# A (Strange) Interview With the Russian-Military-Linked Hackers Targeting US Water Utilities

wired.com/story/cyber-army-of-russia-interview/

Andy Greenberg May 8, 2024

When the activities of Russian hacker groups are exposed in a major public report and tied to a government agency—such as the Russian military's Sandworm unit, which has targeted Ukrainian electrical utilities to trigger three blackouts over the past decade, or the Russian foreign intelligence service's APT29, which is believed to have carried out the notorious SolarWinds supply chain attack—they tend to slink into the shadows and lay low until their next operation.

When the cybersecurity firm Mandiant last month highlighted the Cyber Army of Russia, by contrast, noting its haphazard attacks on Western critical infrastructure and the group's loose ties to the Russian military, the hackers took a very different approach. “Comrades, today the collective rotten West recognized us as the most reckless hacker group 🏆, on which I actually congratulate all of us 🎉," the group posted in Russian to its Telegram channel, along with a screenshot of WIRED's article about the hackers, in which we had described them with that “most reckless” superlative. “As long as they are afraid of us, let them hate us as much as they want.”

After that initial, less-than-friendly exchange of ideas, WIRED reached out to Cyber Army of Russia's Telegram account to continue the conversation. So began a strange, two-week-long interview with the group's spokesperson, “Julia," represented by an apparently AI-generated image of a woman standing in front of Red Square's St. Basil's Cathedral. Over days of intermittent Telegram messages, often interspersed with unsolicited Russian nationalist political talking points, Julia answered WIRED's questions—or at least some of them—laid

out the group's ethos and motivations, and explained the rationale for the hackers' months-long cyber sabotage rampage, which initially focused on Ukrainian networks but has more recently included an unprecedented string of attacks hitting US and European water and wastewater systems.

An apparently AI-generated profile photo for “Julia,” the spokesperson for the Cyber Army of Russia on Telegram, whom WIRED interviewed.

Courtesy of RUSSIAN CYBER ARMY TEAM via Telegram

“We have united with the goal and mission of protecting our country in the information space against the background of unprecedented pressure from the United States, the European Union and Ukraine,” Julia wrote in a long opening statement in response to WIRED's questions.

“Our movement finds and hits the vulnerabilities of the Internet resources of both Ukraine and the countries that openly support the gang of terrorists and extremists, led by Zelensky, who are entrenched in power in Kiev,” Julia continued, using a typical Russian government description of the Ukrainian regime that has, in fact, led the defense against a brutal and unprovoked Russian invasion since 2022 that has led to close to 500,000 dead or wounded. “The most important battle is going on here and now for the minds and hearts of people, both living in Russia and Ukraine, and outside the warring countries. And the main weapon in this battle is information technology.”

## Sending a Message to … Muleshoe?

Whether or not it's winning hearts and minds, Cyber Army of Russia—which also at times calls itself the Cyber Army of Russia Reborn or People's Cyber Army of Russia—seems to at least be getting some of the attention it seeks. Last week, a group of government bodies including the US National Security Agency, the FBI, the Cybersecurity and Infrastructure Security Agency, the UK's National Cybersecurity Center, and several others issued a joint report warning of “Russian hacktivists” targeting so-called operational technology targets like control systems for water and wastewater utilities. The report warned that victims had “experienced minor tank overflow events” and other disruptions—although it noted the effects were temporary, and the hacktivists had historically exaggerated their hacking's impact.

Those agencies didn't name Cyber Army of Russia. But their warning followed another report from Mandiant that had highlighted the group by name, as well as its attacks on civilian critical infrastructure targets including multiple US-based water utilities and a Polish wastewater utility. In the case of the small West Texas town of Muleshoe, *The Washington Post* subsequently reported that the group's manipulation of control systems had gone so far as to cause a leak of tens of thousands of gallons of water. In that case and several others,

Cyber Army of Russia even posted to the group's Telegram account a screen-capture video of the hacking. In their attack on the Polish wastewater facility, for instance, they set the video to a *Super Mario Bros*. soundtrack.

So what is the endgame of the group's trollish acts of sabotage? “Our actions on attacks and hacks of websites and computer systems for remote control of mechanisms … is a really powerful and in some cases very effective method of influencing (and not only psychological) the authorities of the countries of Europe and the USA, as well as their regional authorities,” Cyber Army of Russia's representative Julia told WIRED. “With these attacks we are trying to send the following message to the US authorities: If you continue to supply military equipment and make financial injections into the leadership of Ukraine … be prepared for the fact that in any of your settlements, in any industrial system or at a critical infrastructure facility, something may suddenly fail.”



Yet as unprecedented and disturbing as it may be for a Russian hacker group to trigger a significant water leak at a US utility, Cyber Army of Russia still seems at times to comically overestimate the clarity of its threat against Ukraine's allies. In response to a question about the Muleshoe water utility attack specifically, Julia noted that the group's operation is intended to persuade “mainly representatives of the Democratic Party [because] their support for Ukraine is the most significant"—a head-scratching statement given that Muleshoe is in a Texas congressional district that hasn't elected a Democratic representative since 1982.

In other hacking operations like its targeting of a Polish wastewater utility, cybersecurity researchers who watched the video of the attack told WIRED that Cyber Army of Russia appeared to be arbitrarily changing values in the utility's control system software, with no actual disruptive effect. In another case, the hackers posted a video to their Telegram channel claiming that, in response to French president Emmanuel Macron's threat of sending French military personnel to Ukraine, it had hacked a French hydroelectric dam and caused it to stop generating power. In fact, French newspaper *Le Monde* reported, the group had actually hacked a water mill in a small village and caused its water level to drop by 20 centimeters.

When WIRED pointed out this mistake to Julia, she acknowledged the error but wrote that the group was undeterred by the setback. “It would be correct to consider it experimental,” she wrote of the attempted dam-hacking operation. “In other words, as it often happens in life, the real result did not match the expectation at all. However, we are not very saddened by this fact, there are many hydroelectric power plants in France, so we will still have the opportunity to gain more experience to commit more large-scale sabotage.”

Despite this relatively amateurish track record, Mandiant pointed in its report to evidence linking Cyber Army of Russia to the hacker group known as Sandworm, a cyberwarfare unit of Russia's military intelligence agency the GRU tied to many of Russia's most disruptive cyberattacks of the last decade. Cyber Army of Russia's short-lived YouTube channel, for instance, was created from a computer with an IP address that Mandiant—itself a subsidiary of YouTube's owner Google—had previously tied to Sandworm. Over the last year, Cyber Army of Russia also repeatedly dumped data to its Telegram channel that appeared to have been stolen from Ukrainian hacking targets breached by Sandworm not long before.

When WIRED asked about those ties to Sandworm and the GRU, Julia denied them without directly addressing Mandiant's evidence. “Hundreds of people of different ages, different nationalities, different professions (not related to IT), different levels of computer literacy, different levels of financial wealth and political beliefs joined the ranks of the Cyber Army,” Julia wrote. “We emphasize that despite the fact that there are individual representatives of the Russian security forces in our ranks and some of our participants are professionals in the field of information security, we are a completely people's project that has nothing to do with the GRU, or with any other military special forces, or with hacker groups like Sandworm.”



She later added, somewhat confusingly, that “the Sandworm hacker group does have something in common [with us] … This is the commander-in-chief of our Cyber Army.” It wasn't clear, however, whether that comment was referring to a shared leader overseeing the two groups—or even a kind of imagined ideological leader such as Russian president Vladimir Putin—or whether Julia meant that Sandworm itself gives the Cyber Army its orders, in contradiction to her previous statements. Julia didn't respond to WIRED's requests for clarification on that question or, in fact, to any questions following that comment.

## A Hacktivist Hype Machine

Russian information warfare and influence operations experts with whom WIRED shared the full text of the interview noted that, despite Cyber Army of Russia's claims of acting as an independent grassroots organization, it closely adheres to both Russian government talking points as well the Russian military's published information warfare doctrine. The group's rhetoric about changing “minds and hearts” beyond the front lines of a conflict through attacks targeting civilian infrastructure mirrors a well-known paper on “information confrontation” by Russian military general Valery Gerasimov, for instance. Other portions of Julia's comments—an unprompted polemic against “non-traditional sexual relations” and a description of Russia as a conservative cultural “Noah's Ark of the 21st century”—echo similar statements made by Russian leaders and Russian state media.

None of that proves that Cyber Army of Russia has anything more than the thin ties to the GRU that Mandiant uncovered, says Gavin Wilde, a Russia-focused senior fellow at the Carnegie Endowment for International Peace. He argues instead that the group's comments appear to be an attempt to score points with a potential government sponsor, perhaps in the hopes of gaining a more official relationship. “They're really trying to hone their messaging, but not for a Western audience, necessarily, so much as to try to put points on the board domestically and with potential political or financial benefactors in Moscow,” he says.

At one point in the interview with WIRED, in fact, Julia explicitly voiced that request for more official government support. “I really hope that the People's Cyber Army of Russia will have great prospects, that our government agencies will not just pay attention to us, but support our actions, both financially and through the formation of full-fledged cyber troops as part of the Russian Armed Forces,” she wrote.

Outside of the conversation with WIRED, Cyber Army of Russia posts to its Telegram channel in Russian, not English—a strange move for a group that claims to be trying to influence Western politics in its favor. Other Russian influence operations created by the GRU itself, such as the Guccifer 2.0 and DCLeaks fronts created to influence the 2016 presidential election, wrote in English. Even other “hacktivist” groups targeting civilian critical infrastructure, such as Israel-linked Predatory Sparrow, take credit for their attacks in the language of their targets—in Predatory Sparrow's case, posting to Telegram in Persian in an apparent attempt to influence Iranians.

- Security

  What You Need to Know About Grok AI and Your Privacy

  By Kate O'Flaherty

-

All of that suggests that, despite its claims, Cyber Army of Russia may be currently functioning more as a cheerleading campaign for Russians domestically than a real influence operation targeting the West, says Olga Belogolova, a Russia-focused influence operations researcher at the Johns Hopkins School of Advanced International Studies. If the group is as grassroots and decentralized as it claims to be, it may not even be aware of that disconnect. “These patriotic keyboard warrior types are going to try to curry favor with the government, but they also might be true believers of these talking points,” says Belogolova, adding that the group's Telegram account “feels like a marketing exercise or a tech bro hype machine.”

She points out, though, that the group's exposure by Mandiant and an alert from a half-dozen government agencies suggests that, regardless of the group's intended audience, it's now on Americans' radar, too. As it gains the West's attention, she notes, we shouldn't overblow the threat it represents—and in doing so succumb to its hit-and-miss attempts at instilling fear through its disruptive hacking.

“The more time I spend working on Russia and Russian influence operations,” Belogolova says, "the more I've become a believer that they're very into just hyping themselves up. And then we sometimes fall for the hype, too.”