Hackers are trying to topple Belarus's dictator, with help from the inside

technologyreview.com/2021/08/26/1033205/belarus-cyber-partisans-lukashenko-hack-opposition/

Patrick Howell O'Neill

Since becoming president of Belarus in 1994, Alexander Lukashenko has built Europe's most repressive police state and ruthlessly used his power to stay in office as a dictator.

Now hackers are trying to turn the extensive surveillance state against Lukashenko to end his reign—and to do it, they claim to have pulled off one of the most comprehensive hacks of a country in history.

The hackers, known as the Belarus Cyber Partisans, have been regularly leaking information they say has been obtained by breaching dozens of sensitive police and government databases. So far they have published what they say is evidence of crimes by police, information showing that the regime covered up the country's true covid-19 mortality rate, and recordings of illegal orders to violently crack down on peaceful protests. The partisans also say that they have successfully hacked almost every part of the Lukashenko administration and that the information released so far is just a fraction of the data they have.

"What we want is to stop the violence and repression from the terroristic regime in Belarus and to bring the country back to democratic principles and rule of law," an anonymous spokesperson for the hackers told MIT Technology Review.

Related Story

Inside the FBI, Russia, and Ukraine's failed cybercrime investigation

Russia and Ukraine promised to cooperate and help catch the world's most successful hackers. But things didn't quite go to plan.

But the Partisans are not operating alone. According to interviews, the hackers benefit from a partnership with a key group of Belarusian law enforcement and intelligence officers.

A group called BYPOL, which includes current and former regime officials, has been offering close guidance for many months. Some of them are providing help from outside the country, having defected after Lukashenko's fraudulent claims of victory in the 2020 presidential election and the brutal crackdown that followed. But others, the group says, are working against Lukashenko from within in the conviction that his regime—which arrested more than 27,000 people in the wake of protests last year—must fall.

"They're making the regime's crimes transparent," says Andrei Sannikov, a former Belarusian diplomat who is not part of either the Cyber Partisans or BYPOL. "The information they're getting by hacking the state really is very eloquent in witnessing the criminal activities of the regime against the citizens."

"I saw falsifications with my own eyes"

While Belarus has been under Lukashenko's control for almost 30 years, protests and opposition have ramped up significantly since the elections held in August 2020. His disputed victory led to a swell of anti-regime protests as Lukashenko violently crushed peaceful dissent.

The crackdowns were a breaking point for many. Aliaksandr Azarau was a lieutenant colonel in Belarus's police force, and before that, he worked to combat organized crime and corruption for the Ministry of Interior. He says what he saw turned him against the regime.

"I was present at the election," Azarau says. "I saw falsifications with my own eyes. I decided to resign after I received unlawful orders from superior officers. A lot of people were detained in the first days after the election. My colleagues were illegally sending false documents about crimes these people committed. I decided Lukashenko kept his power illegally."

He was one of a significant number of law enforcement officials who left Belarus as a result. About a dozen of them reconvened in Warsaw, in neighboring Poland, and launched BYPOL in October. (The group's name means Belarus Police.) They say they have hundreds of members and contacts still inside government security agencies including the secret police (known as the KGB), the Ministry of Interior, and border control.

> "They wanted to know how to penetrate inside these organizations to steal information. Because we work there, we know everything inside."

The Cyber Partisans say they are made up of around 15 IT experts from Belarus's technology sector: the country has a thriving scene, including numerous gaming and social startups, although many experts have left in opposition to the regime.

They began defacing government websites in September 2020, a simple but highly visible act of protest that got them attention as the country convulsed in turmoil.

In December of that year, according to Azarau, the Partisans reached out to BYPOL with bigger goals in mind.

"The Cyber Partisans wrote to us to help them find a way to understand all the law enforcement and intelligence agencies," he says. "They wanted to know how to penetrate inside these organizations to steal information. Because we work there, we know everything inside. We consulted with them on how to do this."

After those early discussions, the Cyber Partisans say they ended up carrying out the actual hacks themselves. BYPOL's current and former security force members have helped them understand the structure of government databases, process the data they access, and identify individuals from hacked phone calls. Insiders are also able to "provide feedback from within the system on how the hack affected the security forces," the hacking group's spokesperson says.

In exchange, BYPOL has access to material from the Cyber Partisans to help them conduct investigations into the regime, which are then published on BYPOL's own Telegram channel. Those investigations have been popular and successful, and one of their documentaries was cited during an American congressional hearing on Belarus which took place shortly before the US imposed sanctions against Lukashenko and his allies.

The hackers say their latest series of attacks has given them access to drone footage from protest crackdowns, the Ministry of Interior Affairs's mobile-phone surveillance database, and databases for passports, motor vehicles, and more. They also say they have accessed audio recordings from emergency services and video feeds from road speed and surveillance cameras, as well as from isolation cells where detainees are held.

The Partisans say their intention is to undermine the regime at every level. "We have a strategic plan that includes cyberattacks to paralyze as much as possible of the regime's security forces, to sabotage the regime's weak points in the infrastructure, and to provide protection for protesters," said the spokesperson.

"The hack is important because it shows the regime is not as unstoppable and unbeatable as it projects to be," says Artyom Shraibman, a political analyst at the Carnegie Moscow Center. "It shows the weakness of their system. It emboldens the protesters. Many people in the protest have met these leaks with joy and a sense of victory."

The hacks were previously reported by Current Time and Bloomberg.

"We don't have any professional hackers"

The Cyber Partisans say they are not criminal hackers but technology-sector employees who cannot stand by any longer. The group's spokesperson says that four individuals conduct "actual ethical hacking" while the others provide support, analysis, and data processing.

"We don't have any professional hackers," they told MIT Technology Review. "All of us are IT specialists and some cybersecurity specialists that learned on the go."

Pavel Slunkin, who was a Belarusian diplomat until last year and is now working with the European Council on Foreign Relations, says that the Partisans reflect the technology industry's importance to the country.

> "The Belarusian people who work in tech not only want economic impact, but they want to transform it into political influence."

"The Belarusian people who work in tech not only want economic impact but they want to transform it into political influence," he says. "These kinds of people have houses, cars, and everything—except they can't choose their own future. But now they've decided that they can participate in political life. They have played a very important role, if not the most important role, in what happened in Belarus in 2020."

In the run-up to last year's election campaign, opposition candidate Viktor Babariko recruited a number of tech experts. He was arrested and sentenced to 14 years in prison for corruption in a trial critics called a "sham."

“When Babariko was put in prison, the protest movement felt destroyed,” Slunkin says. “This was the starting point for people trying to oppose the regime, not on the streets, but instead where they feel stronger and more secure than the government.”

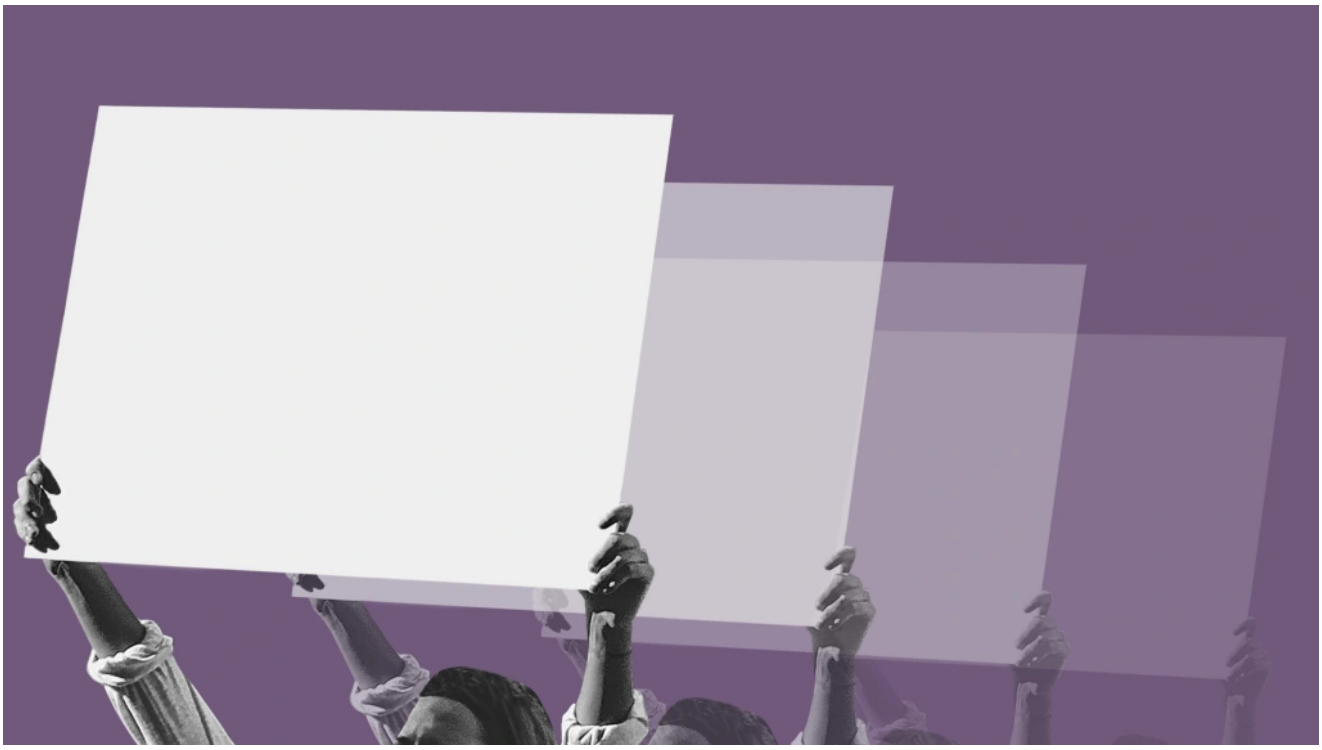
The Belarusian government blamed the hacks on “foreign special services."

“As comprehensive a hack as one can imagine”

Lukashenko’s iron grip on media and information inside Belarus has forced political opponents to move to apps like Telegram, which are harder to block or regulate. The hackers’ Telegram channel has more than 77,000 subscribers.

Their most recent postings include a recording of a conversation between two senior Belarusian police officials on August 8, 2020, the day before the presidential election. In the recording, the deputy chief of the Minsk police and his subordinate discuss “preventative” arrests of protesters and major political opponents. Their targets include staff working for Tsikhanouskaya.

Related Story



The internet of protest is being built on single-page websites

Simple, shareable, and private, these pages are Gen Z’s choice for not just learning about something, but doing something about it.

If the Cyber Partisans deliver on their promises and threats, this may turn out to be the most thorough hack a country has ever experienced.

“If we speak about possible future prosecution of the people who committed crimes on behalf of the regime, like persecuting the opposition, these hacked databases could potentially be used for tribunals and investigations,” says Shraibman.

An international coalition of human rights organizations is currently investigating and documenting torture and other human rights violations to hold the Lukashenko regime accountable for crimes committed since the 2020 election protests began.

As the enormous scope of the Cyber Partisan operation became clear to the Western world, an expert called it “as comprehensive of a hack of a state as one can imagine.” But the impact of the hack, as with so much in Belarus, remains unclear.

“I honestly don’t know what comes next,” Shraibman says. “Politically in Belarus, it’s so volatile. Lukashenko has of course managed to suppress the street protests, that is true. But he continues to be in a vulnerable position internationally and economically. He keeps provoking all the other international actors. He can’t help but escalate. He keeps escalating. That can lead us to a very dark, dangerous place.”