How an Entire Nation Became Russia's Test Lab for Cyberwar

wired.com/story/russian-hackers-attack-ukraine/

Andy Greenber g

The clocks read zero when the lights went out.

It was a Saturday night last December, and Oleksii Yasinsky was sitting on the couch with his wife and teenage son in the living room of their Kiev apartment. The 40-year-old Ukrainian cybersecurity researcher and his family were an hour into Oliver Stone's film *Snowden* when their building abruptly lost power.

"The hackers don't want us to finish the movie," Yasinsky's wife joked. She was referring to an event that had occurred a year earlier, a cyberattack that had cut electricity to nearly a quarter-million Ukrainians two days before Christmas in 2015. Yasinsky, a chief forensic analyst at a Kiev digital security firm, didn't laugh. He looked over at a portable clock on his desk: The time was 00:00. Precisely midnight.

Yasinsky's television was plugged into a surge protector with a battery backup, so only the flicker of images onscreen lit the room now. The power strip started beeping plaintively. Yasinsky got up and switched it off to save its charge, leaving the room suddenly silent.

July 2017. Subscribe to WIRED.

He went to the kitchen, pulled out a handful of candles and lit them. Then he stepped to the kitchen window. The thin, sandy-blond engineer looked out on a view of the city as he'd never seen it before: The entire skyline around his apartment building was dark. Only the gray glow of distant lights reflected off the clouded sky, outlining blackened hulks of modern condos and Soviet high-rises.

Noting the precise time and the date, almost exactly a year since the December 2015 grid attack, Yasinsky felt sure that this was no normal blackout. He thought of the cold outside—close to zero degrees Fahrenheit—the slowly sinking temperatures in thousands of homes, and the countdown until dead water pumps led to frozen pipes.

That's when another paranoid thought began to work its way through his mind: For the past 14 months, Yasinsky had found himself at the center of an enveloping crisis. A growing roster of Ukrainian companies and government agencies had come to him to analyze a plague of cyberattacks that were hitting them in rapid, remorseless succession. A single group of hackers seemed to be behind all of it. Now he couldn't suppress the sense that those same phantoms, whose fingerprints he had traced for more than a year, had reached back, out through the internet's ether, into his home.

The Cyber-Cassandras said this would happen. For decades they warned that hackers would soon make the leap beyond purely digital mayhem and start to cause real, physical damage to the world. In 2009, when the NSA's Stuxnet malware silently accelerated a few hundred Iranian nuclear centrifuges until they destroyed themselves, it seemed to offer a preview of this new era. "This has a whiff of August 1945," Michael Hayden, former director of the NSA and the CIA, said in a speech. "Somebody just used a new weapon, and this weapon will not be put back in the box."

Now, in Ukraine, the quintessential cyberwar scenario has come to life. Twice. On separate occasions, invisible saboteurs have turned off the electricity to hundreds of thousands of people. Each blackout lasted a matter of hours, only as long as it took for scrambling engineers to manually switch the power on again. But as proofs of concept, the attacks set a new precedent: In Russia's shadow, the decades-old nightmare of hackers stopping the gears of modern society has become a reality.

And the blackouts weren't just isolated attacks. They were part of a digital blitzkrieg that has pummeled Ukraine for the past three years—a sustained cyberassault unlike any the world has ever seen. A hacker army has systematically undermined practically every sector of Ukraine: media, finance, transportation, military, politics, energy. Wave after wave of intrusions have deleted data, destroyed computers, and in some cases paralyzed organizations' most basic functions. "You can't really find a space in Ukraine where there *hasn't* been an attack," says Kenneth Geers, a NATO ambassador who focuses on cybersecurity.

In a public statement in December, Ukraine's president, Petro Poroshenko, reported that there had been 6,500 cyberattacks on 36 Ukrainian targets in just the previous two months. International cybersecurity analysts have stopped just short of conclusively attributing these

attacks to the Kremlin, but Poroshenko didn't hesitate: Ukraine's investigations, he said, point to the "direct or indirect involvement of secret services of Russia, which have unleashed a cyberwar against our country." (The Russian foreign ministry didn't respond to multiple requests for comment.)

To grasp the significance of these assaults—and, for that matter, to digest much of what's going on in today's larger geopolitical disorder—it helps to understand Russia's uniquely abusive relationship with its largest neighbor to the west. Moscow has long regarded Ukraine as both a rightful part of Russia's empire and an important territorial asset—a strategic buffer between Russia and the powers of NATO, a lucrative pipeline route to Europe, and home to one of Russia's few accessible warm-water ports. For all those reasons, Moscow has worked for generations to keep Ukraine in the position of a submissive smaller sibling.

But over the past decade and a half, Moscow's leash on Ukraine has frayed, as popular support in the country has pulled toward NATO and the European Union. In 2004, Ukrainian crowds in orange scarves flooded the streets to protest Moscow's rigging of the country's elections; that year, Russian agents allegedly went so far as to poison the surging pro-Western presidential candidate Viktor Yushchenko. A decade later, the 2014 Ukrainian Revolution finally overthrew the country's Kremlin-backed president, Viktor Yanukovych (a leader whose longtime political adviser, Paul Manafort, would go on to run the US presidential campaign of Donald Trump). Russian troops promptly annexed the Crimean Peninsula in the south and invaded the Russian-speaking eastern region known as Donbass. Ukraine has since then been locked in an undeclared war with Russia, one that has displaced nearly 2 million internal refugees and killed close to 10,000 Ukrainians.

> "Russia will never accept a sovereign, independent Ukraine. Twenty-five years since the Soviet collapse, Russia is still sick with this imperialistic syndrome."

From the beginning, one of this war's major fronts has been digital. Ahead of Ukraine's post-revolution 2014 elections, a pro-Russian group calling itself CyberBerkut—an entity with links to the Kremlin hackers who later breached Democratic targets in America's 2016 presidential election—rigged the website of the country's Central Election Commission to announce ultra-right presidential candidate Dmytro Yarosh as the winner. Administrators detected the tampering less than an hour before the election results were set to be declared. And that attack was just a prelude to Russia's most ambitious experiment in digital war, the barrage of cyberattacks that began to accelerate in the fall of 2015 and hasn't ceased since.

Yushchenko, who ended up serving as Ukraine's president from 2005 to 2010, believes that Russia's tactics, online and off, have one single aim: "to destabilize the situation in Ukraine, to make its government look incompetent and vulnerable." He lumps the blackouts and other cyberattacks together with the Russian disinformation flooding Ukraine's media, the

terroristic campaigns in the east of the country, and his own poisoning years ago—all underhanded moves aimed at painting Ukraine as a broken nation. “Russia will never accept Ukraine being a sovereign and independent country,” says Yushchenko, whose face still bears traces of the scars caused by dioxin toxicity. “Twenty-five years since the Soviet collapse, Russia is still sick with this imperialistic syndrome.”

But many global cybersecurity analysts have a much larger theory about the endgame of Ukraine’s hacking epidemic: They believe Russia is using the country as a cyberwar testing ground—a laboratory for perfecting new forms of global online combat. And the digital explosives that Russia has repeatedly set off in Ukraine are ones it has planted at least once before in the civil infrastructure of the United States.

One Sunday morning in October 2015, more than a year before Yasinsky would look out of his kitchen window at a blacked-out skyline, he sat near that same window sipping tea and eating a bowl of cornflakes. His phone rang with a call from work. He was then serving as the director of information security at StarLightMedia, Ukraine’s largest TV broadcasting conglomerate. During the night, two of StarLight’s servers had inexplicably gone offline. The IT administrator on the phone assured him that the servers had already been restored from backups.

But Yasinsky felt uneasy. The two machines had gone dark at almost the same minute. “One server going down, it happens,” Yasinsky says. “But two servers at the same time? That’s suspicious.”

Resigned to a lost weekend, he left his apartment and took the 40-minute metro ride to StarLightMedia’s office. When he got there, Yasinsky and the company’s IT admins examined the image they’d kept of one of the corrupted servers. Its master boot record, the deep-seated, reptile-brain portion of a computer’s hard drive that tells the machine where to find its own operating system, had been precisely overwritten with zeros. This was especially troubling, given that the two victim servers were domain controllers, computers with powerful privileges that could be used to reach into hundreds of other machines on the corporate network.

> Yasinsky printed the code and laid the papers across his kitchen table and floor. He'd been in information security for 20 years, but he’d never analyzed such a refined digital weapon.

Yasinsky quickly discovered the attack was indeed far worse than it had seemed: The two corrupted servers had planted malware on the laptops of 13 StarLight employees. The infection had triggered the same boot-record overwrite technique to brick the machines just

as staffers were working to prepare a morning TV news bulletin ahead of the country's local elections.

Nonetheless, Yasinsky could see he'd been lucky. Looking at StarLight's network logs, it appeared the domain controllers had committed suicide prematurely. They'd actually been set to infect and destroy 200 more PCs at the company. Soon Yasinsky heard from a competing media firm called TRK that it had been less fortunate: That company lost more than a hundred computers to an identical attack.

Yasinsky managed to pull a copy of the destructive program from StarLight's network. Back at home, he pored over its code. He was struck by the layers of cunning obfuscation—the malware had evaded all antivirus scans and even impersonated an antivirus scanner itself, Microsoft's Windows Defender. After his family had gone to sleep, Yasinsky printed the code and laid the papers across his kitchen table and floor, crossing out lines of camouflaging characters and highlighting commands to see its true form. Yasinsky had been working in information security for 20 years; he'd managed massive networks and fought off crews of sophisticated hackers before. But he'd never analyzed such a refined digital weapon.

> "With every step forward, it became clearer that our *Titanic* had found its iceberg. The deeper we looked, the bigger it was."

Beneath all the cloaking and misdirection, Yasinsky figured out, was a piece of malware known as KillDisk, a data-destroying parasite that had been circulating among hackers for about a decade. To understand how it got into their system, Yasinsky and two colleagues at StarLight obsessively dug into the company's network logs, combing them again and again on nights and weekends. By tracing signs of the hackers' fingerprints—some compromised corporate YouTube accounts, an administrator's network login that had remained active even when he was out sick—they came to the stomach-turning realization that the intruders had been inside their system for more than six months. Eventually, Yasinsky identified the piece of malware that had served as the hackers' initial foothold: an all-purpose Trojan known as BlackEnergy.

Soon Yasinsky began to hear from colleagues at other companies and in the government that they too had been hacked, and in almost exactly the same way. One attack had hit Ukrzaliznytsia, Ukraine's biggest railway company. Other targets asked Yasinsky to keep their breaches secret. Again and again, the hackers used BlackEnergy for access and reconnaissance, then KillDisk for destruction. Their motives remained an enigma, but their marks were everywhere.

"With every step forward, it became clearer that our *Titanic* had found its iceberg," says Yasinsky. "The deeper we looked, the bigger it was."

Even then, Yasinsky didn't know the real dimensions of the threat. He had no idea, for instance, that by December 2015, BlackEnergy and KillDisk were also lodged inside the computer systems of at least three major Ukrainian power companies, lying in wait.

CURT MERLO

At first, Robert Lee blamed the squirrels.

It was Christmas Eve 2015—and also, it so happened, the day before Lee was set to be married in his hometown of Cullman, Alabama. A barrel-chested and bearded redhead, Lee had recently left a high-level job at a three-letter US intelligence agency, where he'd focused on the cybersecurity of critical infrastructure. Now he was settling down to launch his own security startup and marry the Dutch girlfriend he'd met while stationed abroad.

As Lee busied himself with wedding preparations, he saw news headlines claiming that hackers had just taken down a power grid in western Ukraine. A significant swath of the country had apparently gone dark for six hours. Lee blew off the story—he had other things on his mind, and he'd heard spurious claims of hacked grids plenty of times before. The cause was usually a rodent or a bird—the notion that squirrels represented a greater threat to the power grid than hackers had become a running joke in the industry.

The next day, however, just before the wedding itself, Lee got a text about the purported cyberattack from Mike Assante, a security researcher at the SANS Institute, an elite cybersecurity training center. That got Lee's attention: When it comes to digital threats to power grids, Assante is one of the most respected experts in the world. And he was telling Lee that the Ukraine blackout hack looked like the real thing.

> The hackers had spread through the power companies' networks and eventually compromised a VPN used for remote access.

Just after Lee had said his vows and kissed his bride, a contact in Ukraine messaged him as well: The blackout hack was real, the man said, and he needed Lee's help. For Lee, who'd spent his career preparing for infrastructure cyberattacks, the moment he'd anticipated for years had finally arrived. So he ditched his own reception and began to text with Assante in a quiet spot, still in his wedding suit.

Lee eventually retreated to his mother's desktop computer in his parents' house nearby. Working in tandem with Assante, who was at a friend's Christmas party in rural Idaho, they pulled up maps of Ukraine and a chart of its power grid. The three power companies' substations that had been hit were in different regions of the country, hundreds of miles from one another and unconnected. "This was not a squirrel," Lee concluded with a dark thrill.

By that night, Lee was busy dissecting the KillDisk malware his Ukrainian contact had sent him from the hacked power companies, much as Yasinsky had done after the StarLightMedia hack months before. ("I have a very patient wife," Lee says.) Within days, he'd received a sample of the BlackEnergy code and forensic data from the attacks. Lee saw how the intrusion had started with a phishing email impersonating a message from the Ukrainian parliament. A malicious Word attachment had silently run a script on the victims' machines, planting the BlackEnergy infection. From that foothold, it appeared, the hackers had spread through the power companies' networks and eventually compromised a VPN the companies had used for remote access to their network—including the highly specialized industrial control software that gives operators remote command over equipment like circuit breakers.

> The same group that snuffed out the lights for nearly a quarter-million Ukrainians had infected American electric utilities with the very same malware.

Looking at the attackers' methods, Lee began to form a notion of who he was up against. He was struck by similarities between the blackout hackers' tactics and those of a group that had recently gained some notoriety in the cybersecurity world—a group known as Sandworm. In 2014 the security firm FireEye had issued warnings about a team of hackers that was planting BlackEnergy malware on targets that included Polish energy firms and Ukrainian government agencies; the group seemed to be developing methods to target the specialized computer architectures that are used for remotely managing physical industrial equipment. The group's name came from references to *Dune* found buried in its code, terms like *Harkonnen* and *Arrakis*, an arid planet in the novel where massive sandworms roam the deserts.

No one knew much about the group's intentions. But all signs indicated that the hackers were Russian: FireEye had traced one of Sandworm's distinctive intrusion techniques to a presentation at a Russian hacker conference. And when FireEye's engineers managed to access one of Sandworm's unsecured command-and-control servers, they found instructions for how to use BlackEnergy written in Russian, along with other Russian-language files.

Most disturbing of all for American analysts, Sandworm's targets extended across the Atlantic. Earlier in 2014, the US government reported that hackers had planted BlackEnergy on the networks of American power and water utilities. Working from the government's findings, FireEye had been able to pin those intrusions, too, on Sandworm.

For Lee, the pieces came together: It looked like the same group that had just snuffed out the lights for nearly a quarter-million Ukrainians had not long ago infected the computers of American electric utilities with the very same malware.

It had been just a few days since the Christmas blackout, and Assante thought it was too early to start blaming the attack on any particular hacker group—not to mention a government. But in Lee's mind, alarms went off. The Ukraine attack represented something more than a faraway foreign case study. "An adversary that had already targeted American energy utilities had crossed the line and taken down a power grid," Lee says. "It was an imminent threat to the United States."

On a cold, bright day a few weeks later, a team of Americans arrived in Kiev. They assembled at the Hyatt, a block from the golden-domed Saint Sophia Cathedral. Among them were staff from the FBI, the Department of Energy, the Department of Homeland Security, and the North American Electric Reliability Corporation, the body responsible for the stability of the US grid, all part of a delegation that had been assigned to get to the bottom of the Ukrainian blackout.

The Feds had also flown Assante in from Wyoming. Lee, a hotter head than his friend, had fought with the US agencies over their penchant for secrecy, insisting that the details of the attack needed to be publicized immediately. He hadn't been invited.

On that first day, the suits gathered in a sterile hotel conference room with the staff of Kyivoblenergo, the city's regional power distribution company and one of the three victims of the power grid attacks. Over the next several hours, the Ukrainian company's stoic execs and engineers laid out the blow-by-blow account of a comprehensive, almost torturous raid on their network.

> "The message was, 'I'm going to make you feel this everywhere.' These attackers must have seemed like they were gods."

As Lee and Assante had noticed, the malware that infected the energy companies hadn't contained any commands capable of actually controlling the circuit breakers. Yet on the afternoon of December 23, Kyivoblenergo employees had watched helplessly as circuit after circuit was opened in dozens of substations across a Massachusetts-sized region, seemingly commanded by computers on their network that they couldn't see. In fact, Kyivoblenergo's engineers determined that the attackers had set up their own perfectly configured copy of the control software on a PC in a faraway facility and then had used that rogue clone to send the commands that cut the power.

Once the circuit breakers were open and the power for tens of thousands of Ukrainians had gone dead, the hackers launched another phase of the attack. They'd overwritten the firmware of the substations' serial-to-ethernet converters—tiny boxes in the stations' server closets that translated internet protocols to communicate with older equipment. By rewriting the obscure code of those chunks of hardware—a trick that likely took weeks to

devise—the hackers had permanently bricked the devices, shutting out the legitimate operators from further digital control of the breakers. Sitting at the conference room table, Assante marveled at the thoroughness of the operation.

The hackers also left one of their usual calling cards, running KillDisk to destroy a handful of the company's PCs. But the most vicious element of the attack struck the control stations' battery backups. When the electricity was cut to the region, the stations themselves also lost power, throwing them into darkness in the midst of their crisis. With utmost precision, the hackers had engineered a blackout within a blackout.

"The message was, 'I'm going to make you feel this everywhere.' *Boom boom boom boom boom boom boom*," Assante says, imagining the attack from the perspective of a bewildered grid operator. "These attackers must have seemed like they were gods."

That night, the team boarded a flight to the western Ukrainian city of Ivano-Frankivsk, at the foot of the Carpathian Mountains, arriving at its tiny Soviet-era airport in a snowstorm. The next morning they visited the headquarters of Prykarpattyaoblenergo, the power company that had taken the brunt of the pre-Christmas attack.

The power company executives politely welcomed the Americans into their modern building, under the looming smokestacks of the abandoned coal power plant in the same complex. Then they invited them into their boardroom, seating them at a long wooden table beneath an oil painting of the aftermath of a medieval battle.

> Before their eyes, phantom hands clicked through dozens of breakers—each serving power to a different swath of the region—and one by one by one, turned them cold.

The attack they described was almost identical to the one that hit Kyivoblenergo: BlackEnergy, corrupted firmware, disrupted backup power systems, KillDisk. But in this operation, the attackers had taken another step, bombarding the company's call centers with fake phone calls—possibly to delay any warnings of the power outage from customers or simply to add another layer of chaos and humiliation.

There was another difference too. When the Americans asked whether, as in Kiev, cloned control software had sent the commands that shut off the power, the Prykarpattyaoblenergo engineers said no, that their circuit breakers had been opened by another method. That's when the company's technical director, a tall, serious man with black hair and ice-blue eyes, cut in. Rather than try to explain the hackers' methods to the Americans through a translator, he offered to show them, clicking Play on a video he'd recorded himself on his battered iPhone 5s.

The 56-second clip showed a cursor moving around the screen of one of the computers in the company's control room. The pointer glides to the icon for one of the breakers and

Watch as hackers take over the mouse controls of Ukrainian grid operators, part of a breach that caused a blackout for a quarter million people.

clicks a command to open it. The video pans from the computer's Samsung monitor to its mouse, which hasn't budged. Then it shows the cursor moving again, seemingly of its own

The hackers hadn't sent their blackout commands from automated malware, or even a cloned machine as they'd done at Kyivoblenergo. Instead, the intruders had exploited the company's IT helpdesk tool to take direct control of the mouse movements of the stations' operators. They'd locked the operators out of their own user interface. And before their eyes, phantom hands had clicked through dozens of breakers—each serving power to a different swath of the region—and one by one by one, turned them cold.

In August 2016, eight months after the first Christmas blackout, Yasinsky left his job at StarLightMedia. It wasn't enough, he decided, to defend a single company from an onslaught that was hitting every stratum of Ukrainian society. To keep up with the hackers, he needed a more holistic view of their work, and Ukraine needed a more coherent response to the brazen, prolific organization that Sandworm had become. "The light side remains divided," he says of the balkanized reaction to the hackers among their victims. "The dark side is united."

So Yasinsky took a position as the head of research and forensics for a Kiev firm called Information Systems Security Partners. The company was hardly a big name. But Yasinsky turned it into a de facto first responder for victims of Ukraine's digital siege.

Not long after Yasinsky switched jobs, almost as if on cue, the country came under another, even broader wave of attacks. He ticks off the list of casualties: Ukraine's pension fund, the country's treasury, its seaport authority, its ministries of infrastructure, defense, and finance. The hackers again hit Ukraine's railway company, this time knocking out its online booking system for days, right in the midst of the holiday travel season. As in 2015, most of the attacks culminated with a KillDisk-style detonation on the target's hard drive. In the case of the finance ministry, the logic bomb deleted terabytes of data, just as the ministry was preparing its budget for the next year. All told, the hackers' new winter onslaught matched and exceeded the previous year's—right up to its grand finale.

On December 16, 2016, as Yasinsky and his family sat watching *Snowden*, a young engineer named Oleg Zaychenko was four hours into his 12-hour night shift at Ukrenergo's transmission station just north of Kiev. He sat in an old Soviet-era control room, its walls

covered in beige and red floor-to-ceiling analog control panels. The station's tabby cat, Aza, was out hunting; all that kept Zaychenko company was a television in the corner playing pop music videos.

> The 20th and final circuit switched off and the lights in the control room went out, along with the computer and TV.

He was filling out a paper-and-pencil log, documenting another uneventful Saturday evening, when the station's alarm suddenly sounded, a deafening continuous ringing. To his right Zaychenko saw that two of the lights indicating the state of the transmission system's circuits had switched from red to green—in the universal language of electrical engineers, a sign that it was off.

The technician picked up the black desk phone to his left and called an operator at Ukrenergo's headquarters to alert him to the routine mishap. As he did, another light turned green. Then another. Zaychenko's adrenaline began to kick in. As he hurriedly explained the situation to the remote operator, the lights kept flipping: red to green, red to green. Eight, then 10, then 12.

As the crisis escalated, the operator ordered Zaychenko to run outside and check the equipment for physical damage. At that moment, the 20th and final circuit switched off and the lights in the control room went out, along with the computer and TV. Zaychenko was already throwing a coat over his blue and yellow uniform and sprinting for the door.

The transmission station is normally a vast, buzzing jungle of electrical equipment stretching over 20 acres, the size of more than a dozen football fields. But as Zaychenko came out of the building into the freezing night air, the atmosphere was eerier than ever before: The three tank-sized transformers arrayed alongside the building, responsible for about a fifth of the capital's electrical capacity, had gone entirely silent. Until then Zaychenko had been mechanically ticking through an emergency mental checklist. As he ran past the paralyzed machines, the thought entered his mind for the first time: The hackers had struck again.

This time the attack had moved up the circulatory system of Ukraine's grid. Instead of taking down the distribution stations that branch off into capillaries of power lines, the saboteurs had hit an artery. That single Kiev transmission station carried 200 megawatts, more total electric load than all the 50-plus distribution stations knocked out in the 2015 attack combined. Luckily, the system was down for just an hour—hardly long enough for pipes to start freezing or locals to start panicking—before Ukrenergo's engineers began manually closing circuits and bringing everything back online.

But the brevity of the outage was virtually the only thing that was less menacing about the 2016 blackout. Cybersecurity firms that have since analyzed the attack say that it was far more evolved than the one in 2015: It was executed by a highly sophisticated, adaptable piece of malware now known as "CrashOverride," a program expressly coded to be an automated, grid-killing weapon.

Lee's critical infrastructure security startup, Dragos, is one of two firms that have pored through the malware's code; Dragos obtained it from a Slovakian security outfit called ESET. The two teams found that, during the attack, CrashOverride was able to "speak" the language of the grid's obscure control system protocols, and thus send commands directly to grid equipment. In contrast to the laborious phantom-mouse and cloned-PC techniques the hackers used in 2015, this new software could be programmed to scan a victim's network to map out targets, then launch at a preset time, opening circuits on cue without even having an internet connection back to the hackers. In other words, it's the first malware found in the wild since Stuxnet that's designed to independently sabotage physical infrastructure.

> "In 2015 they were like a group of brutal street fighters. In 2016, they were ninjas."

And CrashOverride isn't just a one-off tool, tailored only to Ukrenergo's grid. It's a reusable and highly adaptable weapon of electric utility disruption, researchers say. Within the malware's modular structure, Ukrenergo's control system protocols could easily be swapped out and replaced with ones used in other parts of Europe or the US instead.

Marina Krotofil, an industrial control systems security researcher for Honeywell who also analyzed the Ukrenergo attack, describes the hackers' methods as simpler and far more efficient than the ones used in the previous year's attack. "In 2015 they were like a group of brutal street fighters," Krotofil says. "In 2016, they were ninjas." But the hackers themselves may be one and the same; Dragos' researchers have identified the architects of CrashOverride as part of Sandworm, based on evidence that Dragos is not yet ready to reveal.

For Lee, these are all troubling signs of Sandworm's progress. I meet him in the bare-bones offices of his Baltimore-based critical infrastructure security firm, Dragos. Outside his office window looms a series of pylons holding up transmission lines. Lee tells me that they carry power 18 miles south, to the heart of Washington, DC.

For the first time in history, Lee points out, a group of hackers has shown that it's willing and able to attack critical infrastructure. They've refined their techniques over multiple, evolving assaults. And they've already planted BlackEnergy malware on the US grid once before. "The people who understand the US power grid know that it can happen here," Lee says.

To Sandworm's hackers, Lee says, the US could present an even more convenient set of targets should they ever decide to strike the grid here. US power firms are more attuned to cybersecurity, but they are also more automated and modern than those in Ukraine—which means they could present more of a digital "attack surface." And American engineers have less experience with manual recovery from frequent blackouts.

> "Tell me what *doesn't* change dramatically when key cities across half of the US don't have power for a month."

No one knows how, or where, Sandworm's next attacks will materialize. A future breach might target not a distribution or transmission station but an actual power plant. Or it could be designed not simply to turn off equipment but to *destroy* it. In 2007 a team of researchers at Idaho National Lab, one that included Mike Assante, demonstrated that it's possible to hack electrical infrastructure to death: The so-called Aurora experiment used nothing but digital commands to permanently wreck a 2.25-megawatt diesel generator. In a video of the experiment, a machine the size of a living room coughs and belches black and white smoke in its death throes. Such a generator is not all that different from the equipment that sends hundreds of megawatts to US consumers; with the right exploit, it's possible that someone could permanently disable power-generation equipment or the massive, difficult-to-replace transformers that serve as the backbone of our transmission system. "Washington, DC? A nation-state could take it out for two months without much issue," Lee says.

In fact, in its analysis of CrashOverride, ESET found that the malware may already include one of the ingredients for that kind of destructive attack. ESET's researchers noted that CrashOverride contains code designed to target a particular Siemens device found in power stations—a piece of equipment that functions as a kill-switch to prevent dangerous surges on electric lines and transformers. If CrashOverride is able to cripple that protective measure, it might already be able to cause permanent damage to grid hardware.

An isolated incident of physical destruction may not even be the worst that hackers can do. The American cybersecurity community often talks about "advanced persistent threats"—sophisticated intruders who don't simply infiltrate a system for the sake of one attack but stay there, silently keeping their hold on a target. In his nightmares, Lee says, American infrastructure is hacked with this kind of persistence: transportation networks, pipelines, or power grids taken down again and again by deep-rooted adversaries. "If they did that in multiple places, you could have up to a month of outages across an entire region," he says. "Tell me what *doesn't* change dramatically when key cities across half of the US don't have power for a month."

It's one thing, though, to contemplate what an actor like Russia *could* do to the American grid; it's another to contemplate why it *would*. A grid attack on American utilities would almost certainly result in immediate, serious retaliation by the US. Some cybersecurity analysts argue that Russia's goal is simply to hem in America's own cyberwar strategy: By turning the lights out in Kiev—and by showing that it's capable of penetrating the American grid—Moscow sends a message warning the US not to try a Stuxnet-style attack on Russia or its allies, like Syrian dictator Bashar al-Assad. In that view, it's all a game of deterrence.

> "It would be hard to say we're not vulnerable. Anything connected to something else is vulnerable."

But Lee, who was involved in war-game scenarios during his time in intelligence, believes Russia might actually strike American utilities as a retaliatory measure if it ever saw itself as backed into a corner—say, if the US threatened to interfere with Moscow's military interests in Ukraine or Syria. "When you deny a state's ability to project power, it has to lash out," Lee says.

People like Lee have, of course, been war-gaming these nightmares for well over a decade. And for all the sophistication of the Ukraine grid hacks, even they didn't really constitute a catastrophe; the lights did, after all, come back on. American power companies have already learned from Ukraine's victimization, says Marcus Sachs, chief security officer of the North American Electric Reliability Corporation. After the 2015 attack, Sachs says, NERC went on a road show, meeting with power firms to hammer into them that they need to shore up their basic cybersecurity practices and turn off remote access to their critical systems more often. "It would be hard to say we're not vulnerable. Anything connected to something else is vulnerable," Sachs says. "To make the leap and suggest that the grid is milliseconds away from collapse is irresponsible."

But for those who have been paying attention to Sandworm for almost three years, raising an alarm about the potential for an attack on the US grid is no longer crying wolf. For John Hultquist, head of the team of researchers at FireEye that first spotted and named the Sandworm group, the wolves have arrived. "We've seen this actor show a capability to turn out the lights and an interest in US systems," Hultquist says. Three weeks after the 2016 Kiev attack, he wrote a prediction on Twitter and pinned it to his profile for posterity: "I swear, when Sandworm Team finally nails Western critical infrastructure, and folks react like this was a huge surprise, I'm gonna lose it."

CURT MERLO

The headquarters of Yasinsky's firm, Information Systems Security Partners, occupies a low-lying building in an industrial neighborhood of Kiev, surrounded by muddy sports fields and crumbling gray high-rises—a few of Ukraine's many lingering souvenirs from the Soviet Union. Inside, Yasinsky sits in a darkened room behind a round table that's covered in 6-

foot-long network maps showing nodes and connections of Borgesian complexity. Each map represents the timeline of an intrusion by Sandworm. By now, the hacker group has been the consuming focus of his work for nearly two years, going back to that first attack on StarLightMedia.

Yasinsky says he has tried to maintain a dispassionate perspective on the intruders who are ransacking his country. But when the blackout extended to his own home four months ago, it was "like being robbed," he tells me. "It was a kind of violation, a moment when you realize your own private space is just an illusion."

Yasinsky says there's no way to know exactly how many Ukrainian institutions have been hit in the escalating campaign of cyberattacks; any count is liable to be an underestimate. For every publicly known target, there's at least one secret victim that hasn't admitted to being breached—and still other targets that haven't yet discovered the intruders in their systems.

> "They're testing out red lines, what they can get away with. You push and see if you're pushed back. If not, you try the next step."

When we meet in ISSP's offices, in fact, the next wave of the digital invasion is already under way. Behind Yasinsky, two younger, bearded staffers are locked into their keyboards and screens, pulling apart malware that the company obtained just the day before from a new round of phishing emails. The attacks, Yasinsky has noticed, have settled into a seasonal cycle: During the first months of the year, the hackers lay their groundwork, silently penetrating targets and spreading their foothold. At the end of the year, they unleash their payload. Yasinsky knows by now that even as he's analyzing last year's power grid attack, the seeds are already being sown for 2017's December surprises.

Bracing for the next round, Yasinsky says, is like "studying for an approaching final exam." But in the grand scheme, he thinks that what Ukraine has faced for the past three years may have been just a series of practice tests.

He sums up the attackers' intentions until now in a single Russian word: *poligon.* A training ground. Even in their most damaging attacks, Yasinsky observes, the hackers could have gone further. They could have destroyed not just the Ministry of Finance's stored data but its backups too. They probably could have knocked out Ukrenergo's transmission station for longer or caused permanent, physical harm to the grid, he says—a restraint that American analysts like Assante and Lee have also noted. "They're still playing with us," Yasinsky says. Each time, the hackers retreated before accomplishing the maximum possible damage, as if reserving their true capabilities for some future operation.

Many global cybersecurity analysts have come to the same conclusion. Where better to train an army of Kremlin hackers in digital combat than in the no-holds-barred atmosphere of a hot war inside the Kremlin's sphere of influence? "The gloves are off. This is a place

where you can do your worst without retaliation or prosecution," says Geers, the NATO ambassador. "Ukraine is not France or Germany. A lot of Americans can't find it on a map, so you can practice there." (At a meeting of diplomats in April, US secretary of state Rex Tillerson went so far as to ask, "Why should US taxpayers be interested in Ukraine?")

In that shadow of neglect, Russia isn't only pushing the limits of its technical abilities, says Thomas Rid, a professor in the War Studies department at King's College London. It's also feeling out the edges of what the international community will tolerate. The Kremlin meddled in the Ukrainian election and faced no real repercussions; then it tried similar tactics in Germany, France, and the United States. Russian hackers turned off the power in Ukraine with impunity—and, well, the syllogism isn't hard to complete. "They're testing out red lines, what they can get away with," Rid says. "You push and see if you're pushed back. If not, you try the next step."

What will that next step look like? In the dim back room at ISSP's lab in Kiev, Yasinsky admits he doesn't know. Perhaps another blackout. Or maybe a targeted attack on a water facility. "Use your imagination," he suggests drily.

Behind him the fading afternoon light glows through the blinds, rendering his face a dark silhouette. "Cyberspace is not a target in itself," Yasinsky says. "It's a medium." And that medium connects, in every direction, to the machinery of civilization itself.
