Time.- 18.04.2022
Vera Bergengruen

How Ukraine Is Crowdsourcing Digital Evidence of War Crimes

Як Україна займається краудсорсингом цифрових доказів військових злочинів

З самого початку російського вторгнення українські офіційні особи, юристи та правозахисні групи намагалися розробити нові способи систематизації та перевірки величезної кількості відео- та фотоматеріалів, а також свідчень очевидців про злочинну поведінку російських сил. Розроблені програми, чат-боти та вебсайти класифікують різні види військових злочинів та порушень прав людини, і всі вони потрапляють до єдиної централізованої бази даних, створеної Генеральною прокуратурою України. Міністр цифрової трансформації України М. Федоров, каже, що збирання та використання в країні, так званих, «громадянських доказів» - це ще один спосіб, за допомогою якого Україна веде сучасну війну.
https://time.com/6166781/ukraine-crowdsourcing-war-crimes/

It all looks like a game at first. Verified users of Ukraine's government mobile app are greeted with options illustrated by icons of military helmets and targets. An automated prompt helps you report Russian troop movements in your area, and rewards you with a flexed-arm emoji. "Remember," the message says. "Each of your shots in this bot means one less enemy." Another option on the menu, illustrated by a droplet of blood, prompts Ukrainians to report and submit footage of war crimes in places now associated with horrific atrocities: Bucha, Irpin, Gostomel.

This chatbot, created by Ukraine's Digital Ministry and dubbed "e-Enemy," is one of half a dozen digital tools the government has set up to crowdsource and corroborate evidence of alleged war crimes. Since the start of the invasion, Ukrainian officials, lawyers and human-rights groups have scrambled to design new ways to catalogue and verify reams of video, photo and eyewitness accounts of criminal behavior by Russian forces. Ukraine has adapted popular government apps to allow citizens to document damage to their homes, used facial-recognition software to identify Russian military officials in photos, and rolled out new tools to guide users through the process of geo-tagging and time-stamping their footage in hopes it may help authorities hold the perpetrators responsible.

The result is a systematic effort unlike any in the history of modern warfare, experts say. Crowdsourcing digital proof of war crimes from witnesses has been done in other conflicts, but "the use of open-source information as evidence in the case of Ukraine may be at altogether a different level," says Nadia Volkova, director of the Ukrainian Legal Advisory Group and a member an alliance of Ukrainian human-rights organizations called the 5AM coalition. Named for the time the Russian invasion began on Feb. 24, the group trains volunteers to document eyewitness testimony, and to collect, preserve and verify evidence in accordance with international protocols. The goal is not only to achieve justice for the victims, Volkova says, "but also contribute to the development of international law and the use of open-source information as evidence in complex cases."

The apps, chatbots and websites designed by Ukrainian officials categorize different kinds of war crimes and human-rights violations and all feed into one centralized database set up by the office of Ukraine's Prosecutor General. These include the killing or injury of civilians by Russians; physical violence or imprisonment; denial of medical care; looting; and seizure of property by occupying forces. Verified users are prompted to report violence against medical staff or religious clergy; damage to civilian infrastructure; and the use of military equipment in residential areas. Reports from chatbots like "e-Enemy" are also shared with the military, and

have led Ukrainian forces to mount successful attacks on Russian positions, according to Ukraine's Security Service.

Ukrainians are rallying to the cause. A website set up by the office of Ukraine's Prosecutor General, warcrimes.gov.ua, has received more than 10,000 submissions of detailed evidence from citizens, an official told TIME. The government's efforts are supported by a legion of outside human-rights groups, citizen sleuths, cyber-volunteers, retired military officials, journalists, and open-source analysts with experience documenting this kind of proof in previous conflicts.

What all this will yield is still unclear. International war-crimes cases are notoriously difficult to prosecute. Successful efforts are typically built on traditional forensic evidence, witness testimonies and documents. But Ukrainian officials say the purpose of using digital tools to crowdsource evidence of Russian atrocities extends far beyond a war-crimes trial in The Hague. They see it as a defense against a flood of Russian disinformation, including claims from high-ranking Kremlin officials that the horrors from Bucha or Mariupol are "fake" or staged. And they believe it will create a historical record that will help hold the guilty responsible and win restitution for the victims.

Mykhailo Fedorov, Ukraine's Minister of Digital Transformation, says the country's collection and use of so-called "citizen evidence" is another way that Ukraine is reinventing modern warfare. "This war has been the most radical shift in warfare since WWII, at least in Europe," Fedorov tells TIME. "If you look at what happened in cyber war, we have changed the playbook basically overnight…I firmly believe that we will be able to change the way international justice is being administered as well in the aftermath of this war."

How Ukrainians are collecting digital evidence

A few weeks into the war, a column of Russian armored vehicles with missile launchers rumbled through a neighborhood near Kherson, in southern Ukraine. As it rolled past an intersection, staff at Ukraine's digital ministry back in Kyiv watched as the "e-Enemy" chatbot, which is monitored 24/7, lit up with dozens of reports from residents' windows block by block. "Almost every apartment sent us a report," Fedorov recalls. "So we could geolocate them to almost every apartment on those two streets."

Since the beginning of the invasion, Fedorov's ministry has encouraged citizens to see the government apps on their phones as essential wartime tools. Ukrainians can use them for everything from applying for relocation funds to reporting the actions of Russian forces. But government officials quickly realized that their pre-war project to digitize the country's government services—passport applications, registering newborns—had now become an invaluable tool for documenting war crimes. The apps they had set up not only gave millions of Ukrainians a direct line to the government and military through the device in their pockets, but also automatically verified their identities.

Read More: 'It's Our Home Turf.' The Man On Ukraine's Digital Frontline

In order to report anything through the e-Enemy chatbot, users have to log in through a portal launched in 2020 that lets Ukrainians share digital identifying documents on their smartphones for more than 50 government services. More than 17 million Ukrainians—roughly 40% of the population—uses the app, according to Fedorov. "We use rigorous authentication in order to weed out fake content, so we know who the person behind the report is," he says.

One example of an interaction shared with TIME show emojis and arrows guiding users through a series of automated prompts: first making sure they are safe, then telling them to focus their camera on enemy actions, shooting video for up to one minute, and attaching a timestamp and geolocation. “It corrals you towards doing the right things, so it will require several photos from certain angles and so forth,” Fedorov says. “As a result, about 80% to 90% of the user-submitted content is usable by us and by our authorities.”

More than 253,000 people have sent reports and footage of Russian forces’ movements and actions through the chatbot, according to digital ministry officials. More than 66,000 people have submitted evidence of damage to their homes and cities, which a new state service is cataloging for future reparations. All this information is tied to a verified identity and location, creating a stream of information fed into a centralized database maintained by the Office of the Prosecutor General to corroborate reports of war crimes.

Read More: A Visit to the Crime Scene Russian Troops Left Behind at a Summer Camp in Bucha

Many Ukrainian prosecutors now working on war-crimes investigations had previously been trained in using open-source intelligence, or OSINT, in human-rights cases following Russia’s invasion of eastern Ukraine in 2014, says Serhiy Kropyva, a digital adviser to the Prosecutor General. “So we have experience with this kind of evidence, and we’ve focused all the forces of our prosecutors on the war crimes claims,” Kropyva tells TIME. “It’s still really hard, and all of us understand we need to operate really quickly to store all the evidence from the beginning if we want to use [it] in different courts.”

The dashboard on the government’s war crimes portal lists almost 6,500 submissions of photos, videos, and other documentation. One graphic on “crimes against children” counts at least 191 children killed and 349 wounded. The Prosecutor General’s office has advertised the site through television interviews as well as billboards and digital banners, Kropvya says, encouraging Ukrainians to report any violations.

A simple interface allows users to share their current location to show coordinates, upload files, and submit a link to Facebook, TikTok, or other social media. The site offers 18 detailed categories, including sexual violence, torture, death, hostage taking, kinds of weapons, and whether victim is a child.

Another section is labeled “Enemy’s personal data,” allowing the user to provide any identifying information about Russian troops, including “documents, passports, call signs and pseudonyms, identification marks.” As of April 14, the office said it has identified 570 “suspects,” including Russian military and political officials, ministers, and heads of law enforcement.

The protocols for prosecution

Holding them accountable will be a complicated process. Even though Ukraine is not part of the International Criminal Court (ICC), a permanent body that has investigated war crimes for two decades, it has given it jurisdiction to prosecute war crimes committed in its territory. Last month, the ICC said it was opening an investigation and gathering evidence. But it too has been grappling with how to handle the barrage of digital evidence. Its top prosecutor, Karim Khan, has asked for new funding for technology to help his office. “Conflicts and international crises now generate audio, visual and documentary records on a massive scale,” he said in a statement on March 28. “The commission of international crimes leaves a significant digital footprint.”

Several countries have sent their own fact-finding missions, and the U.N. Human Rights Council has established a commission to investigate violations. These efforts are also backed up by a dizzying array of international human-rights analysts and organizations that use OSINT, including satellite imagery, weapons analysis, and geolocations tools.

While the use of OSINT to document war crimes is not new, one change has been the widespread adoption of the Berkeley Protocol, the first set of global guidelines that lays out standards for the collection of public digital information, including social media, as evidence for the investigation of human-rights violations. The protocol was published in 2020 after a three-year collaboration between the U.N. Office of Human Rights and the Human Rights Center at the University of California, Berkeley, building largely on the lessons of the war in Syria.

Read More: 'We Became Like a Big Startup.' How Kyiv Adapted the City's Tech to Save Lives

Most Ukrainian groups who spoke to TIME said they were using the Berkeley Protocol to determine how best to document and preserve evidence, as well as ethical and legal guidance for gathering eyewitness accounts. That could mean that a larger share of the evidence collected by these organizations and by the Ukrainian government will meet evidentiary standards of international courts of law. One key, experts say, is to focus on documentation that could identify those involved and communications that would help provide evidence of intent.

"Trying war criminals is incredibly difficult because the burden of proof is so high," says Flynn Coleman, an international human-rights lawyer who has focused on digital war-crimes documentation. "The technology often moves faster than the laws…But there are indications that the legal system is moving toward accepting more of this citizen evidence."

Still, the value of Ukraine's crowdsourced evidence goes beyond what can be proven in international court. "It's a basic right for all the survivors and families," Coleman says. "We need a record for humanity of what happened here: not just justice, but a record, because memories fade. And we need to do it now, while recollections are fresh."

This urgency has also led Fedorov and other officials to ask social-media companies to reconsider some of their practices, like pulling down content that might document eyewitness accounts of war crimes for violating its rules.

"The community guidelines were made in peaceful countries to account for normal, everyday communication going on in peacetime," says Fedorov, who said he has recently asked companies like Meta to revise these guidelines for countries that are in an active state of war. "Some content which might not be permissible in peacetime could be instrumental to proving war crimes."

Meta, which owns Facebook and Instagram, is "exploring ways to preserve this type and other types of content when we remove it" when it comes to the war in Ukraine, spokesman Andy Stone said on April 4. (Stone declined to provide further details to TIME.)

Ukrainian officials say they'll continue ramping up their efforts to create the most comprehensive body of digital evidence ever assembled in a modern war. Asked if he believes these efforts will be successful, Fedorov does not hesitate. "One hundred percent," he tells TIME. "We have satellite imagery, we have the verified content from our apps, we have other sources that I'm not at liberty to disclose…I am very sure it will help us prove our case in international jurisdictions."

For now, that promise is repeated every time a Ukrainian citizen uses the “e-Enemy” app to provide information about the actions of Russian forces. With every new crowdsourced report, a message pops up in the app: “Their relatives, friends and the whole world will learn about their brutal crimes against the Ukrainian people.”