THE INTERNET RUNS FASTER AT NIGHT

THE BELARUS CYBER PARTISANS

BY MARIJETA BOZOVIC AND BENJAMIN PETERS

Two Harriman alumni working on a contemporary media history project, *Imagining Russian Hackers*, encounter the most ambitious current hack on a stage—in Belarus. An intrepid band of hacktivists claims to be on the verge of toppling the Lukashenka regime, bringing new tools to an old political playbook. When is hacking revolutionary? And what happens next?

***

The nighttime explosion of a rocket on a military base in Belarus appeared relatively minor. (Hackers possess many technologies, but an organized militia is not yet one of them.) Still, the footage from an armed drone striking against the Lukashenka regime appears to tremble with both nighttime air turbulence and anticipation. Can a transnational movement of hacktivist partisans really overthrow "Europe's last dictator"? If the Belarus Cyber Partisans (BCP) succeed, what happens next—in Belarus, or in Russia and Ukraine?

Months after the fall 2021 explosion, at a virtual event cohosted by the Berkman Klein Center at Harvard and Yale's Beinecke Working Group on Art & Protest, three representatives of the Cyber Partisans spoke for themselves. The BCP self-describe as a leaderless collective of former information technology professionals, including a few sysadmins—not "career" hackers—driven to use off-the-shelf tools to hack

Screenshot from footage of the armed drone strike.

Background image source: White-and-red ornament pattern that resembles *ruchnik* designed in 1917 by Matrona Markevich for the Flag of Belarus.

in the service of public interest. In an anonymous interview with Gabriella Coleman (the anthropologist famed for her work with Anonymous) as well as the authors of this paper, the three BCP representatives, including the group's spokesperson in New York City, joined a virtual room full of journalists and invited specialists.

Through an encrypted typepad, the BCP reported that they had formed a significant coalition with other resistance movements on the ground as well as with former members of the state police who had had enough of Lukashenka's war against his own people. The BCP claimed that they had received neither technological nor financial help from any foreign powers, although they were open to help from any quarter. At least one representative of the group sketched out a political philosophy that borrows both from the American Revolution and from the Russian Revolution of 1917, asserting that, given sufficiently violent repression, the Belarusian people have a legal and moral right to take up arms against the regime. For now, their weapon of choice is code; namely, code to pilot rocket-launching drones, mobilize resistance fighters, and target the regime's vulnerabilities.

After delivering their message and appealing for international attention, the Cyber Partisans typed that they were happy to go on as long as there were questions. It may have grown late in Belarus, or perhaps in Poland—where so many Belarus dissidents are finding refuge—but as their parting words spelled out, one expectant character at a time: "The internet runs faster at night."

***

The internet does, in fact, tend to run faster at night, when ISP loads are lessened while most of the population sleeps. Vladimir Putin infamously overlooked this fact in one tactical riff about not being personally responsible if patriotic Russian hackers felt inspired to rise in the morning and do their peculiar work. ("Hackers, work in the morning?" scoffed Twitter users in response.) The reality is more mundane: hacktivists work in the daytime if they can get away with it on the job, or at

nighttime if not. But there's another metaphorical reading of these closing words: in the darkest of times, hope—and rebellion—burns bright.

Times in Minsk have indeed grown dark: Lukashenka won his sixth term as president of Belarus in August 2020 by internationally recognized fraudulent election results. Hundreds of thousands of citizens marched in protest across the streets of Minsk; at least 10 were killed and many more tortured in the resulting brutal crackdown carried out by marked and unmarked police. The EU then imposed economic sanctions on Belarus, in response to which Lukashenka began weaponizing immigrant bodies in an unprecedented crime against humanity in the region: his regime recruited roughly 20,000 immigrants from around the world to fly into Minsk and then drove them to the Polish border. When the Polish border police, instead of assessing each case one-on-one as law requires, pushed the immigrants back into Belarus, those seeking a better life were caught in a deadly stalemate, stranding families and children in the freezing forests on the eve of deadly winter months, trapped between beatings from the Belarusian police and rejection from the Polish police. The international border crisis in November has since subsided, but only because, perhaps more worryingly, the Lukashenka regime has whisked the immigrants off to undisclosed locations under unknown conditions. The situation is untenable: What is to be done in Belarus?

Are the BCP right? Does the internet really (still? yet?) have revolutionary potential? For many, the hope that computer networks offer in dark times appears at best poetic and at worst quixotic and counterproductive. And yet the Cyber Partisans appear to be a startling exception to what scholars have dubbed the growing "techlash" over the last five to ten years—a rising critical awareness of and resistance against the tech optimist and even utopian dreams that ran roughshod over technology discourse in the 1990s and aughts: What has the internet wrought in the 2010s except, critics observe, more rich-get-richer surveillance capitalism, political polarization, splintering disinformation campaigns, and the creeping erosion of basic democratic institutions? Against such rocks of tech neorealism, the Cyber Partisans offer a striking, even refreshingly retro, wave of tech utopianism. Belarus may prove an oasis in a desert of Eurasian tech defeatism, not to mention a model for foment elsewhere (although who is to say whether it will be on the left or the right?).

The Cyber Partisans may well be perfecting the next generation of what anthropologist Gabriella Coleman has called the public-interest hack, or "a computer infiltration for the purpose of leaking documents that will have political consequence." The group, as first reported by the *Washington Post* in September 2021, successfully carried out an unprecedented series of hacks into the cyber defenses of the Lukashenka regime. The spoils are significant: the group now claims to have 5.3 million records of phone taps, the regime's own documentation of its violence against its people, the contact information for police informants and enforcers, and the entire national passport database. The group, in scooping these documents, discovered for example that the regime underreported

Logo of the Cyber Partisans on their YouTube channel.

COVID mortality rates by a factor of at least 15. The hacks have also made it possible to monitor the regime's ongoing abuses and politicization of immigrant men, women, children, and families.

The BCP have a relatively sophisticated media team and publicity strategy. Building on lessons learned from other hacktivist traditions around the world, they report that their plan is to slowly release over six terabytes of sensitive data, dripping one story at a time into the hands of hungry journalists. The aim, of course, is to use the data to continuously refocus and heighten the scrutiny of the international press on the plight of Belarusians living under Lukashenka. Coleman, a leading anthropologist of hackers, has called the work of the Cyber Partisans "the most comprehensive hack of a state by a group of hacktivists to date." The group—which maintains active Telegram, YouTube, and other social media channels—even offers video primers, with English subtitles, to train the everyday Belarusian citizen as well as the outside observer on its emerging plan to mobilize international support against the regime, to develop logistical coordination apps for Belarusian citizens ready to fight, and to provide countersurveillance and strikes against the regime's military defenses. Should a toppled Lukashenka regime be held responsible for its horrendous crimes against humanity in the international criminal court, the BCP will be holding the digital receipts.

The Cyber Partisans present a beautiful contradiction to the current global imaginaries about Russian and East European hackers. On the one

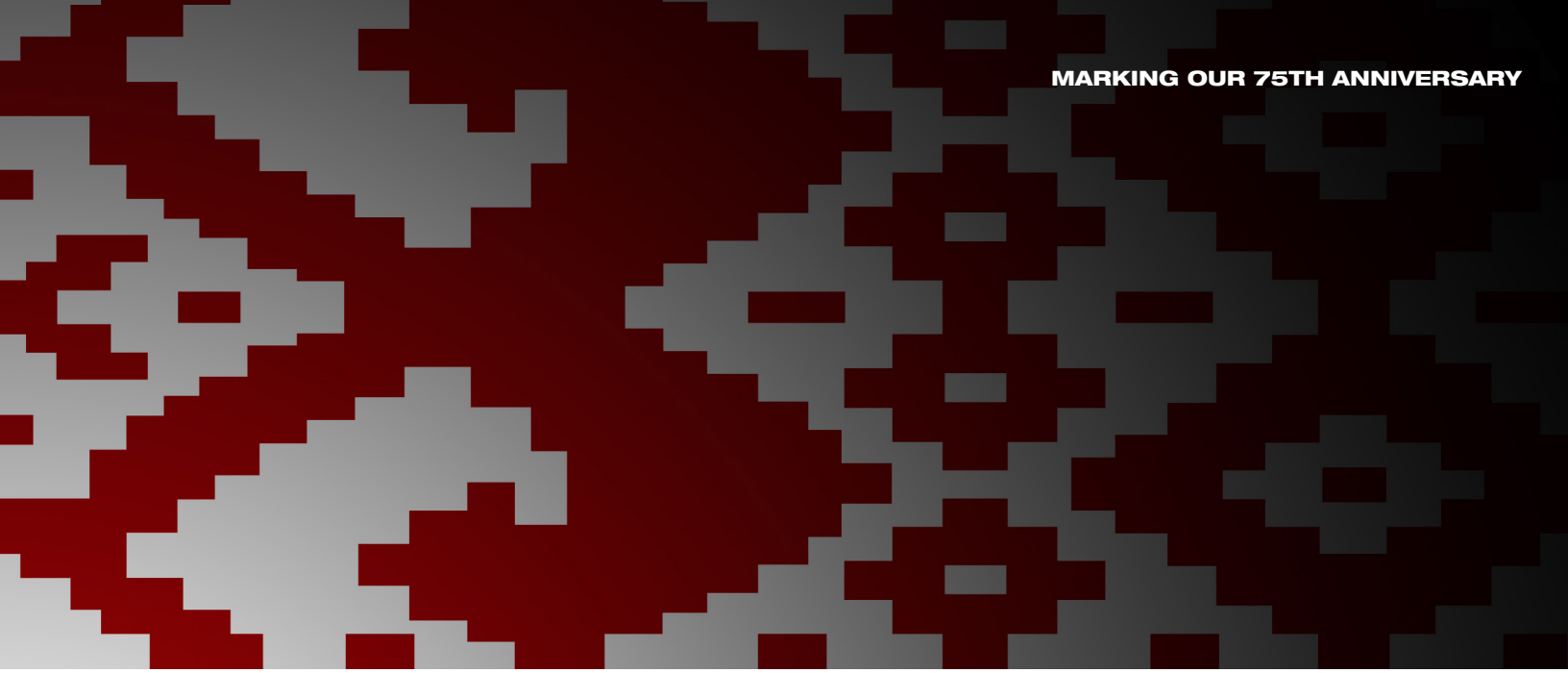
NO ONE KNOWS WHETHER THE BCP WILL SPEED A CHANGE OF POWER IN BELARUS. THE BLUEPRINT THEY ARE FOLLOWING, HOWEVER, OFFERS A SENSE OF DISCONCERTING DÉJÀ VU AS WELL AS AWE AND WONDER.

hand, they appear almost the opposite of the anxieties driving Russian hacker discourse of late, where, in a motif all too familiar to scholars of the long Soviet century, the Russian spy (reimagined) emerges as the favorite enemy Other around whose neck may be perennially hung the responsibility for most U.S. and Western struggles. The Russian hacker is conveniently (imagined as) white and male—an unproblematically demonizable enemy, easy enough to hate without setting off U.S.-centrist worries about its own racism and sexism. In this sense, the Russian hacker serves as a convenient imagined Other for the U.S. political center to police both the American left and the right. More convenient than scrutinized, the imagined Russian hacker offers a kind of media event across transnational culture, tech, and screens, embodying recurrent 20th-century anxieties upgraded with the technology of the mid-21st.

The Belarus Cyber Partisans, of course, appear a stark contrast from fears of foreign hackers as extensions of dictatorial states. Yet at the same time there is a striking commonality between the BCP's hopes for speeding a long-overdue social revolution in Belarus and the often underarticulated American anxieties about Russian hackers doing the same to U.S. democracy over the last decade. The Cyber Partisans and American critics both, knowingly or unknowingly, take their strategic direction from Lenin's playbook: the first step is to seize the means of communication; to plan the strategic and tactical ground war; and to win over, whether through genuine messaging or disinformation campaigns, enough of the public goodwill to erode the regime's strengths from the inside out.

The aesthetics of the two hacker imaginaries diverge to an extent: the Cyber Partisans offer YouTube and Telegram videos full of voice camouflaging, jarring montage, anarchic energy, and rage against the machine. American concerns about Russian disinformation campaigns, by contrast, feature idiot uncle misspellings; underwhelming reactionary memes; the subtle crucifixion of religious values onto the political agenda of the far right; and a much longer, slower game for whom the boogeyman of the Russian

Demonstration in Munich in April 2022.



hacker normalizes these concerns for the American center. The BCP imagine themselves to be partisan professionals mobilizing all tools and resources available to them to end state violence on their streets, as might Robin Hood; by contrast, the American imagines Russian hackers as malicious state-sponsored bot kings, thinly disguised cold war spies with laptops and hoodies, preying on perennial fault lines (race, class, political bifurcation) to distort public discourse. Both visions are, of course, fantasy, but oddly potent, enduring, and revealing.

No one knows whether the Cyber Partisans will speed a change of power in Belarus. The blueprint they are following, however, offers a sense of disconcerting déjà vu as well as awe and wonder. Perhaps the internet really does run faster at night. ■

January 2022

Editor's note: *Marijeta Bozovic and Benjamin Peters, the coauthors of this article, met through the Harriman Institute as doctoral students at Columbia University and are now principal researchers of the* Imagining Russian Hackers *project at Yale University (see https://hackersinitiative.yale.edu/). Their research analyzes the dramatic revival of what some have termed the rhetoric of Cold War 2.0, following mainstream media coverage of various tales of "Russian hackers" in the United States and the former West alongside studies of fictional portrayals in television and film. How does the Russian hacker narrative shape, stand in for, or obfuscate the popular imagination of Web 2.0 technologies more broadly? This is a story of mediation, motivated imaginaries, the political power of aesthetic productions, and media (more even than state) rivalries—an intersecting story that follows the actual intellectual histories of IT specialists from the Soviet-era and post-Soviet era, spanning across the world. The Soviet Union may have failed to network first, but the internet even today remains curiously Soviet. Through these two intercutting stories, Bozovic and Peters show how interrogating practices of "imagining Russian hackers" illuminate the political fissures and blind spots in our global media landscapes.*

Marijeta Bozovic is assistant professor of Slavic languages and literatures, affiliated with Film and Media Studies and Women's, Gender, and Sexuality Studies at Yale University. She is the author of Nabokov's Canon: From Onegin to Ada *(2016) and coeditor of* Watersheds: Poetics and Politics of the Danube River *(2016) and* Nabokov Upside Down *(2017). She recently completed work on her second monograph, "Avant-Garde Post–: Radical Poetics after the Soviet Union." Bozovic is coeditor of the journal* Russian Literature*; film and media editor of* Slavic Review*; and associate editor of* ASAP/Journal.

Benjamin Peters is a media scholar and author of How Not to Network a Nation: The Uneasy History of the Soviet Internet *(2016), editor of* Digital Keywords: A Vocabulary of Information Society & Culture *(2016), and coeditor of* Your Computer Is on Fire *(2021). He is Hazel Rogers Associate Professor and chair of Media Studies at the University of Tulsa and affiliated fellow at the Information Society Project at Yale Law School.*