage on the bargaining table. Universal suffrage is a right one holds by being a citizen. The moment it is turned into a prize handed to those who have earned merit, it is already a different institution, and that principle is shaking before the justification of war.

Suspicion about voting runs in the opposite direction too. The Dana Yarova broadcast raised the allegation that the government intends to run elections through the Diia app. Once an app holding identity documents and administrative services also holds voting, certain questions follow. What becomes of people who cannot access the app. Who verifies the count. What prevents the coercion of a workplace or a unit demanding that you open the app and show them. One of the things a paper ballot protected was secrecy. The public record holds no government document supporting the allegation and no independent verification dismissing it; what is confirmed is only that the suspicion exists.

The Ministry of Digital Transformation has answered suspicions of this kind with documents. On 30 June 2026, the ministry issued an official statement addressing "manipulative claims" about Diia City, the regime for IT companies it had been promoting. That document is a defense the ministry wrote for itself. To be unable to hear the criticism in the critic's own voice, learning it only through the summary in a rebuttal, is itself an asymmetry of ground. What reports Ukraine's civil society and human rights organizations have issued on Diia and the digitization of conscription — those documents could not be obtained. To paper over that gap and write "the concerns are exaggerated" would be to treat a government announcement as carrying the same weight as verification.

The instruments of surveillance have already become part of the war. Ukraine adopted the technology of the American facial recognition firm Clearview AI in the war's earliest days. Facial recognition converts the features of a face in a photograph into numbers, then matches them against a vast pre-assembled database of faces to identify a person. The system is reported to have identified more than 230,000 Russian soldiers and to have been used in tracking war crimes. The same company has been fined heavily in France, Italy, and other European countries for building its database by scraping billions of photographs from social media without consent. The tool that exposes war crimes and the tool ruled unlawful in Europe are the same tool, and the urgency of war erases the lines that peacetime law had drawn.

Inside the cities the situation is much the same. Kyiv and other major cities are covered by a "Safe City" camera network equipped with facial recognition and license plate recognition. Civic groups called it "Big Brother's sharp eye" and warned of surveillance over private life. In March 2022 the parliament passed a law (No. 2123-XI) granting police access to biometric databases including fingerprints and facial data, and human rights organizations warned that collecting biometric information without safeguards leaves an injury that cannot be undone.

"Cannot be undone" should be taken at face value. Fingerprints and faces are not passwords. A leaked password can be changed; a fingerprint cannot. And what war justifies remains after war ends. The cameras are not taken down, and the databases are not deleted. This surveillance network is not something Fedorov personally began, but it runs on the plumbing of the state that he laid.

Individual rights can be violated in the course of corruption investigations and administrative reform as well. That Fedorov pushed through large-scale polygraph testing inside the Ministry of Defense and the procurement bodies immediately after taking office is something he stated himself in interviews. Those who refused the test and those who failed it alike lost their posts, he said.

The aim of rooting out corruption is legitimate. When money meant to buy weapons leaks away, soldiers at the front die. But a polygraph merely measures the bodily reactions believed to appear when a person lies — changes in pulse, perspiration, breathing — and cannot read the lie itself. Its accuracy has been disputed for a long time, and courts in many countries do not admit the results as evidence. A procedure that dismisses public officials on the basis of a test result or a refusal to take the test, with no indictment and no trial, collides head-on with the principle of due process. On what legal basis this was carried out, whether anyone lodged an objection, and what came of it — here the public record stops.

The use of state power against critics has surfaced as a problem too. According to the Dana Yarova broadcast, the businessman Ihor Kryvetskyi, who publicly criticized ministry policy by arguing that conscripting men aged 18 to 24 amounts to destroying the reserve, subsequently had his vehicle searched on the road by the Security Service (SBU) and received a summons on suspicion of obstructing the lawful activity of the Ukrainian armed forces. This too is one channel's reporting, and no investigative file or independent confirmation by another outlet exists in the public documents. But if it is true, it means the threshold has dropped for treating criticism of military policy as the crime of obstructing military activity. When the line between criticizing policy and aiding the enemy blurs, people say less, and what remains is silence.

The root of this problem runs deeper than any one man. In July 2025, before Fedorov became defense minister, a bill (draft No. 12414) came before Ukraine's parliament that could in effect have dismantled the independence of the National Anti-Corruption Bureau (NABU) and the Specialized Anti-Corruption Prosecutor's Office (SAPO). These are the bodies that investigate and prosecute corruption by senior officials. Immediate pushback from civil society, the Anti-Corruption Action Center among them, preserved the two bodies' independence.

There was an attempt by those in power to control the bodies that watch for corruption, and the force that stopped it came from civil society's resistance. This episode is a coordinate to place in the background when reading Fedorov's reform. In Ukraine, the checks were barely held onto by people taking to the streets, and the condition that a ministry wielding large powers in wartime faces checks that were weak to begin with remains, whatever becomes of the reform.

Start with the size of the problem. Fedorov said on a broadcast that roughly two million people are wanted for conscription and that more than 200,000 soldiers are classified as absent without leave. These figures come from the minister himself, and no statistical agency's release or audit document confirming them exists in the public record. Even if the figures are not exact, though, the circumstance remains: a system in which one sheet of paper changes a person's status is running at a scale of hundreds of thousands.

On the question of responsibility, the minister's side has its own explanation. The TCCs belong not to the Ministry of Defense but to the Ground Forces, and politicians nonetheless use them as a club to beat him with. No organizational chart or statute confirming this explanation exists in the public record. Wherever they belong, the anger goes to the defense minister.

Bill No. 8153 is a personal data protection bill introduced in October 2022. Like the European Union's GDPR, it contained rights of access and erasure, minimization of collection, and protection of biometric information. While requiring consent from the individual for the processing of biometric data, it explicitly permitted investigative agencies to install surveillance cameras in public places. It also established a general right to refuse automated processing, but did not tier the risk levels of AI use. Protective clauses and surveillance exceptions sat together in a single bill, and human rights organizations demanded that the checks be written out more concretely.

3. How to Hold On to Accountability in a Fast Technological War

The faster machines make judgments, the blurrier it can become who bears responsibility for a wrong decision. The second issue of the American military policy journal Modern War Journal answers this question in short, hard sentences. Innovation does not by itself mean advantage, the journal writes; technology without doctrine breeds vulnerability, speed without judgment invites strategic risk, and autonomy without accountability destroys the trust that is the foundation of the soldier's profession.

Three pairs emerge. Technology and doctrine, speed and judgment, autonomy and accountability. Doctrine means the military's rules for when and how a weapon is used; accountability means the principle that whoever decides must explain and bear the outcome. Hold on to the first of each pair and empty out the second, and what remains is an army that is wrong quickly.

How far speed can go has already been shown on another battlefield. The same journal records that Gospel, the target recommendation system Israel used in Gaza, reviews targets and issues strike recommendations at least fifty times faster than a human analyst. Fifty times is a speed no person can keep up with, and to say a person cannot keep up is joined at the hip to saying a person cannot check. Someone who approves without checking is only pressing a button.

So the policy literature nails down artificial intelligence's role. An IFRI report distilling the mil-tech war into eight lessons defines AI as a "process accelerator" and does not place it in the seat of the commander who decides. It is a tool that combs through thousands of hours of drone footage and satellite imagery to assemble and surface candidate targets, a tool that holds up a commander who has gone days without sleep so their judgment does not run dry. With no legal framework yet defining a machine's responsibility, the report writes, AI must not become a system that substitutes for human authority.

Military doctrine calls this principle Human-in-the-Loop. It means a human must always be inside the loop of any decision that can kill a person. Modern War Journal writes that there is no evidence any country has yet fielded an AI weapons system in combat without keeping a human in the loop. That is a confirmation that one line remains uncrossed; it does not carry any guarantee that the line will hold.

There is research that frames why the human must remain in another language. Avi Goldfarb and Jon Lindsay's "Prediction and Judgment" argues that artificial intelligence in fact raises the importance of humans in war. What AI is good at is prediction: finding patterns in data and guessing what comes next. Judgment — weighing what that prediction means in the present political and military context, what striking this target signifies for the war as a whole — remains the human's share. The cheaper and more abundant prediction becomes, the higher the price of judgment climbs.

The problem is whether people can keep making that judgment. When a machine produces a plausible answer, doubting it takes effort. Not doubting is always faster, and in wartime fast looks like right.

What Fedorov's Ministry of Defense holds up is speed. The speed of procurement, the speed of distribution, the speed with which feedback from the front loops back into production. Look at the examples he gives on broadcasts, and even the line about one measure taking three months to pass comes out in the form of a boast. It sounds like saying that in the past such a measure would never have passed at all.

What was established earlier is a list on the other side. The performance figures are tallied by the ministry itself. No external audit document exists in the public record by which the savings from procurement reform could be checked. The General Staff's rebuttal was never recorded. Where the people who lost their posts to polygraphs took their objections cannot be known, and while there is reporting that a citizen who criticized ministry policy was summoned by the Security Service, no document exists by which the full course of that episode could be confirmed.

Holding power to account requires that disclosure of records, independent audit, and parliamentary control all function. That is: records, verification, and room to object. What a strike was based on must remain on file; someone other than the person who made the tally must check it; and those harmed and those criticizing must have a channel to speak. As of 13 July 2026, within the public record, those three functions at Fedorov's Ministry of Defense are either empty or filled by the ministry itself.

Jere Perez's piece in Modern War Journal turns the question over. Autonomous systems will not decide who holds the advantage on the future battlefield, he writes. The people trusted enough to be

handed those systems will. He closes with a sentence saying the decisive advantage comes not from what equipment an army fields but from what kind of people it raises.

Fedorov set out to change an old military organization and its procurement procedures. Data instead of paper, metrics instead of meetings, tenders instead of custom. That fight has its case, and soldiers at the front may well have gained something real from it.

But one of the things the establishment table did was tie authority to a document. The very document that forced a demand for eleven radars was also the document that stopped anyone from turning eleven into twenty on a whim. Slow and tied down are usually one body, and where custom has been cleared away, the blank left by the brake that custom used to supply is left behind with it.

The document that would tie down the authority now moved into data has not yet been written. Who will write it? As of 13 July 2026, no public document holds the answer.

How leaning on algorithms eats away at command was written by Adam Ropelewski in the same journal. Lean on the machine's recommendation again and again, and a commander's power to move first shrinks, while the flexibility of mission command is shaved down. Mission command means giving only the objective and letting the commander on the ground decide the method, instead of directing every step from above. When the machine puts the answer out first, there is nothing left for the ground to decide on its own.

The conversation between General Votel and Dean Reeves in the same journal gives that temptation a name. Push the data into the machine and a plausible result comes out, so one starts wanting to hand the deciding over to the machine rather than doing it oneself. Reeves says electronic devices have shortened people's power to concentrate, and that in such a state the deep thinking needed to cut through war's uncertainty does not come. The training he sets himself is to put the devices away and read a paper newspaper and a thick history book all the way through. It means becoming someone who does not freeze when the machine thrusts a conclusion forward, someone who can think their own way out.

This is why Perez traces the matter all the way back to recruitment. Autonomy is not handed down from above; it comes from the identity formed at the first point of contact with the military. Within the public record, Fedorov's reform is about procurement and data and contracts. On how to raise people who will not let go of judgment in front of a machine — here the public record stops.

Conclusion. The New Normal of Twenty-First-Century Digital War

Mykhailo Fedorov's career began at a single screen and ended up inside the Ministry of Defence. Diia moved the door of public administration onto the smartphone, and after the invasion, evacuation aid, damage reports, and wartime information all passed through that door. Starlink revealed that a company outside the national telecommunications network could hold the connective line of a war in its hands. The IT Army left a blank space in law and command between a government's request and the attacks launched by volunteers beyond its borders. Brave1 and the drone programmes showed what it looks like when start-ups, donations, procurement, and combat all move within a single circuit.

The strength of that circuit is speed. A demand from the front reached developers, and the time it took for a prototype to pass testing and arrive at a unit grew shorter. Data came up the chain instead of paper reports, and there were repeated attempts to connect equipment orders with battlefield performance. That a country in the middle of a war tried to change in a matter of months what would ordinarily take years to reform is hard to deny.

On the far side of speed sits accountability. A private company's terms of service divide the scope of operations, volunteers' attacks blend into state action, and a government evaluates the performance of the very companies it has funded. Even when data makes decisions faster, what that data left out does not reveal itself on its own. Audits, parliamentary oversight, and the procedures that protect citizens' rights look slow from the battlefield, but when those procedures vanish, responsibility for failure blurs along with them.

Fedorov carries the face of a reformer and the face of an administrator who has gathered power. He made an old government move quickly, and in doing so he redrew the boundaries between government and business, between citizens and the army. The central question is who will watch that line. As of 13 July 2026, the public institutions do not answer that question adequately.

War tests technology, but it does not grant democracy an exemption from accountability. The next record of Fedorov's tenure will not be written in drone output or app user counts alone. Whether the fast state he built can withstand criticism, open its books, and share its authority — that outcome will set the weight of the chapters still to come.

1. Bibliography

All URLs were verified on 13 July 2026.

Navigating Ukraine's Defense Tech Market. EY, 2025-10-01.

https://www.ey.com/content/dam/ey-unified-site/ey-com/en-ua/insights/defense-tech/navigating-ukraine-defense-tech-market.pdf

Ukraine: Digital resilience in a time of war. Brookings Institution, 2024-01-01.

https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf

Lessons from the First Cyberwar. Henry Jackson Society, 2024-02-01.

https://henryjacksonsociety.org/wp-content/uploads/2024/02/Lessons-from-the-First-Cyberwar-by-Kirichenko.pdf

Drones in Modern Warfare: Lessons Learnt from the War in Ukraine. Australian Army Research Centre, 2024-10-22.

https://researchcentre.army.gov.au/sites/default/files/241022-Occasional-Paper-29-Lessons-Learnt-from-Ukraine_2.pdf

Autonomous Drones: Emerging Trends from Ukraine. CAPSS India, 2026-02-01.

https://capssindia.org/wp-content/uploads/2026/02/8-Abhishek-Kumar.pdf

Russia's War on Ukraine: One Year of Cyber Operations. CERT-EU, 2023-02-01.

https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

Mapping the MilTech War: Eight Lessons from Ukraine's Battlefield. IFRI / Munich Security Conference, 2026-02-01.

https://securityconference.org/assets/01_Bilder_Inhalte/05_Marketplace_of_Ideas/MSC_2026/ifri_tenenbaum_et_al_miltech_war_ukraine_2026_0.pdf

Developments in space governance and the impact of the war in Ukraine. SIPRI, 2023-06-01.

https://www.sipri.org/sites/default/files/SIPRIYB23c11sIII.pdf

Enhancing resilience by boosting digital business transformation in Ukraine. OECD, 2024-05-01.

https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf

Developments in governance of cyberspace and the impact of the war in Ukraine. SIPRI, 2023-06-01.

https://www.sipri.org/sites/default/files/SIPRIYB23c11sIV.pdf

Ukraine's Cyber Defence Evolution. CCDCOE, 2026-03-01.

https://ccdcoe.org/uploads/2026/03/CCDCOE_Policy_Brief_Ukraines_Cyber_Defence_Evolution.pdf

Ukraine's Drone Ecosystem and the Defence of Europe. LSE IDEAS, 2025-04-05.

https://www.lse.ac.uk/ideas/Assets/Documents/Research-Reports/2025-04-05-DRONES-MatlackSchwartzGill-FINAL-WEB.pdf

Digital Transformations of Ukraine's Cybersecurity System in Wartime. ARMG Publishing, 2025-11-01.

https://armgpublishing.com/wp-content/uploads/2025/11/monograph-3-2025.pdf

Nothing Quiet on the Eastern Digital Front. New Strategy Center, 2024-06-01.

https://newstrategycenter.ro/wp-content/uploads/2024/06/NOTHING-QUIET-ON-THE-EASTERN-DIGITAL-FRONT_NSC.pdf

Leveraging Ukraine's Drone Production Capacity. Prism UA, 2025-04-01.

https://prismua.org/wp-content/uploads/2025/04/Blue_and_yellow_annex_on_defense.pdf

Ukrainian Digital Resistance to Russian Aggression. StrategEast, 2022-05-01.

https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf

Wizard Warfare: Ukrainian Technological Developments Overview. Johns Hopkins APL, 2025-01-01.

https://www.jhuapl.edu/sites/default/files/2025-01/WizardWarfare_final.pdf

Lessons from Ukraine's Information Defence for Democratic Resilience. CIGI, 2025-06-01.

https://www.cigionline.org/static/documents/DPH-Paper-Padalko_Summer2025.pdf

A Decade in the Trenches of Cyberwarfare. National Security Archive, 2024-02-02.

https://nsarchive.gwu.edu/sites/default/files/documents/semon9-ryglx/2024-02-02-Cyber-Diia-A-Decade-in-the-Trenches-of-Cyberwarfare.pdf

From policy to victory: Harnessing defence technology. RAND, 2025-12-01.

https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3800/RRA3833-2/RAND_RRA3833-2.pdf

Lessons from the War in Ukraine for Space. RAND, 2025-03-01.

https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2900/RRA2950-1/RAND_RRA2950-1.pdf

Digital Transformation in Ukraine. KPMG, 2025-11-01.

https://assets.kpmg.com/content/dam/kpmg/de/pdf/Themen/2025/11/Digital%20Transformation%20in%20Ukraine.pdf

Building and leveraging Ukraine's drone capabilities in conflict and beyond. Murray Lab, 2025-03-01.

https://murray-lab.org/wp-content/uploads/2025/03/UkraineDroneEcosystem-Analysis_2025.pdf

Ukraine's Cyber Defense. German Marshall Fund, 2023-12-01.

https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf

Ukraine's drones industry: Investments and product innovations. KSE Institute / Brave1, 2024-10-04.

https://kse.ua/wp-content/uploads/2024/10/241004-Brave1-report-v.1.pdf

Building the digital front line. Atlantic Council, 2025-11-01.

https://www.atlanticcouncil.org/wp-content/uploads/2025/11/CSI_CompaniesAtWar.pdf

Assessing Russian Cyber and Information Warfare in Ukraine. CNA, 2023-11-01.

https://www.cna.org/reports/2023/11/Assessing-Russian-Cyber-and-Information-Warfare-in-Ukraine.pdf

EU Defence Industry Transformation Roadmap. European Commission, 2025-12-01.

https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf

Ukraine's Rapid Digitalization. CSIS, 2024-02-14.

https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-02/240214_Flacks_Ukraine_Digitalization.pdf?VersionId=_ZNBi1gSW50ffi6fn0KbZXHMDbEHR_cU

Cyberwarfare in Russia Ukraine War Lessons for India. CENJOWS, 2025-12-01.

https://cenjows.in/wp-content/uploads/2025/12/Flt-Lt-Shobhit-Mehta-Gp-Capt-Umang-Kumar-_-Article.pdf

Mapping the MilTech War: Eight Lessons from Ukraine's Battlefield. IFRI, 2026-02-01.

https://www.ifri.org/sites/default/files/2026-02/ifri_tenenbaum_et_al_miltech_war_ukraine_2026.pdf

The Ukrainian defense technology market. KSE Institute, 2026-03-31.

https://institute.kse.ua/wp-content/uploads/2026/03/the-ukrainian_defense_technology_market_eng_march_2026.pdf

Six Key Lessons from Ukraine's Drone War. Irregular Warfare Center, 2026-05-20.

https://irregularwarfarecenter.org/wp-content/uploads/I_10_Six_Key_Lessons_from_Ukraine_Drone_War.pdf

Business Ukraine Spring 2026. Business Ukraine, 2026-05-01.

https://businessukraine.ua/wp-content/uploads/2026/05/BUSINESS_UKRAINE_SPRING_2026.pdf

Enabling Ukraine's Response at Scale. World Bank, 2026-03-01.

https://documents1.worldbank.org/curated/en/099713103262663347/pdf/IDU-8f5a661b-317c-4cbb-ab7e-0a9c95156336.pdf

Progressive Policy Institute Ukraine defense tech report. Progressive Policy Institute, 2026-04-01.

https://www.progressivepolicy.org/wp-content/uploads/2026/04/2026_04_TJacoby_FINAL.pdf

Dronisation without militarisation. EPIK, 2026-03-01.

https://epik.eu/?ut_download=1329&ut_token=5fb94e345668040f3f9c87be282918f9

UAVs: ISR, Deterrence and War. IISS, 2026-03-01.

https://www.iiss.org/globalassets/media-library---content--migration/files/publications---free-files/strategic-dossier/uavs-2026/iiss_uavs-isr-deterrence-and-war_032026.pdf

Towards Smart Defence. Cambridge Centre for Geopolitics, 2026-02-01.

https://www.cfg.cam.ac.uk/wp-content/uploads/2026/02/Towards-Smart-Defence.-Victoria-Vdovychenko-2.pdf

Teaching Humans in the Loop. LSE IDEAS, 2026-06-01.

https://www.lse.ac.uk/asset-library/matlack-j-and-gill-o-teachinghumansintheloop-1.pdf

2026 Annual Threat Assessment. ODNI, 2026-03-01.

https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf

Modern War Journal second edition. Modern War Institute, 2026-03-19.

https://mwi.westpoint.edu/wp-content/uploads/2026/03/Modern-War-Journal-MWJ-second-edition-final-draft-as-of-19MAR26.pdf

Mapping peacetime reconstruction needs of Ukraine. European Parliament, 2026-07-01.

https://www.europarl.europa.eu/RegData/etudes/STUD/2026/783617/EXPO_STU%282026%29783617_EN.pdf

Tactical Energy Delivery and Management in the Ukraine War. US Army, 2026-03-30.

https://api.army.mil/e2/c/downloads/2026/03/30/c260713f/no-26-1116-powering-the-front-tactical-energy-delivery-and-management-in-the-ukraine-war.pdf

Про призначення Федорова М.А... | від 14.01.2026 № 4756-IX [On the appointment of M. A. Fedorov | 14 January 2026, No. 4756-IX]. Verkhovna Rada of Ukraine, 2026-01-14.

https://zakon.rada.gov.ua/laws/show/4756-20

Сьогодні ми почали суттєве перезавантаження - зміни внутрішні, щоб Україна була більш стійкою - звернення Президента [Today we began a substantial reset — internal changes so that Ukraine is more resilient: address by the President] - Офіційне інтернет-представництво Президента України. President of Ukraine, 2026-01-13.

https://www.president.gov.ua/news/sogodni-mi-pochali-suttyeve-perezavantazhennya-zmini-vnutris-102277

Mykhailo Fedorov appointed as Ukraine's new Minister of Defence | MoD News. Ministry of Defence of Ukraine, 2026-01-14.

https://mod.gov.ua/en/news/mykhailo-fedorov-appointed-as-ukraine-s-new-minister-of-defence

Mykhailo Fedorov signs order to launch Mission Control drone command and control system in DELTA | MoD News. Ministry of Defence of Ukraine, 2026-01-23.

https://mod.gov.ua/en/news/mykhailo-fedorov-signs-order-to-launch-mission-control-drone-command-and-control-system-in-delta

Понад 75 млн доларів внесків та оголошення набору до Армії дронів: UNITED24 звітує про два місяці роботи [More than 75 million dollars in contributions and the announcement of recruitment to the Army of Drones: UNITED24 reports on two months of work]. UNITED24, 2022-07-01.

https://u24.gov.ua/uk/news/reports_on_two_months_of_activity

Михайло Федоров: Армію дронів посилять ударні БПЛА українського виробництва. Підписали контракти про співпрацю з чотирма компаніями [Mykhailo Fedorov: The Army of Drones will be reinforced by Ukrainian-made strike UAVs. Cooperation contracts signed with four companies]. Ministry of Digital Transformation of Ukraine, 2022-10-30.

https://thedigital.gov.ua/news/army/mikhaylo-fedorov-armiyu-droniv-posilyat-udarni-bpla-ukrainskogo-virobnitstva-pidpisali-kontrakti-pro-spivpratsyu-z-chotirma-kompaniyami

Brave1 defense tech cluster. Brave1, 2026-07-13.

https://brave1.gov.ua/en/

Diia - information about the project Diia. Digital State UA, 2026-04-10.

https://digitalstate.gov.ua/projects/govtech/diia

Brave1 - information about the project Brave1. Digital State UA, 2026-01-20.

https://digitalstate.gov.ua/projects/tech/brave1

Fedorov Becomes Defense Minister: From Digital Ukraine to Drone Warfare - UNITED24 Media. UNITED24 Media, 2026-01-14.

https://united24media.com/war-in-ukraine/ukraines-new-defense-minister-is-the-mind-behind-the-countrys-digital-transformation-15021

Ukraine's Digital Transformation: Innovation for Resilience | Harvard Kennedy School. Harvard Kennedy School CID, 2025-03-01.

https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience

Ukraine: Digital Innovation and Wartime Resilience. Stanford Social Innovation Review, 2023-01-01.

https://ssir.org/articles/entry/wartime_digital_resilience

The IT Army of Ukraine - Release of OP 35 | Australian Army Research Centre (AARC). Australian Army Research Centre, 2026-04-22.

https://researchcentre.army.gov.au/library/land-power-forum/it-army-ukraine-release-op-35

The Future of Drones in Ukraine: A Report from the DIU-Brave1 Warsaw Conference | Center for Security and Emerging Technology. CSET Georgetown, 2023-10-01.

https://cset.georgetown.edu/article/the-future-of-drones-in-ukraine-a-report-from-the-diu-brave1-warsaw-conference/

米哈伊洛·费多罗夫 [Mykhailo Fedorov] - 维基百科，自由的百科全书. Wikipedia zh, 2026-01-14.

https://zh.wikipedia.org/zh-hans/%E7%B1%B3%E5%93%88%E4%BC%8A%E6%B4%9B%C2%B7%E8%B2%BB%E5%A4%9A%E7%BE%85%E5%A4%AB

乌克兰数字化转型部长：乌克兰将开发空对空作战无人机 [Ukraine's Minister of Digital Transformation: Ukraine will develop air-to-air combat drones]. Voice of America Chinese, 2022-12-28.

https://www.voachinese.com/a/ukraine-dronzes-20221228/6895952.html

Ukraine's 34-year-old defence minister has overhauled drone strategy: will he be the relief pitcher? Yonhap News, 2026-01-21.

https://www.yna.co.kr/view/AKR20260121165800109

Four turning points in the Russia-Ukraine war made by satellite communications and drones. Weekly Chosun, 2026-05-01.

https://weekly.chosun.com/news/articleView.html?idxno=50981

Starlink, the new variable in the Ukraine-Russia drone war: Ukraine and SpaceX respond by blocking Russia. Drone Journal, 2026-02-05.

https://www.dronejournal.net/news/articleView.html?idxno=273

Countering russian drones: How to complete Starlink verification to operate terminals in Ukraine | MoD News. Ministry of Defence of Ukraine, 2026-02-02.

https://mod.gov.ua/en/news/countering-russian-drones-how-to-complete-starlink-verification-to-operate-terminals-in-ukraine

Drone Line: implementing a new warfare doctrine | MoD News. Ministry of Defence of Ukraine, 2026-04-09.

https://mod.gov.ua/en/news/drone-line-implementing-a-new-warfare-doctrine

UAVs lead the way, DELTA remains a challenge: how service members train in the Army+ app | MoD News. Ministry of Defence of Ukraine, 2026-02-02.

https://mod.gov.ua/en/news/ua-vs-lead-the-way-delta-remains-a-challenge-how-service-members-train-in-the-army-app

Service members will receive air threat alerts in the DELTA Mobile app | MoD News. Ministry of Defence of Ukraine, 2026-03-10.

https://mod.gov.ua/en/news/service-members-will-receive-air-threat-alerts-in-the-delta-mobile-app

Mykhailo Fedorov: Ukraine is boosting battlefield effectiveness and calling on the EU to strengthen defence support | MoD News. Ministry of Defence of Ukraine, 2026-03-10.

https://mod.gov.ua/en/news/mykhailo-fedorov-ukraine-is-boosting-battlefield-effectiveness-and-calling-on-the-eu-to-strengthen-defence-support

Estonia prepares a new assistance package for Ukraine, encompassing drones and counter-drone capabilities | MoD News. Ministry of Defence of Ukraine, 2026-02-03.

https://mod.gov.ua/en/news/estonia-prepares-a-new-assistance-package-for-ukraine-encompassing-drones-and-counter-drone-capabilities

Ukraine and Germany step up efforts to accelerate the delivery of air defence munitions | MoD News. Ministry of Defence of Ukraine, 2026-06-10.

https://mod.gov.ua/en/news/ukraine-and-germany-step-up-efforts-to-accelerate-the-delivery-of-air-defence-munitions

DELTA | MoD News. Ministry of Defence of Ukraine, 2024-05-22.

https://mod.gov.ua/en/news/dou-day-2024-conference-ukrainian-developers-presented-delta-combat-system-1

"Army of Drones Bonus" program delivers results: nearly 820,000 russian targets hit in 2025, says Mykhailo Fedorov | MoD News. Ministry of Defence of Ukraine, 2026-01-26.

https://mod.gov.ua/en/news/army-of-drones-bonus-program-delivers-results-nearly-820-000-russian-targets-hit-in-2025-says-mykhailo-fedorov

Ukraine's DELTA Combat System Passes NATO Audit | MoD News. Ministry of Defence of Ukraine, 2024-07-17.

https://mod.gov.ua/en/news/in-ukraine-for-the-first-time-the-cyber-security-of-the-combat-system-was-tested-according-to-nato-standards

Invest in Ukraine's defense industry | MoD News. Ministry of Defence of Ukraine, 2024-11-12.

https://mod.gov.ua/en/news/ministry-of-defense-urges-european-partners-to-invest-in-ukraine-s-defense-industry-including-through-frozen-russian-assets

The Ministry of Defence contracted a record number of multirotor drones for the front | MoD News. Ministry of Defence of Ukraine, 2026-03-11.

https://mod.gov.ua/en/news/the-ministry-of-defence-contracted-a-record-number-of-multirotor-drones-for-the-front

Combat brigades received 500,000 items, including drones, ground robotic systems, and other equipment, through DOT-Chain Defence | MoD News. Ministry of Defence of Ukraine, 2026-03-11.

https://mod.gov.ua/en/news/combat-brigades-received-500-000-items-including-drones-ground-robotic-systems-and-other-equipment-through-dot-chain-defence

White list for Starlink terminals: How to find the KIT number and UTID identifier to complete verification and use your terminal in Ukraine | MoD News. Ministry of Defence of Ukraine, 2026-02-03.

https://mod.gov.ua/en/news/white-list-for-starlink-terminals-how-to-find-the-kit-number-and-utid-identifier-to-complete-verification-and-use-your-terminal-in-ukraine

Brave1 Defense Tech Valley 2026: Ukraine is shaping a new global standard for defense solutions | MoD News. Ministry of Defence of Ukraine, 2026-04-09.

https://mod.gov.ua/en/news/brave1-defense-tech-valley-2026-ukraine-is-shaping-a-new-global-standard-for-defense-solutions

Over 10 military units are now equipped with a Ukrainian AI-powered turret capable of destroying UAVs with a single button press | MoD News. Ministry of Defence of Ukraine, 2026-05-09.

https://mod.gov.ua/en/news/over-10-military-units-are-now-equipped-with-a-ukrainian-ai-powered-turret-capable-of-destroying-ua-vs-with-a-single-button-press

«Інформацію потрібно вносити лише один раз»: як вчителька з Тернопільщини допомогла 20 школам перейти на Мрію ["The information only has to be entered once": how a teacher from the Ternopil region helped 20 schools move to Mriia]. Ministry of Digital Transformation of Ukraine, 2026-07-10.

https://thedigital.gov.ua/news/education/informatsiiu-potribno-vnosyty-lyshe-odyn-raz-iak-vchytelka-z-ternopilshchyny-dopomohla-20-shkolam-pereyty-na-mriiu

Досліджуємо українське IT: долучайтеся до опитування в межах IT Research Ukraine 2026 [Researching Ukrainian IT: join the survey as part of IT Research Ukraine 2026]. Ministry of Digital Transformation of Ukraine, 2026-07-09.

https://thedigital.gov.ua/news/business/doslidzuyemo-ukrayinske-it-doluchaytesia-do-opytuvannia-v-mezakh-it-research-ukraine-2026

Де є енергонезалежний інтернет? Мінцифра та Дія створюють національну мапу xPON-мереж [Where is there energy-independent internet? The Ministry of Digital Transformation and Diia are building a national map of xPON networks]. Ministry of Digital Transformation of Ukraine, 2026-07-09.

https://thedigital.gov.ua/news/technologies/de-ye-enerhonezaleznyy-internet-mintsyfra-ta-diia-stvoriuiut-natsionalnu-mapu-xpon-merez

Дія.City в регіонах: де технологічні компанії сплатили найбільше податків у 2025 році [Diia.City in the regions: where technology companies paid the most taxes in 2025]. Ministry of Digital Transformation of Ukraine, 2026-07-08.

https://thedigital.gov.ua/news/regions/diiacity-v-rehionakh-de-tekhnolohichni-kompaniyi-splatyly-naybilshe-podatkiv-u-2025-rotsi

Оцифровуємо українські рукописи: хто переміг в AI-челенджі Handwritten to Data [Digitising Ukrainian manuscripts: who won the Handwritten to Data AI challenge]. Ministry of Digital Transformation of Ukraine, 2026-07-08.

https://thedigital.gov.ua/news/shtuchnyy-intelekt/otsyfrovuyemo-ukrayinski-rukopysy-khto-peremih-v-ai-chelendzi-handwritten-to-data

Від навчання до реального оферу: Мінцифра запустила Кар'єрну студію із симулятором співбесіди на Дія.Освіта [From training to a real job offer: the Ministry of Digital Transformation has launched a Career Studio with an interview simulator on Diia.Education]. Ministry of Digital Transformation of Ukraine, 2026-07-08.

https://thedigital.gov.ua/news/education/vid-navchannia-do-realnoho-oferu-mintsyfra-zapustyla-karyernu-studiiu-iz-symuliatorom-spivbesidy-na-diiaosvita

Штучний інтелект у ЦНАПах: яким буде майбутнє державних сервісів [Artificial intelligence in the Administrative Service Centres: what the future of public services will look like]. Ministry of Digital Transformation of Ukraine, 2026-07-03.

https://thedigital.gov.ua/news/progress/shtuchnyy-intelekt-u-tsnapakh-iakym-bude-maybutnye-derzavnykh-servisiv

Україна та Естонія створюють AI-рішення для держави майбутнього: на міжнародному хакатоні визначили переможців [Ukraine and Estonia are building AI solutions for the state of the future: winners named at an international hackathon]. Ministry of Digital Transformation of Ukraine,

2026-07-03.

https://thedigital.gov.ua/news/shtuchnyy-intelekt/ukrayina-ta-estoniia-stvoriuiut-ai-rishennia-dlia-derzavy-maybutnyoho-na-miznarodnomu-khakatoni-vyznachyly-peremoztsiv

Італія очолила Талліннський механізм: країна виділить ще €1 млн на кіберзахист України [Italy has taken the lead of the Tallinn Mechanism: the country will allocate a further €1 million for Ukraine's cyber defence]. Ministry of Digital Transformation of Ukraine, 2026-07-01.

https://thedigital.gov.ua/news/technologies/italiia-ocholyla-tallinnskyy-mekhanizm-krayina-vydilyt-shche-eur1-mln-na-kiberzakhyst-ukrayiny

Позиція Мінцифри щодо маніпулятивних заяв про проєкт Дія.City [The Ministry of Digital Transformation's position on manipulative claims about the Diia.City project]. Ministry of Digital Transformation of Ukraine, 2026-06-30.

https://thedigital.gov.ua/news/business/pozytsiia-mintsyfry-shchodo-manipuliatyvnykh-zaiav-pro-proyekt-diiacity

Цифровізуємо державні сервіси та реєстри швидше, простіше й дешевше: Мінцифра провела форум Дія.Engine [Digitising public services and registries faster, more simply, and more cheaply: the Ministry of Digital Transformation held the Diia.Engine forum]. Ministry of Digital Transformation of Ukraine, 2026-06-22.

https://thedigital.gov.ua/news/technologies/tsyfrovizuyemo-derzavni-servisy-ta-reyestry-shvydshe-prostishe-y-deshevshe-mintsyfra-provela-forum-diiaengine

Від чинних документів до генерації нових ключів: як і коли відбудеться перехід на новий стандарт е-підпису [From existing documents to the generation of new keys: how and when the transition to the new e-signature standard will take place]. Ministry of Digital Transformation of Ukraine, 2026-06-25.

https://thedigital.gov.ua/news/technologies/vid-chynnykh-dokumentiv-do-heneratsiyi-novykh-kliuchiv-iak-i-koly-vidbudetsia-perekhid-na-novyy-standart-e-pidpysu

Трансформація Сил оборони України: перший етап | Михайло Федоров [The transformation of Ukraine's Defence Forces: stage one | Mykhailo Fedorov]. Телеканал Рада, 2026-06-17.

https://www.youtube.com/watch?v=ytv97owmMn0

ФЕДОРОВ. ЕКСКЛЮЗИВ. Як закінчиться війна, зарплати 300 тис. в армії, нові контракти та демобілізація [FEDOROV. EXCLUSIVE. How the war will end, 300,000-hryvnia army salaries, new contracts, and demobilisation]. ТСН, 2026-06-16.

https://www.youtube.com/watch?v=cTobgzbBMMY

ЦЕ ІНТЕРВ'Ю Федорова НАРОБИЛО такого ГАЛАСУ! На нас чекають капітальні ЗМІНИ в ЗСУ. Ось що готується [THIS INTERVIEW with Fedorov caused such an UPROAR! Sweeping CHANGES await the Armed Forces. Here is what is being prepared]. Ми - Україна, 2026-06-18.

https://www.youtube.com/watch?v=3RjW0qVk1S4

Федоров сказав КОЛИ БУДЕ ДЕМОБІЛІЗАЦІЯ! Ексклюзивно про ТРАНСФОРМАЦІЮ Сил оборони [Fedorov has said WHEN DEMOBILISATION WILL COME! Exclusively on the TRANSFORMATION of the Defence Forces]. УНІАН TV, 2026-06-17.

https://www.youtube.com/watch?v=fXtp18GwIjg

ПОВНА ВІДСТАВКА УРЯДУ! Є лише ОДНА СВІТЛА ПЛЯМА. Федоров ПІШОВ ПРОТИ СИРСЬКОГО. Підстава БАНКОВОЇ [THE ENTIRE GOVERNMENT RESIGNS! There is only ONE BRIGHT SPOT. Fedorov has GONE AGAINST SYRSKYI. Bankova's setup]. Фабрика новин, 2026-07-10.

https://www.youtube.com/watch?v=kE4-WiKxx2E

Як ДІЯти далі? Михайло Федоров | Business Breakfast із Володимиром Федоріним [How to ACT next? Mykhailo Fedorov | Business Breakfast with Volodymyr Fedorin]. Forbes Ukraine, 2024-02-07.

https://www.youtube.com/watch?v=1eSQGaYyLS0

Михайло Федоров: «Дія»: вибори та перепис населення, кібервійна, листування з Маском | Інтерв'ю [Mykhailo Fedorov: "Diia": elections and the census, cyberwar, correspondence with Musk | Interview]. Радіо Свобода, 2023-02-04.

https://www.youtube.com/watch?v=AT24xJqQ-IA

Інновації, які змінюють хід війни: Михайло Федоров про дрони, РЕБ та Brave1 | Подкаст Слон [Innovations that are changing the course of the war: Mykhailo Fedorov on drones, electronic warfare, and Brave1 | The Slon podcast]. Дія, 2024-01-12.

https://www.youtube.com/watch?v=63aDfQlslKU

ЦІЄЇ МИТІ! ФЕДОРОВ РОЗМАЗАВ РОСІЯН! ФІНАЛЬНИЙ УДАР ЗСУ: РФ У ВОГНІ! ПУТІН АЖ ВТРАТИВ ДАР МОВИ! [THIS MOMENT! FEDOROV HAS CRUSHED THE RUSSIANS! THE ARMED FORCES' FINAL BLOW: RUSSIA IS ABLAZE! PUTIN HAS BEEN LEFT SPEECHLESS!]. СПЕЦКОР | Новини 2+2, 2026-07-12.

https://www.youtube.com/watch?v=U4OddMn3eQw

Ukraine's New War Cabinet Explained: What Changes Now? (Budanov, Fedorov, Energy Crisis). KI Insights, 2026-01-28.

https://www.youtube.com/watch?v=5z6NhcHIf5Q

Ukraine's Defense Minister: Crimea Becomes an Island | Army Revolution | How Ukraine Changes War. PEICHEV, 2026-06-17.

https://www.youtube.com/watch?v=oN3zPUlnFWc

СТЕРНЕНКО | УДАРИ ПО РОСІЇ | ПРО "СКЕЛЮ" | РАДНИК У ФЕДОРОВА | Ремовська [STERNENKO | STRIKES ON RUSSIA | ON "SKELIA" | ADVISER TO FEDOROV | Removska]. Суспільне Новини, 2026-07-11.

https://www.youtube.com/watch?v=IfjIS883a7g

ФЕДОРОВ: СТОСУНКИ З СИРСЬКИМ/ЧУТКИ ПРО ВІДСТАВКУ/КОРУПЦІЙНІ КЛАНИ В ОБОРОНЦІ [FEDOROV: RELATIONS WITH SYRSKYI / RESIGNATION RUMOURS / CORRUPT CLANS IN THE DEFENCE SECTOR]. PRESSING, 2026-06-17.

https://www.youtube.com/watch?v=EWuI8WYOfF8

ВЕЛИКЕ ІНТЕРВ'Ю З МИХАЙЛОМ ФЕДОРОВИМ | Міністерство оборони України, дрони, технології та майбутнє [A LONG INTERVIEW WITH MYKHAILO FEDOROV | The Ministry of Defence of Ukraine, drones, technology, and the future]. УП UKRAINIAN TRUTH, 2026-06-19.

https://www.youtube.com/watch?v=p-Js4_cbkpE

Після ТЕРОРУ у Києві ФЕДОРОВ озвучив ГАРНІ НОВИНИ! Ця ЗВІСТКА СКОЛИХНУЛА СВІТ. Цього Путін І БОЯВСЯ [After the TERROR in Kyiv, FEDOROV announced GOOD NEWS! This REPORT SHOOK THE WORLD. This is exactly what Putin FEARED]. 24 Канал онлайн, 2026-07-03.

https://www.youtube.com/watch?v=Gvm4NZ35cHM

ТЕРМІНОВА ЗВІСТКА від ФЕДОРОВА! Ось, що ОГОЛОСИЛИ українцям. СТЕРНЕНКО ПОЯСНИВ, що чекати [URGENT NEWS from FEDOROV! Here is what was ANNOUNCED to Ukrainians. STERNENKO EXPLAINED what to expect]. 24 Канал, 2026-03-11.

https://www.youtube.com/watch?v=zVIILiUj6sQ

ФЕДОРОВ вразив зверненням до українців! Такого успіху ще не було. АРАБСЬКИЙ світ відповів КИЄВУ [FEDOROV stunned with an address to Ukrainians! There has never been success like this. The ARAB world has answered KYIV]. 24 Канал, 2026-04-02.

https://www.youtube.com/watch?v=vP1KN2DstD4

ЩОЙНО! НАД УКРАЇНОЮ ЗАКРИЛИ НЕБО! ФЕДОРОВ ЦЕ ЗРОБИВ: РІШЕННЯ ЯКЕ ПЕРЕВЕРНУЛО ВСЕ! | ПРЯМО ЗАРАЗ [JUST IN! THE SKY OVER UKRAINE HAS BEEN CLOSED! FEDOROV DID IT: THE DECISION THAT CHANGED EVERYTHING! | RIGHT NOW]. УКРАЇНА СЬОГОДНІ, 2026-02-27.

https://www.youtube.com/watch?v=0UYBFYulNzk

Те, що задумав Федоров вражає. Повна зміна системи мобілізації через ТЦК | Максим Костецький [What Fedorov has planned is striking. A complete overhaul of the mobilisation system through the recruitment centres | Maksym Kostetskyi]. Radio NV, 2026-04-24.

https://www.youtube.com/watch?v=MQRiiiWjRS0

Федоров як дзеркало Зеленського Чому військових почали допитувати Вони ХОЧУТЬ Вибори в Дії [Fedorov as Zelensky's mirror. Why service members have begun to be interrogated. They WANT elections through Diia]. Dana Yarova, 2026-02-16.

https://www.youtube.com/watch?v=OQcOmxjz3S8

ФЕДОРОВ: BRAVE1 - НАЙБІЛЬШИЙ АНГЕЛЬСЬКИЙ ІНВЕСТОР УКРАЇНИ | ДІПСТРАЙКИ, ЗЕНІТНІ ДРОНИ, МАШИННИЙ ЗІР [FEDOROV: BRAVE1 IS UKRAINE'S LARGEST ANGEL INVESTOR | DEEP STRIKES, ANTI-AIRCRAFT DRONES, MACHINE VISION]. Army TV - Ukrainian military channel, 2025-09-22.

https://www.youtube.com/watch?v=ePBwCKgrdrg

Pistorius y Fédorov a 30 km del frente: Alemania entra en Brave1 y el fracaso de los planes de Rusia [Pistorius and Fedorov 30 km from the front: Germany joins Brave1 and the failure of Russia's plans]. UATV Español, 2026-06-23.

https://www.youtube.com/watch?v=zAS7t-oO5HE

100 днів Федорова / Антидроновий купол / Хаос в малій ППО - ЄЛІЗАРОВ | УП. Інтерв'ю [Fedorov's 100 days / The counter-drone dome / Chaos in short-range air defence - YELIZAROV | Ukrainska Pravda. Interview]. Ukrainska Pravda, 2026-04-30.

https://www.youtube.com/watch?v=nR3SYLP1CfE

PISTORIUS I FEDOROW BLISKO FRONTU: rozmowa o BRAVE1 MID-STRIKE'ach i ZMIANACH we WSPÓŁCZESNEJ WOJNIE [PISTORIUS AND FEDOROV NEAR THE FRONT: a conversation on BRAVE1, MID-STRIKES, and the CHANGES IN MODERN WAR]. UATV po polsku, 2026-06-07.

https://www.youtube.com/watch?v=BL4d96Uw3O0

Олександр Борняков про майбутнє мінцифри, експорт зброї, Brave1, виробництво чипів та українську LLM [Oleksandr Bornyakov on the future of the Ministry of Digital Transformation, arms exports, Brave1, chip manufacturing, and a Ukrainian LLM]. УТ-2, 2026-01-27.

https://www.youtube.com/watch?v=BI0ZWuLFXQM

Support This AI Library Book

If this book was useful, you can support future translations, public editions, and open AI knowledge projects through PayPal.

PayPal

https://paypal.me/kimkjj

Scan the QR code or open the link above.