Time.- 14.11.2023
Vera Bergengruen

Ukraine’s ‘Secret Weapon’ Against russia Is a Controversial U.S. Tech Company

«Секретна зброя» України проти росії — суперечлива технологічна компанія США

Старша кореспондентка журналу «Time» Віра Бергенгруен присвятила статтю висвітленню роботи компанії "Clearview AI" в Україні. Для Хоана Тон-Тата, генерального директора австралійської компанії "Clearview AI", початок війни в Україні став нагодою продемонструвати цінність програмного забезпечення його компанії для розпізнавання осіб. За даними компанії, за 20 місяців з початку війни Україна провела щонайменше 350 000 пошукових запитів у базі даних "Clearview". Заступник міністра внутрішніх справ України Леонід Тимченко зауважує, що у Національній поліції України цю технологію використовують понад п'ять відділів. Начальник відділу інформаційних технологій Державного бюро розслідувань України Андрій Кулалаєв заявив, що впровадження "Clearview" стало важливим кроком у розвитку правоохоронного відомства. Віцепрем'єр-міністр - міністр цифрової трансформації України Михайло Федоров зазначив, що "Clearview AI" готовий допомогти побудувати цифрову інфраструктуру України, яка буде заснована на новітніх технологіях.

https://time.com/6334176/ukraine-clearview-ai-russia/

Leonid Tymchenko spent the first month of Russia’s invasion sitting in his dark government office after curfew. Unable to go home, Ukraine's Deputy Minister of Internal Affairs scrolled through Telegram, looking at thousands of videos and images of advancing Russian soldiers. When Tymchenko was offered a chance to test a new facial-recognition tool, he uploaded some of the photos to try it out.

He could not believe the results. Every time Tymchenko added a photo of a Russian soldier, the software, made by the American facial-recognition company Clearview AI, seemed to come back with an exact hit, linking to pages that revealed the soldier’s name, hometown, and social-media profile. Even when he uploaded grainy photos of dead soldiers, some with their eyes closed or their faces partially burned, the software was often able to identify the person. "Every day we identified hundreds of Russians who came to Ukraine with weapons,” Tymchenko tells TIME in a video interview from his office in Kyiv.

In the ongoing war against Russia, Clearview has become the Ukrainian government’s “secret weapon,” Tymchenko says. More than 1,500 officials across 18 Ukrainian government agencies are using the facial-recognition tool, which has helped them identify more than 230,000 Russian soldiers and officials who have participated in the military invasion. Ukraine's use of Clearview has rapidly expanded beyond identifying Russian troops on their soil. The nation has come to rely on the private U.S. tech company, which has just 35 employees, to assist with a vast range of wartime tasks, many of which have not been previously reported, according to interviews with officials from half a dozen government agencies, law-enforcement officers, Ukrainian analysts, and Clearview executives.

Ukrainian officials have used Clearview to detect infiltrators at checkpoints, process citizens who lost their IDs, identify and prosecute members of pro-Russia militias and Ukrainian collaborators, and even to locate more than 190 abducted Ukrainian children who were transported across the border to live with Russian families. Ukraine has run at least 350,000 searches of Clearview’s database in the 20 months since the outbreak of the war, according to the

company. “The volume is insane,” Clearview AI’s CEO, Hoan Ton-That, tells TIME. “Using facial recognition in war zones is something that's going to save lives.”

The partnership between the Ukrainian government and the American tech company has been a boon to both sides. Ukraine's tech-savvy government was desperate to use any tools it could find to defend itself against a larger invading army. And Clearview was eager to provide its tools for free—which it is still doing now—to showcase an effective use for its facial-recognition technology, which has been maligned for harvesting its data by scraping billions of public photographs from the Internet, allegedly violating privacy rights, and selling access to law enforcement.

Ukraine’s extensive use of Clearview raises complicated questions about when and how controversial or invasive technology should be used in wartime, and how far digital privacy-rights should extend in the midst of an armed conflict. To proponents, the value of the technology is worth the cost: if you can use a digital tool to identify alleged war criminals or find abducted children, why wouldn't you? But human-rights groups and privacy advocates warn that Ukraine may find it difficult to rein in its use of Clearview when the war is over. Those critics accuse the company of attempting to harness the conflict to burnish its image. And Ukraine indicates it’s making plans to embed Clearview tools in the country's long-term security infrastructure, which experts say could lead to mass surveillance or other abuses. Ukrainian civil-society groups say this might also jeopardize the nation’s bid to join the European Union, several of whose member states have deemed Clearview illegal, issued steep fines, and attempted to ban it from collecting the faces of its citizens.

"I don't want Ukrainian authorities to have the reputation of the guys who use very intrusive and abusive services, which could [later] be used to persecute activists or civil society,” says Tetiana Avdieieva, a human-rights lawyer in Kyiv and legal counsel for Digital Security Lab Ukraine. “That's very dangerous."

For Hoan Ton-That, the 35-year-old Australian CEO of Clearview AI, the outbreak of the war in Ukraine was an opportunity to demonstrate the value of his company’s facial-recognition software. "It's a technology that shines and only really is appreciated in times of crisis," he explains in a recent video interview from New York. "I think people really understand it when it's their life on the line or someone close to them."

Founded in 2017 with the backing of a group of investors including Peter Thiel, Clearview initially operated in relative secrecy. For several years, it built up the world’s largest database of human faces by scraping the Internet and running them through a facial-recognition algorithm that it says can identify people with 99.85% accuracy. (Clearview’s library of images of people’s faces has grown to 40 billion—an average of five images for every person on Earth, and a 400% increase since the start of the war, Ton-That tells TIME.) By 2018, Clearview was quietly selling access to its database to a host of eager government clients, which grew to more than 600 law enforcement agencies, including U.S. Immigrations and Customs Enforcement (ICE) and the FBI.

But in 2020, Clearview became something of a tech pariah after the company's existence, the size of its database, and its use by law enforcement were revealed by a New York Times investigation. Critics slammed Clearview as “creepy,” “terrifying,” and “dystopian” in the press. Since then, it has been hit with a wave of lawsuits, fines, and cease-and-desist orders from companies whose data it scraped. Ton-That, an Australian programmer and former model who tried his luck with several failed iPhone games before landing on facial recognition, was lambasted for his alleged ties to far-right figures. Clearview was accused of violating data-

privacy laws in the EU, deemed illegal in Austria, France, Greece, Italy, and the U.K, and largely prohibited from selling access to its database to U.S. private companies.

"We were attacked by a lot of different privacy groups," acknowledges Ton-That, who sought to highlight Clearview's potential use for the public good—finding child abusers, rescuing human-trafficking victims, even identifying the rioters who attacked the U.S. Capitol in 2021. When Russia invaded Ukraine, Ton-That mined his network for contacts in the Ukrainian government. At the time, Clearview's database already contained more than two billion images it had previously scraped from Russian social-media sites like VKontakte. "The thing that makes it so much better than DNA and fingerprints is that you have those for your own citizens," Ton-That says, "but you don't have a database of your enemies."

In a letter addressed to Ukrainian officials just days after the invasion began, Ton-That offered free training and access to Clearview. The technology "may be of help during this time of terrible conflict," he wrote, "to prevent harm, save innocent people and protect lives." Ton-That first demonstrated the tool to a handful of Ukrainian defense officials over Zoom in early March 2022. Two weeks later, he was leading a training session for 85 members of Ukraine's National Police, aided by a translator. Halfway through the session, one of them shared his screen to show how he had already identified two dead Russian soldiers, Ton-That recalls.

More Ukrainian agencies began to request access: the state Border Guard Service, the Crimean Prosecutor's Office, the State Bureau of Investigations. When Ton-That visited Ukraine in April, officials rolled out the red carpet, showering him with gifts: bottles of Crimean wine and Ukrainian vodka, rare commemorative war stamps, decorative military medals, and letters of gratitude that he later had framed. "It was like a parallel universe," he says. "It's inconceivable to them that someone wouldn't like this technology."

***

The Ukrainians found a variety of uses for Clearview. To counteract Russian propaganda denying that their troops were suffering heavy casualties, Ukraine's Ministry of Internal Affairs set up a website called Poter.net, the Russian term for "No Losses," and posted a searchable database with the names of dead Russian soldiers that Clearview helped identify, linking to open-source information from Russian social media so their families could find them. (As of Nov. 13, there were more than 71,000 Russians identified on the site.) The facial-recognition technology was so effective, Tymchenko says, that Russian troops began wearing masks and face coverings, even in sweltering summer months. "They wore them despite the heat because they now knew that we could identify them," Tymchenko says, "and they knew their life wouldn't be the same, that they would never be able to visit normal countries after this activity."

Clearview accelerated Ukraine's process of collecting evidence to prosecute alleged war criminals, which previously relied on sifting through witness testimony and other data to identify them, Ukrainian officials say. Igor Ponochovnyi, the head of the Prosecutor's Office for Crimea, says his office has used advanced open-source investigations to prosecute war crimes in occupied territories since 2014. But Clearview was something new. For years, it had been impossible for Ukrainian prosecutors to verify the identities of the low-ranking members who made up the bulk of the Crimean Self-Defense forces, an armed militia that has helped Russia occupy the peninsula. Using Clearview, the prosecutor's office quickly identified more than 70, allowing authorities to arrest them when they entered Ukrainian territory. "We realized we needed to use Clearview on a regular basis for our activities," Ponochovnyi tells TIME.

The prosecutor's office also found another use for the tool: identifying Ukrainian children who were forcibly taken from orphanages and temporary shelters, many to be reportedly adopted by Russian families or sent to "re-education" camps. Using images Clearview took from Russian social-media, like family photos, Ponochovnyi says his office was able to identify 198 of the missing children and confirm that they were in Russia or Russian-occupied territories, as well as identify their adoptive parents.

"The implementation of Clearview became an important step in the development of our law-enforcement agency," says Andrii Kulalayev, the head of the IT Department at Ukraine's State Bureau of Investigation, citing examples where Clearview helped identify Ukrainian business owners who continued working with Russian companies after the invasion. Kulalayev also notes a number of cases unrelated to the war, like the identification of drug dealers. "We continue to actively use Clearview and explore new possibilities for its application," he says. "This tool has become an integral part of our work."

There are no signs that the Ukrainian government is eager to wind down its use of Clearview when the war is over. That's part of what alarms human-rights groups and privacy advocates inside and outside the country, who warn that Ukraine has outdated privacy laws which could fail to curtail the potential surveillance of citizens without proper justification. "The deep collaboration on the state level, extending into the peacetime systems, really concerns me," says Avdieieva, the human rights lawyer in Kyiv who serves as the legal counsel for Digital Security Lab Ukraine. There is no way to guarantee that it won't fall into the hands of bad actors, Avdieieva adds, or even Russians who might capture access to digital tools along with physical infrastructure as the war continues.

There are also unanswered questions about how the tool is being used and how long the data collected is being stored, which Ukrainian officials have been reluctant to answer, advocates say. "We're basically trying to justify the breach of personal data all around the globe by saying that at least in an armed conflict it might be useful," says Avdedieva.

How Ukraine uses facial recognition and other digital tools "once the fog of war dissipates," says Juan Espindola, a researcher at the National Autonomous University of Mexico (UNAM), will have an impact on how other countries decide to treat citizens' privacy during a time of crisis. "It's a slippery slope," Espindola says. Government officials "will always find a way to justify an ever-expanding use of these tools when they're at war. But then it becomes a never-ending war. Even if the invasion is over, there will always be the threat."

Indeed, Ukrainian officials have signaled they intend to expand their relationship with the company. "Clearview AI is ready to help build the digital infrastructure of Ukraine, which will be based on the latest technologies," Mykhailo Fedorov, Ukraine's influential Minister of Digital Transformation, announced in a Telegram post on April 13 next to a photo of himself and Ton-That in Kyiv. Fedorov named customs and banking as two areas the company's tech could be integrated further.

For his part, Ton-That is considering opening a Clearview AI office in Kyiv to strengthen the partnership and continue developing the company's products. He believes the technology's use in Ukraine will convince critics that a facial-recognition company often derided as "creepy" is a force for good. "Future conflicts will use facial recognition a lot," says Ton-That. "War's a terrible thing, right? If these wars didn't exist, then people wouldn't need something like Clearview."