BORN IN LE BRASSUS

AUDEMARS PIGUET
*Le Brassus*

RAISED AROUND THE WORLD

AUDEMARS PIGUET BOUTIQUES : NEW YORK | ATLANTA | BAL HARBOUR
BEVERLY HILLS | BRICKELL | EAST HAMPTON | LAS VEGAS | MANHASSET

# 打赏 - JUST FOR FUN

> - 支持分享! 一杯咖啡钱, 打赏金额随意，感谢大家~ :)

| 支付宝 | 微信 |
| --- | --- |
|  |  |

资源来自：https://github.com/hehonghui/the-economist-ebooks

# WIRED

JUNE 2020 ▪ WANNA CRY

Inside the Race to Develop a Vaccine
P. 58

WHAT HAPPENED ON THE DIAMOND PRINCESS?
P. 66

**Marcus Hutchins stopped one of the worst cyberattacks in history. Then the FBI arrested him. This is his untold story.**

BY ANDY GREENBERG

## THE ~~HERO~~ ~~CRIMINAL~~ HACKER WHO SAVED THE INTERNET

# FRIEND OR FOE?

**Today's cyber-attackers are masters of disguise.**

Sophisticated email attacks, compromised cloud systems, vulnerable devices - it's hard to predict tomorrow's threats. AI can distinguish between legitimate activity and an emerging cyber-threat, and fight back in seconds.

**darktrace.com**

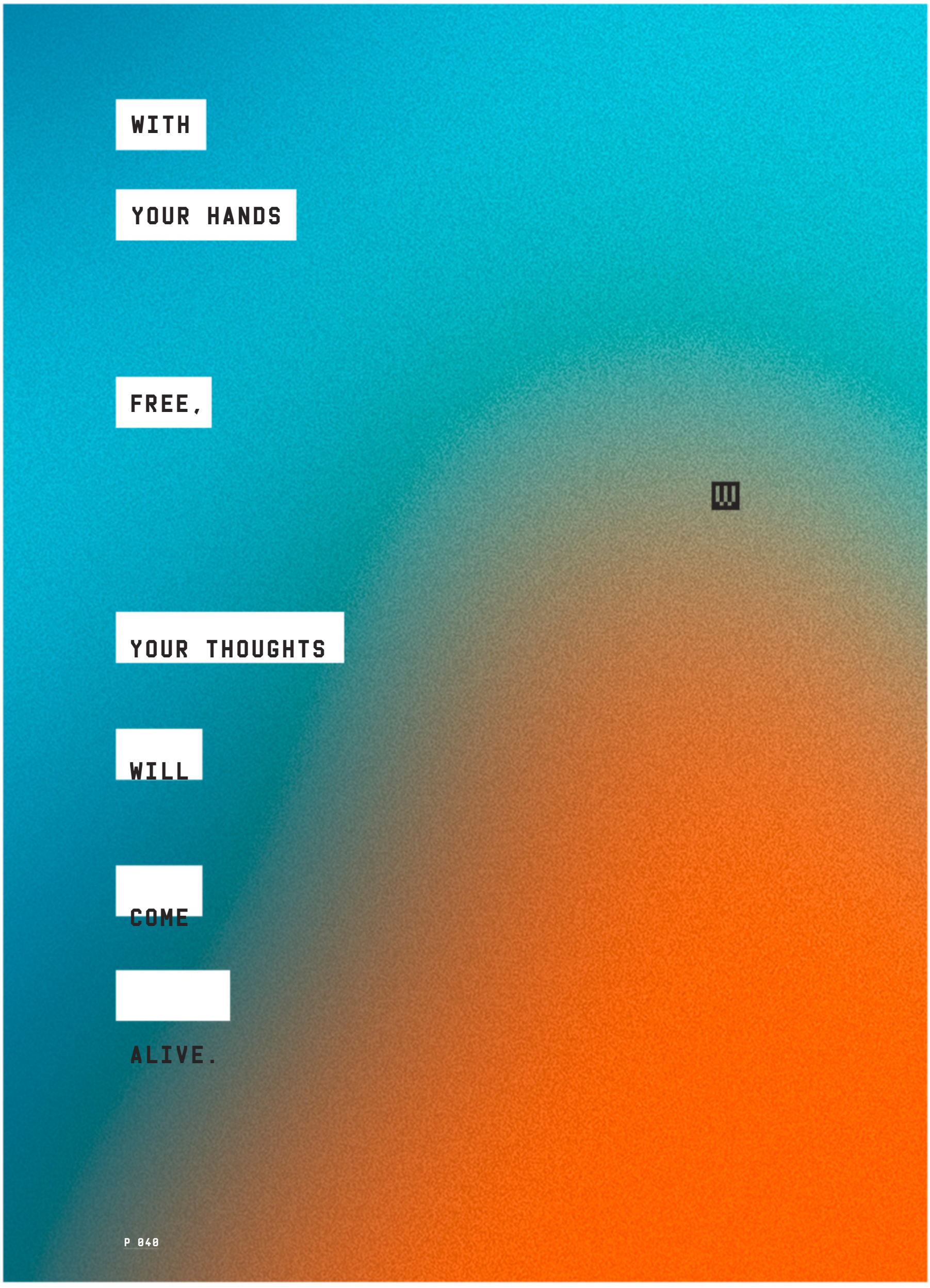

DARKTRACE
World-Leading Cyber AI

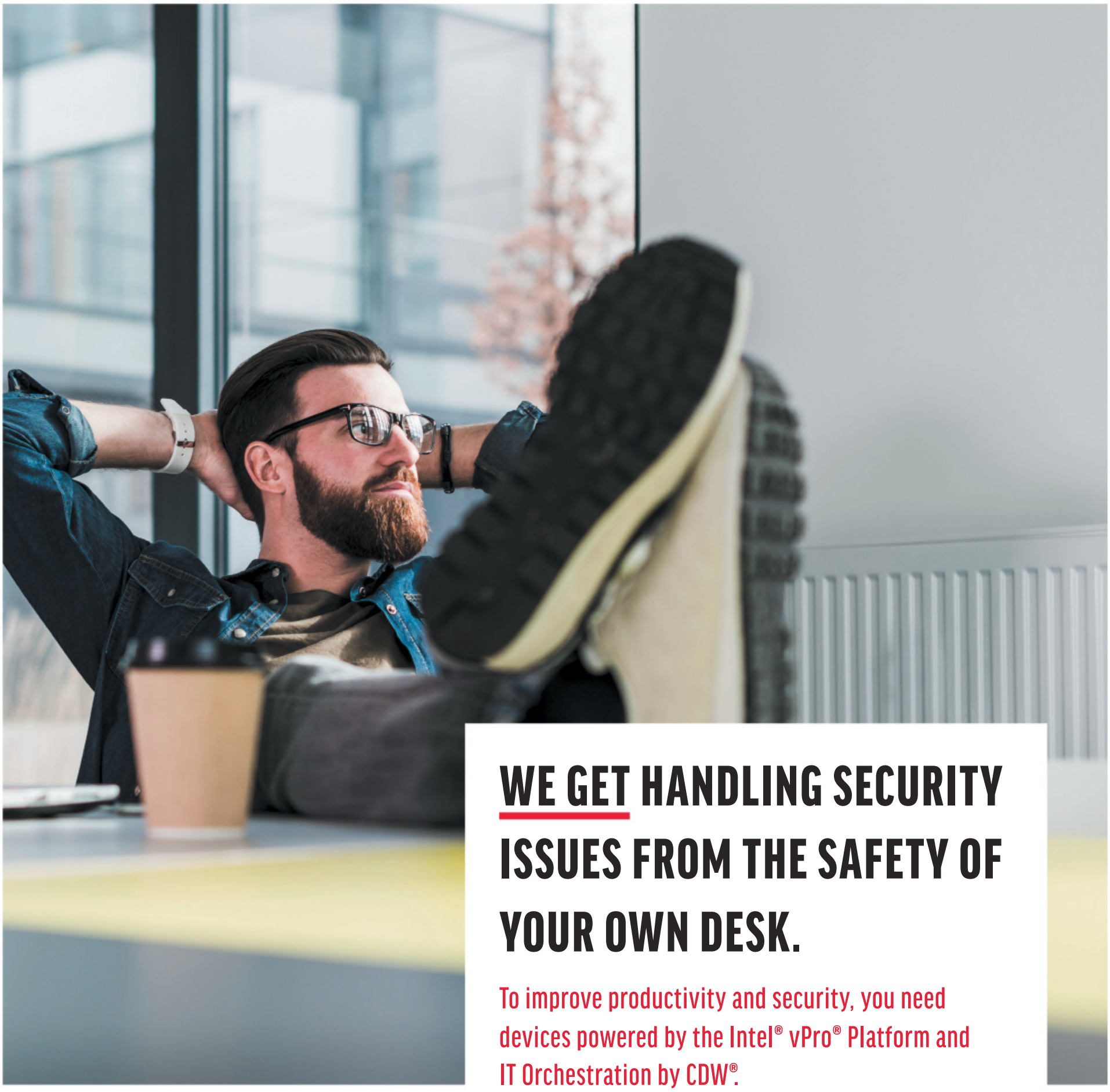
# DO YOU LIKE SAVING MONEY?

Get GEICO.

GEICO®

geico.com | 1-800-947-AUTO (2886) | Local Agent


WITH
YOUR HANDS
FREE,
YOUR THOUGHTS
WILL
COME
ALIVE.
P 040



# WE GET HANDLING SECURITY ISSUES FROM THE SAFETY OF YOUR OWN DESK.

## To improve productivity and security, you need devices powered by the Intel® vPro® Platform and IT Orchestration by CDW®.

With Intel® Hardware Shield and remote manageability, the Intel® vPro® Platform can improve both employee productivity and security while reducing costs. And when they're on devices preconfigured and optimized by the experts at CDW, you'll handle more security issues in less time without having to travel into the field.

**CDW.com/BeGreatMakeTheShift**

Getty Images

## P.66 27 DAYS IN TOKYO BAY

The *Diamond Princess* captivated the world as it docked in Yokohama, harboring the new coronavirus —and 3,711 people, who became reluctant subjects in a life-and-death quarantine experiment.
**by Lauren Smiley**


P.40 **FLYING FISH IS LISTENING**
In China, the tech giant iFlytek knows people by the sound of their voice.
**by Mara Hvistendahl**

P.52 **THE FIVE BIGGEST QUESTIONS IN A.I.**
Machines are learning faster by the moment. How are humans supposed to keep up?

P.58 **PLEASE, LET US BE LUCKY**
Inside the record-breaking race for a Covid-19 vaccine.
**by Brooke Jarvis**

P.78 **THE CONFESSIONS OF MARCUS HUTCHINS**
The untold story of the hacker who stopped WannaCry.
**by Andy Greenberg**


## WE WERE CURIOUS ABOUT THAT TOO

Because you are our greatest curiosity. So we designed a steering wheel with a shape as unique as the hands that grip it. Not just at nine and three, but wherever you hold the steering wheel. Each point, purposefully formed to fit snugly in your palm, giving you greater connection, greater control and greater confidence. So what you grip with your hands, you'll feel in your soul. What amazing ideas will you inspire next? Discover the answer at lexus.com/curiosity.

ERGONOMIC
STEERING
WHEEL

LEXUS
EXPERIENCE AMAZING

# ELECTRIC WORD

P.8 Totally Wired

P.9 Rants and Raves

# ON THE COVER


Photograph
**by Ramona Rosales**

**About the cover**
We sent Ramona Rosales to photograph Marcus Hutchins in Los Angeles while everyone was social distancing. Unlike your cliché hacker, Hutchins goes outside, surfs even. "I found great, bright backgrounds near a business that was closed due to the virus," Rosales says. She and her "assistant" (aka husband) maintained a safe distance as she shot portraits of our cover subject.

# MIND GRENADES

P.13 Metaphors Matter During Pandemics
**by Virginia Heffernan**

P.16 Software Needs to Help Us All Be Stars of the Screen
**by Paul Ford**

P.18 The New Startup: No Code, No Problem
**by Clive Thompson**

P.20 SARS-CoV-2 Gets Its Close-Up
**by Laura Mallonee**

# GADGET LAB: HOME ENTERTAINMENT

P.23 **Fetish**
Roli Lumi keyboard

P.24 **Level Up**
Noise-canceling headphones

P.26 **Screen Time**
Videogames for the lonely

P.28 **Watch List**
Free streaming TV services

P.30 **Sing Along**
DIY karaoke party

P.32 **Game Night**
New Monopoly alternatives

P.36 **Essay**
A lesson in "crisis schooling"

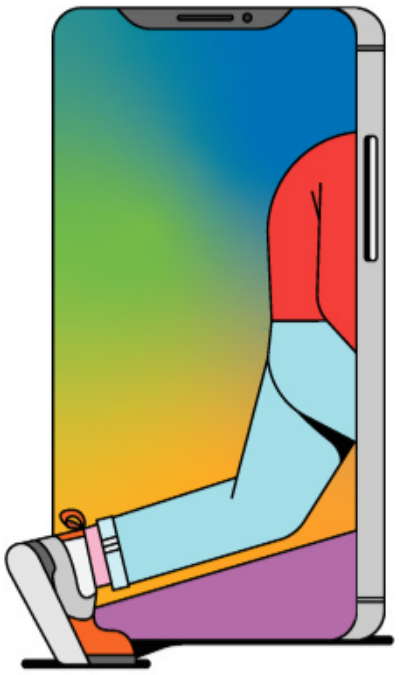
# SIX-WORD SCI-FI

P.96 Very Short Stories
**by WIRED readers**

Top to bottom: Erik Carter, Amanda Ringstad, Maxime Mouysset

# TOTALLY WIRED

## DIARIES OF AN UNBRIDLED DIGITOPIAN



**Well, friends, here we are,** in what they call interesting/crazy/insane times. Here I am, at least; you have your own Here. A There! Yet one blurs into the other—your There contains (metaphysically as well as orthographically) my Here, which can be everywhere. Confused? Welcome to my wonderful life.

Is it a lonely life? Isolated? Without colleagues, friends, kinfolk, skinfolk? Never. While I love my toys, Ripley is, and has always been, a person of the people. Ask my quantum trivia team, my space-ska band (Skarthur C. Clarke for life), or my niece Sheniece. But lean closer—careful, don't bump your head—and I'll tell you a secret, from one Here to another: All of these relationships, these pastimes and pursuits and pleasures, take place at what's come to be called—somewhat regrettably—a "social distance."

Distant? Dismal? I defy such denigrations. Come look at all the tools of my togetherness. Wearables that let me convene in shared phantom spaces. Games that bring old friends together for a nightly ritual of cracking jokes and dispatching Nazi zombies. Zero-latency sights and sounds. Contra the perennial chatter, virtualization technologies thrum with a heartbeat strong and true—and deep within that diodic pulse, intimacy stirs.

Ask my bandmate Karl, who plays the Electronium (and who insists we call him Krazy Khords, but, well, no), if he knows Ripley well. I guarantee he'll be able to describe everything from the melodic wheeze of my laugh to the brand of kelp sherbet you're likely to find in my freezer. Ask Sheniece about the secret handshake she shares with her favorite relative. Sure, all she can really say is that it involves both hands, some spins, and a triumphant yawp, but she can show it to you—because that's how we do it, our meatsack bodies twirling and yawping in our respective habs as our avatars do the same on the beach in Europa.

Human-to-human touch isn't going anywhere; I never said I don't thrill to fleshly contact. My sweet habmate can attest to my appetites, besmooched and benuzzled as they are at this moment, snoozing off our latest tryst. (My randiness is all the more understandable if you've seen my love playing low-g VirtuaBall—that crash suit fits so good in all the wrong places.) But there is succor to be found in sequester too. Before I retreat to my own Here and leave you to yours, I say to you: Take heart. If from time to time we need to maintain some physical space from others, so be it. Who are we, ancient agrarians cowering from the moon? We have a universe of universes alive in our brains and our networks. We need only change our definitions of connection to realize that "together" is in the eye of the besmoocher. See you at the next Skarthur C. Clarke concert.

RIPLEY D.LIGHT
@RIPLEYDLIGHT

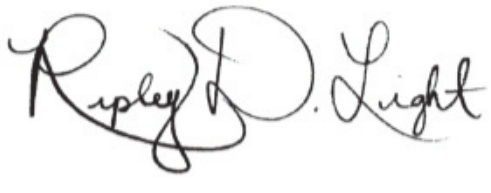


ILLUSTRATION / SAM WHITNEY

# RANTS AND RAVES

## We Have One Earth

For the April issue, we devoted the entire magazine to the *other* crisis of our time: climate change. In its pages, Mary Annaïse Heglar summoned each of us to collective climate action; Adam Rogers pedaled through San Francisco with the head of the city's transportation office; Samanth Subramanian followed the cargo shipping industry's attempt to get off sludge-like heavy fuel oil; Virginia Heffernan wrote about the anthropological endeavors of Impossible Burgers; Emma Marris visited California farms in an effort to separate GMO fact from hype; and readers responded.

**Readers share their optimism, skepticism, and tales of green living:**

### RE: "EMISSION CONTROL"

**"When did capitalism become about getting a free ride?"**

—Peter Gregory, via Facebook

When people talk of conservation, going electric, carbon taxes, they ignore the much bigger fact that the world needs 5 times to 10 times the current power produced to eliminate slums and poverty, to bring the world to some parity. It needs it soon. Since none of that new power should generate $CO_2$, it has to be nuclear: fission now, fusion later. Period, full stop. Your climate issue does not even touch nuclear. When I say nuclear, I mean micro-nuclear, millions of small, safe, no-waste plants, more like generators. Simple fact: Coal has two times the energy density of wood. Uranium has at least 2 million times the energy density of coal. —Nicholas Negroponte, professor, MIT, via email

### RE: HERE'S WHERE YOU COME IN

If you only read one essay about climate action this year—or ever—make it the one by @MaryHeglar. These are healing words at a time when we all need it. —Sarah Katz-Lavigne (@SarahGeoKL), via Twitter

I love how @MaryHeglar reminds me that I'm not crazy for thinking a new world is possible, and that I'm far from alone in this aspiration. —Lena Moffitt (@LenaMDC), via Twitter

### RE: ROAD WARRIOR

Adam Rogers' story made me cry because: One, I'll never write as beautifully. Two, @jeffreytumlin just redesigned SF's entire freaking bus system in a weekend. Three, it made me yearn for a time of solving simple problems like dismantling freeways. —Alissa Walker (@awalkerinLA), via Twitter

Today's quieter streets are a huge opportunity to make lasting change. Planners, engineers, grab a notebook and camera, get out of your home offices for a while, and see your cities through fresh eyes. —Martyn Schmoll (@martynschmoll), via Twitter

### RE: THE SHIPPING POINT

I am in ocean shipping. One thing you didn't mention is the lack of use of the coastal ocean routes between US ports. The fuel savings by using direct ocean routes can be substantial. —Bill Lauderdale, via mail@WIRED.com

### RE: BY ANY SEEDS NECESSARY

I have no doubt that GMO technology could be used in a responsible way, but I have zero confidence in the ability of the government to regulate effectively so that our land-grant universities have the ability to get this technology into the right hands. If breeding programs were able to revert to the farmer-scientist public collaborations that produced most of our modern food crops, GMO use in organic agriculture would be a much easier sell to organic stakeholders. Until then, what I'm afraid of is not the tech, but the monopolistic control of said tech by a few massive corporations who have shown that they have no interest in food-system health. —Robin Turner, Roots and Shoots Farm, via mail@WIRED.com

### RE: MEATSPACE

As it becomes more obvious that using animals for meat drives not only global warming but pandemics, removing animals from food production will become ever more pressing. Fortunately, we now understand how to use plants to create plant-based meat that tastes identical to animal-based meat. We can grow real animal meat directly from cells, with no contribution to antibiotic resistance or threat of starting the next pandemic. —Bruce Friedrich, executive director, Good Food Institute, via mail@WIRED.com

Even beef can be part of the equation. Instead of factory farms, there are operations that are climate positive and actually carbon negative. —Bernard Baran, via mail@WIRED.com

### GET MORE WIRED

If you are a print subscriber, you can read all WIRED stories online. To authenticate your subscription, go to: WIRED.com/register.

Illustration by Alvaro Dominguez

# THE NEW REALITY OF WORK

**The COVID-19 pandemic triggered seismic shifts in our social, political, and economic lives. Since early March, tens of millions of workers shifted out of offices and into their homes as physical distancing and shelter-in-place mandates attempted to slow the spread of the deadly virus.**

**BUSINESSES HAVE LONG EXPERIMENTED WITH WORK-FROM-HOME POLICIES**—laptops, smart phones, the ubiquity of fast and reliable Internet, and virtual meeting software made it easy and convenient. Few companies tried to enable a remote workforce on this large a scale, however, and none this quickly.

## A RAPID TRANSITION

But within just a few short weeks, it was clear that the aspirational future of work was the new IT reality.

Suddenly, massive numbers of newly remote employees were accessing sensitive company resources and corporate networks, many via insecure devices and connections. Malicious actors quickly took advantage of this state of flux, probing Wi-Fi configurations, VPN connections, and network firewalls for security vulnerabilities.

Capitalizing on the confusion brought on by the pandemic, they launched relentless attacks on corporate and remote users, using malware, spam, phishing campaigns, fake sites, and ransomware. But even as cyber criminals moved to exploit the upheaval, IT organizations mobilized to manage the disruption instead of improvising through the chaos.

Their number-one requirement: improved visibility across all activity in their environments.

For one financial services organization that meant establishing monitoring for a flood of network traffic from newly displaced workers. Their IT team powered up 1,500 remote employees in a little over a day. Many were call-center employees using their personal computers to access sensitive applications—a sudden gear shift that required configuring more than 600 new VPNs.

The firm employed network detection and response (NDR) technology from ExtraHop to confirm that new services were properly configured and secure. The organization then extended NDR to their cloud workloads to provide a real-time perspective of their applications and quickly identify anomalous traffic patterns indicative of a compromise.

PRESENTED BY

ExtraHop

> "This is now the reality of IT and it must be done without compromising security or access."
>
> **RAJA MUKERJI,** co-founder and Chief Customer Officer, **ExtraHop**

## THE FUTURE OF WORK

The swift transition of the past few months has been painful for the security and IT departments across almost every industry. While the first wave of this "new normal" was about access, many organizations are planning for the next phase, which will be about predictable availability and continuity.

Security will play a central role. It must be done with proper configuration, policies, and enforcement, and include the ability to detect and respond to threats not only within the data center but across cloud workloads and out to the edges of where the devices are located.

"This is now the reality of IT," said Raja Mukerji, co-founder and Chief Customer Officer at ExtraHop. "It must be done without compromising security or access." Companies that ensure a secure transition to remote work today will be well equipped to support a more agile, adaptable workforce.

## HOW CAN EXTRAHOP HELP?

No one can predict the future. But we can strengthen the bedrock security that helps companies maintain business continuity amid widespread disruption and uncertainty. ExtraHop is dedicated to supporting our customers through this time every step of the way.

With ExtraHop, IT departments can assess the security posture of remote access configurations across their environment—from the data center to the cloud—and proactively identify mis-configured services and ports (like RDP) to prevent attacks.

ExtraHop Reveal(x) helps organizations reduce security friction and speed cloud adoption with cloud-native network detection and response (NDR). Our SaaS model eliminates deployment headaches and allows for unified management from the cloud, to the data center, to the IoT and user edge. Reveal(x) is also cloud-agnostic, providing detection and response capabilities across multiple clouds in a single UI. Because Reveal(x) uses network traffic to perform sophisticated machine learning for advanced behavioral detection, organizations can monitor any device communicating over that network or accessing network resources—whether it's an employee or intruder.

**WE'RE HERE TO HELP DURING CHALLENGING TIMES. TO LEARN MORE ABOUT OUR WFH RESOURCES, HOW-TO VIDEOS, AND SECURE A FREE TRIAL OF REVEAL(X), GO TO WWW.EXTRAHOP.COM/FUTURE.**

# There's More to Vari® Than Desks

You may know us for the popular VariDesk®, but Vari has seating, storage, tables, lighting, and so much more—all shipped, delivered, and installed for free*. We make it easy for you to create a workspace that can grow and change whenever your business does.

**Get started with your free space plan today at vari.com/wired or call (877) 291-8881.**

vari®

*Free delivery in the contiguous US. Free installation on qualifying orders in the contiguous US.See vari.com/installation for more details. | Availability subject to change

# METAPHORS MATTER

**Warfare may be a rousing way to speechify, but it's perilous when used to describe disasters from Hurricane Katrina to pandemics.**

BY VIRGINIA HEFFERNAN

Vibrating, near-hallucinatory, the Manú National Park in Peru is among the most biodiverse places on earth. Just about every one of the park's 4.3 million acres, where the Tropical Andes meet the Amazon Basin, seethes with raw biology—at least 1,300 species of butterflies and 650 of beetles; numberless white-lipped peccaries, tufted capuchins, green anacondas, turquoise tanagers. Flora and fauna to infinity. ■ It's also the zoomed-out version of a landscape closer to hand: the one that runs up our noses and through our twisted guts. What human flesh lacks in jaguars, it makes up for in microorganisms of every stripe: 10 to 100 trillion swarming creatures, thousands of distinct species of bacteria, viruses, fungi, archaea, and protozoa, which means our bodies at any given minute may contain tens of millions of foreign genes. ■ Why go through all this again, the hideous miracle of the human microbiota? ➜

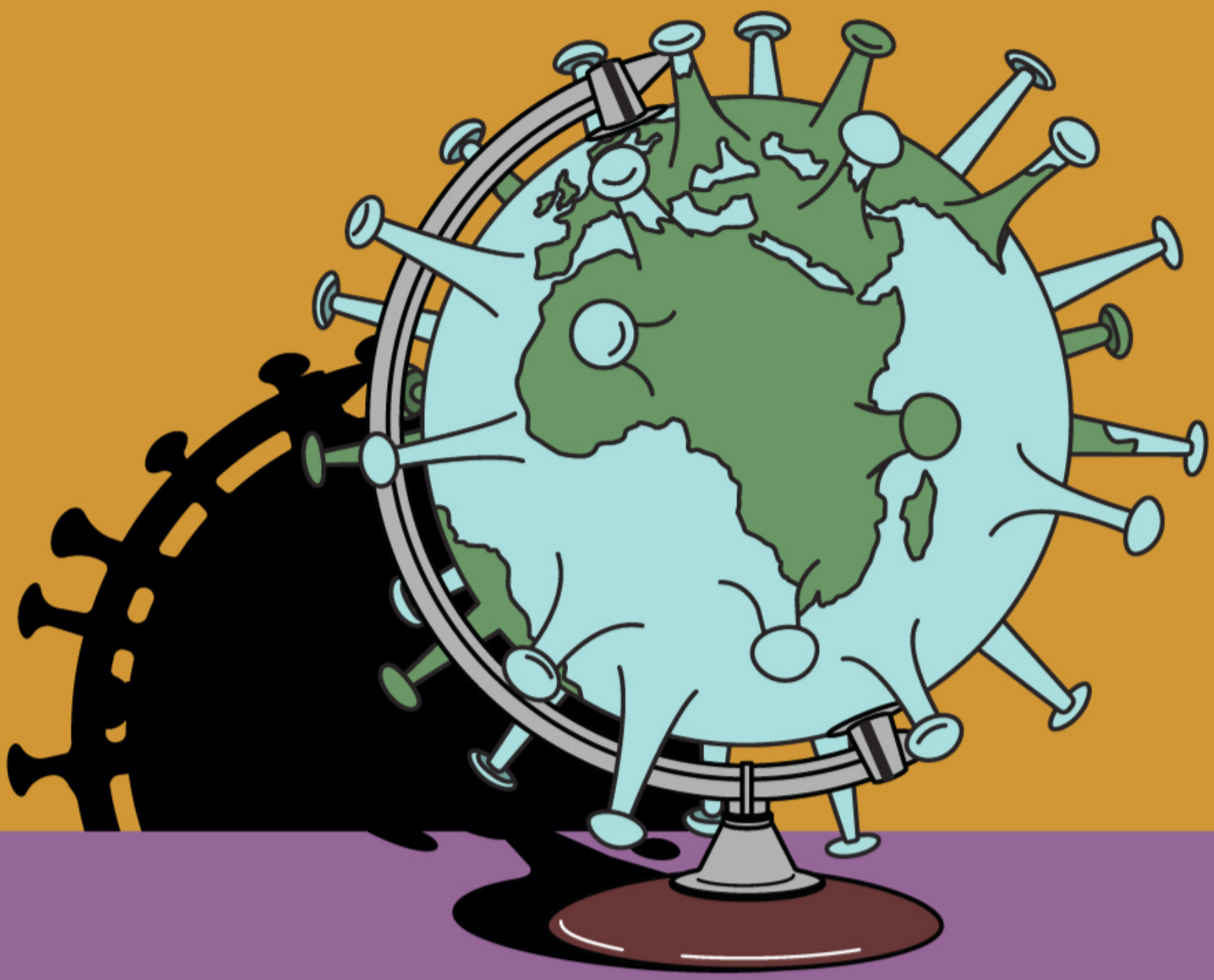


ILLUSTRATION / SAM WHITNEY

Because our teeming abdominal and nasal rain forests are of course contending with a stranger: SARS-CoV-2. The virus has upset the human microbiome in an epochal act of strategic surprise.

Almost instantly, that shock generated a set of metaphors drawn from warfare. This may be inevitable in a time of great fear. But more useful models for confronting a pandemic may come from the microbiome itself—and from the mechanisms, from human care to life-extending machines, used to give our immune systems time to learn the signatures of a new virus. In hypermagnified vanity portraits, the coronavirus that stopped humanity in its tracks this winter looks like the fearsome head of a medieval morning star, fit to kill in a gory blunt-force-puncture attack. SARS-CoV-2, like all viruses, is a biological entity, but it is, many virologists contend, something less than alive; it contains genetic information, but it can't reproduce. Zania Stamataki, a viral immunologist at the University of Birmingham in the UK, likens viruses to robots.

The image of maces or robots bearing spikes and cracking open our cells does at first conjure a military attack. Indeed Bill Gates has said we ought to have prepared for a pandemic as if for armed conflict. In March, Donald Trump dubbed himself a "wartime president." More recently, military veterans have urged people enduring the Covid-19 contagion to think like prisoners of war.

But Scott Knowles, a disaster expert who runs the history department at Drexel, is wary of martial language. Warfare may be a rousing way to speechify, he has written, but it's perilous when used to describe disasters from Hurricane Katrina to pandemics. For one, if we're at war, we expect command-and-control rather than the spontaneous volunteerism we've seen with self-isolation and self-quarantine. War rhetoric also suggests that sacrificial casualties ought to be sustained in the name of patriotism. And, finally, it allows for bad or even inhumane decisions excused as a consequence of the "fog of war."

"We have another set of metaphors at hand," Knowles told me by email. "They're tailor-made for our moment: the metaphors of science and medicine. Doctors, nurses, and support staff work with urgency, but their goal is life, not death. Their mandate is not to save the nation but rather to support humanity." The language of instruction, practice, and the "do no harm" principle could have more explanatory and even predictive power than those drawn from war.

Humanity is externally heterogeneous, of course, and responses to the pandemic must be shared among nations. But each of us is internally heterogeneous also, filled with Manú-caliber biodiversity that defies the us-and-them rhetoric of war. "Support"—as in life support, which extends the resources of an individual with community and technology—carries that plural with it. A single human must indeed pluralize, as she sounds an alarm, makes a 911 call, to multiply her resources with human community and medical professionals, who expand her body's capacities with everything from words of comfort to Tylenol to IV hydration. When nurses and doctors further use ventilators and dialysis with a Covid-19 patient, the machines serve as supplementary lungs and kidneys to give her immune system time to get sorted.

As unlikely as it seems in the thick of this pandemic, one day the new coronavirus will be priced into public health and economic calculations. The American health care system will never again be caught so short of protective gear, ventilators, and hospital beds. And then there's the fate of the virus itself, which will join the swarm of microbes in which humans exist. If a vaccine arrives, we'll deliberately take it in, in small inoculating doses.

In wartime, an enemy army must be styled as hostile to allow for its destruction, but an insensate, nonliving virus has no such valence. Human bodies don't aim to murder a new virus. "Viruses aren't alive," Janelle Ayres, a molecular and systems physiologist at the Salk Institute, put it in an email. "So it doesn't make sense to discuss them in terms of killing them." Instead, immunologists speak of neutralization. The immune system can sometimes incorporate an initially alien virus into its repertoire, the way the mind, with study, might absorb a difficult foreign word into its vocabulary.

**Our bodies must make overtures that combine the microbial version of suspicion, curiosity, and detachment. We have to become doormen to the virus, not doormats.**

To pull this off, unsuspecting human organisms are compelled not to contract in a defensive crouch but to expand. Once the bug is inside us, its spikes attach to cell membranes. The virus fuses with the subjugated cell, sheds its spikes, and releases nucleotides inscribed with hijackers' demands. *Make more like this*, the orders go. *And here's how: a cup of protein, a cup of lipids, and a tablespoon of nucleotides.* (Measurements not to scale.) Our physiologies are now forced, on pain of death, to respond to this violent guest. We can't now lock the virus out, as if it were an invader. But nor can we throw open our arms to it, as if it were a friend. As Stamataki grimly notes, humans did indeed welcome the virus in—to our habitats, our houses, and our noses. Our bodies must make overtures to it that combine the microbial version of suspicion, curiosity, and detachment. We have to become doormen to the virus, not doormats.

Certain patients seem to have cells that

are easier to open and more readily forced into compliance with the nucleotides. But if their bodies hustle too obediently to satisfy the demands of the virus, before immune cells announce the breach, vital organs might be overrun. The virus has been accommodated, but at the expense of the organs of the host. In some patients, according to Randy Cron, a rheumatologist at the University of Alabama at Birmingham, an immune system might rev too high, oversupplying molecules called cytokines that, though usually protective, can attack and destroy vital organs. Some Covid-19 patients may die of the virus; others die of their own excessively aggressive immune response.

In some 97 percent of international cases, according to a preliminary estimate in *The Lancet* in February, the new coronavirus is said to "resolve." What of the coronavirus particles—the ones whose spikes have been rendered impotent by antibodies—that persist in the bodies of those who outlive the siege? They're neutralized—and bounced out. Now their image is on a blacklist: If the body encounters Covid-19's face, the virus, it seems, is rapidly disarmed. When and if a vaccine is developed, it will also likely teach the body, more quickly and at lower cost to our cells, what to look out for. This isn't war. It's enlightenment.

Rookies, once initiated, are often asked to do the worst chores. So too the new antibody, with its powerful memory, will have to play bouncer, spotting and neutralizing chaos agents at a glance. And there will be more breaches. There will likely be another Covid season, and another, and another. But the virus will be known and seen—familiar as a regular, if troublesome, visitor to the jungle of bugs inside us.

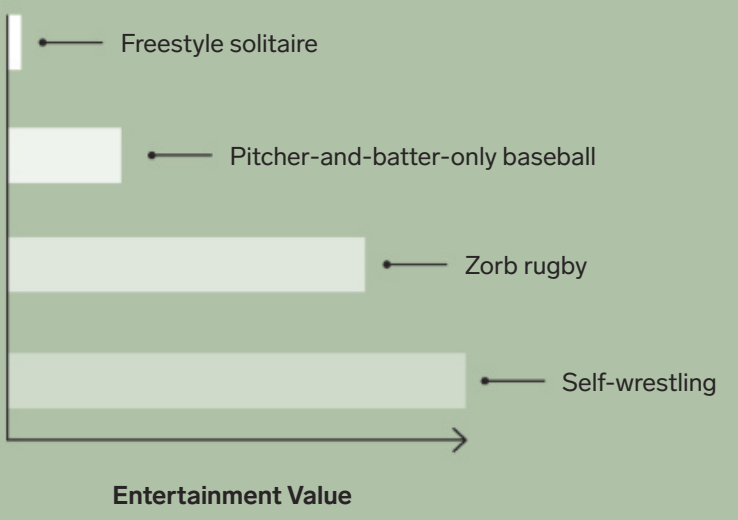
Once we learn a particular operation—in math, say—we can recognize and solve problems that require it when they surface the next time, with decreasing effort. We'll recognize this pathogen when it comes around again. During the vertigo of the quarantine spring of 2020, one of the few consolations is that this coronavirus will never be novel again.

VIRGINIA HEFFERNAN *(@page88) is a regular contributor to* WIRED.

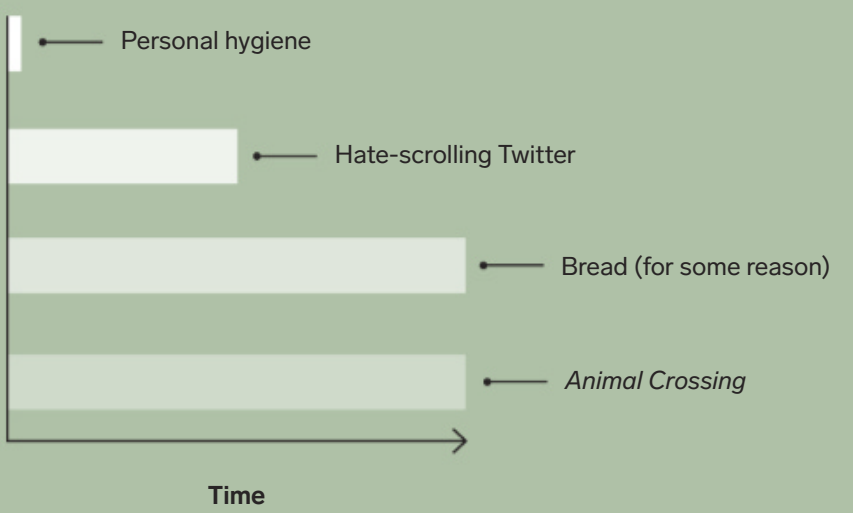
## CHARTGEIST

BY JON J. EILENBERG

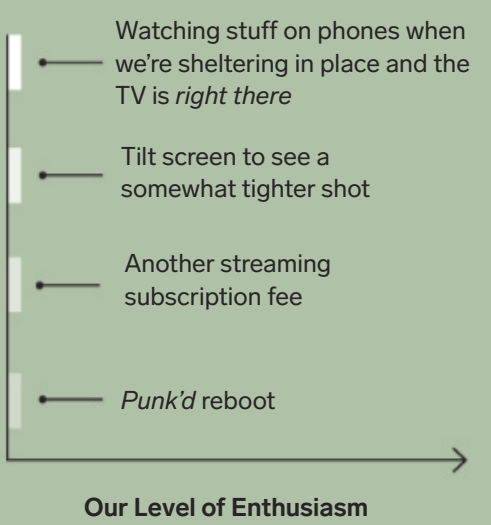
### RESPONSIBLE POST-REOPENING SPORTS

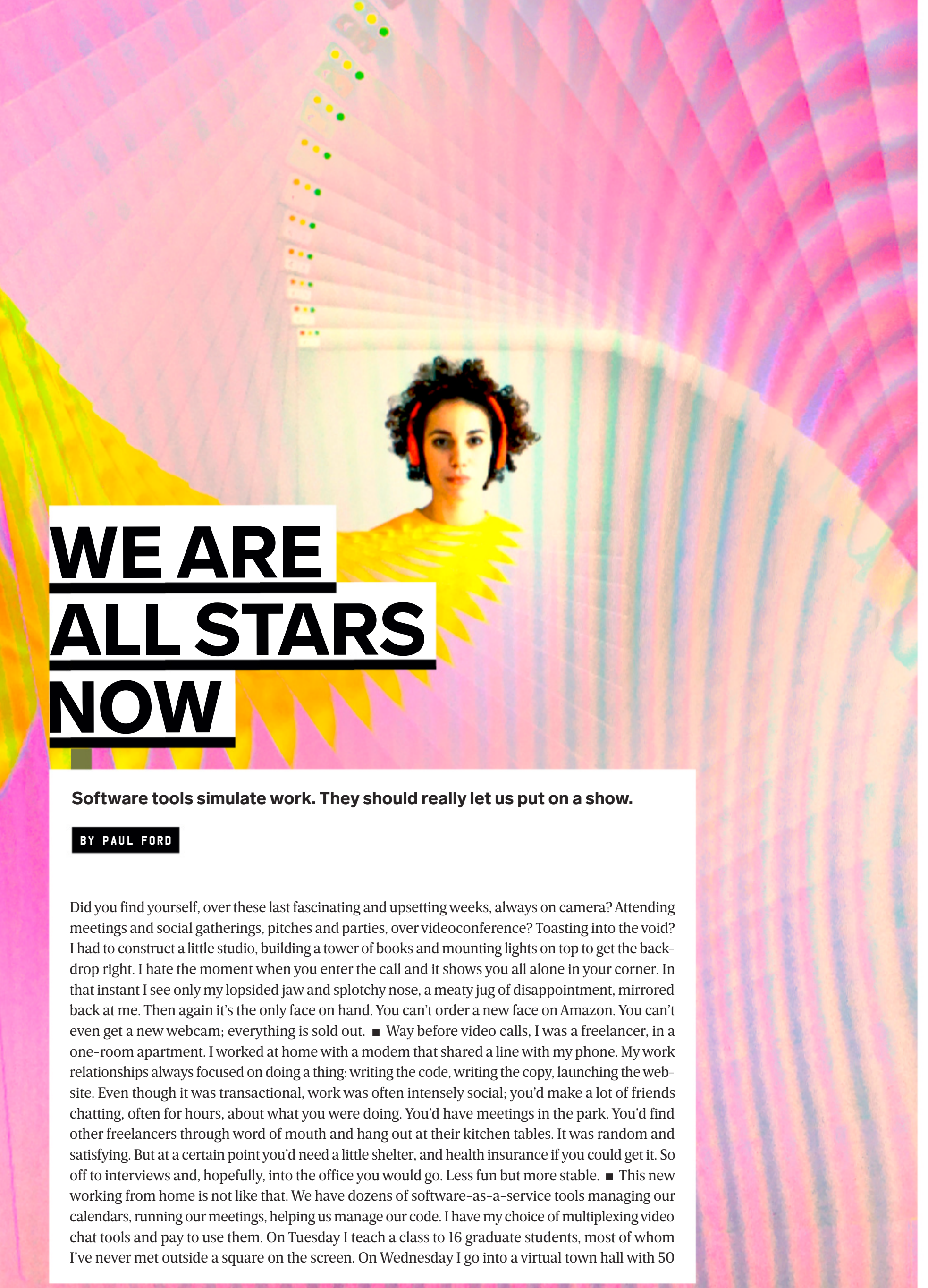



### HOW WE'RE SPENDING OUR QUARANTINE




### THE QUIBI EXPERIENCE





# WE ARE ALL STARS NOW

**Software tools simulate work. They should really let us put on a show.**

BY PAUL FORD

Did you find yourself, over these last fascinating and upsetting weeks, always on camera? Attending meetings and social gatherings, pitches and parties, over videoconference? Toasting into the void? I had to construct a little studio, building a tower of books and mounting lights on top to get the backdrop right. I hate the moment when you enter the call and it shows you all alone in your corner. In that instant I see only my lopsided jaw and splotchy nose, a meaty jug of disappointment, mirrored back at me. Then again it's the only face on hand. You can't order a new face on Amazon. You can't even get a new webcam; everything is sold out. ■ Way before video calls, I was a freelancer, in a one-room apartment. I worked at home with a modem that shared a line with my phone. My work relationships always focused on doing a thing: writing the code, writing the copy, launching the website. Even though it was transactional, work was often intensely social; you'd make a lot of friends chatting, often for hours, about what you were doing. You'd have meetings in the park. You'd find other freelancers through word of mouth and hang out at their kitchen tables. It was random and satisfying. But at a certain point you'd need a little shelter, and health insurance if you could get it. So off to interviews and, hopefully, into the office you would go. Less fun but more stable. ■ This new working from home is not like that. We have dozens of software-as-a-service tools managing our calendars, running our meetings, helping us manage our code. I have my choice of multiplexing video chat tools and pay to use them. On Tuesday I teach a class to 16 graduate students, most of whom I've never met outside a square on the screen. On Wednesday I go into a virtual town hall with 50

or 60 wee square faces looking back at me. I talk too much because I need to fill the air. The faces blur in a way that makes me feel ashamed. How can I pretend to know these postage-stamp people? There are buttons for raising your hand and buttons for applause.

It's awful. I'm too much at the center of my weird little world, alone with my thoughts and my USB microphone. And my calendar is full of these meetings. There's no time for long conversations that stabilize the mind, that allow you to perceive the world as others see it.

It's the simulation of work. Take video chat programs like Meet, Zoom, BlueJeans. These are meeting emulators. They attempt to copy and repeat the form of the meeting but don't capture the actual interactions. You can't read a room, take its temperature. Your little jokes fall flat. Your spine doesn't tingle when things are going well.

I love a real-life meeting. There, I said it. They're theater, and I'm a ham. You plan and prepare, you make a deck, you try to surprise. Meetings, well run, are alchemy; you can turn words and pictures into large checks or people agreeing to work for you, or convince a big company to do something it hates to do. An hour? Two hours? Stop crying. Lock me in a room for three days with a team of five strangers and a stack of sticky notes as high as your eye. Right now I'm 5,000 words into organizing a six-week seminar on knowledge management. I believe firmly in the principle of exhaustion: Once you see them start to collapse, that's your time to glow. Leave the room, splash some water on your face, and get back in there and win. You don't see meetings in terms of who won and lost? Why are you even going to meetings?

But now I'm trapped. I feel two-dimensional. I desperately need to break out of this simulation. After days of muting and unmuting, I go out searching for some software or pattern that will feel less fake—something to do, something to show. What I learn is that, of course, some people have solved this already.

I download a piece of software called OBS, which is an open-source video and audio mixer. It turns your computer into a little mixing room, except that instead of anchors and cameras and mixing boards, it's the different windows on your desktop, the game you're playing, webcams, video from a friend's webcam—it is software that turns digital things into sources of sound and light and lets you arrange them into scenes and fade between them.

You can shrink your head and put it into the bottom right corner. You can play a game or a video, or bring up your text editor and share that. You turn your whole digital reality into a TV show and then select your livestreaming service from a dropdown. Of course the dropdown options today seem to be mostly oriented around videogames or porn, Twitch streamer or cam girl.

I see other people discovering OBS. People download it and complain on Twitter about how it doesn't quite work. Out of the blue, the CEO of Shopify issues a $10,000 bounty for anyone who can make the "virtual camera" software that will link OBS (on a Mac) to Google Meet or Zoom. "I know a lot of people who need OBS now but to broadcast into video conferencing software like zoom/meet/teams," he writes in a GitHub commit.

**I'm trapped. I feel two-dimensional. After days of muting and unmuting, I go searching for some software that will feel less fake.**

My cofounder, who truly loves a good uncomfortable moment, uses a website called Renderforest, and we start adding videos to meetings, overdramatic introductions and announcements of new projects, ridiculous vaporwave scenes, and images of animated people in a cityscape. An imaginary camera pans up and over to reveal, on our building, our logo. What's more ridiculous than purposefully awkward corporate fun? Someone online will take $100 to bring a llama to your video call. It's called Goat 2 Meeting. I am tempted.

We are all livestreamers now.

I start writing a tiny bit of custom software, in the evenings, since there's not much else to do besides bake bread and care for your own health and well-being, neither of which interests me too much. My software shows nice layer-cake diagrams, with components all in harmony and shades of blue. This is a story I usually tell with rectangles in a slide deck, but now, when you click on a component, words pop up, things change. The data is coming alive! You can poke around and show connections. I'm leaving the bottom right of this little app a blank white space, so that I can squeeze my face into it.

I have a lot of fantasies about how it will go. We'll be paging through some boring-ass Google Slides, and I'll say, *Let me switch over to our Custom Platform Explorer,* and my face will swoop down into the bottom right corner, and people will think, *I've never seen this before. I must give this man my money so he can make me things.* Our competitors will be using PowerPoint and Skype, like medieval peasants or big-company automatons. Whereas we'll be corporate Coppolas.

Stop thinking of an office as a meeting place. Think of an office as a cineplex, each conference room a theater of craft and discipline. In my fantasies the networks are always fast and the software never crashes.

I think my idea will become a component of much future software: the empty space where you put your face. *Tune into my livestream, aka any meeting. Let me show you not just slides or ideas but the actual thing that is being made. Chat amongst yourselves. I welcome the back channel. If you miss the show, I've recorded it and it's transcribed in the enormous library of videos that will define our culture.* Yes, that will be the future. We're headed that way. We're all going to be streams of live data, games and toys and windows. It's unavoidable. We should welcome it, in fact. Spend time, spend money, and make this happen. And then, after I think these very important thoughts, my spouse and I do our donations, and then we take our two children onto our little balcony, carrying pots and pans. It's 7 pm and time to cheer for health care workers and first responders, and to wave across the wide street to the neighbors, we who are real, and come from all around the world.

---

PAUL FORD *(@ftrain) is a programmer, essayist, and cofounder of Postlight, a digital product studio.*

Getty Images

ILLUSTRATION / ERIK CARTER

# NO CODE, NO PROBLEM

**Now you don't need to know any programming to launch a startup. We've been approaching this moment for years.**

BY CLIVE THOMPSON

Dani Bell was a British copywriter who hankered for her own marketing startup. Like many founders today, though, she faced a roadblock. She couldn't code. ■ Normally, an entrepreneur in that situation would need to spend money, and maybe even raise it, to hire developers. But Bell did something different: She bolted together software from various online services. ■ Bell used a point-and-click tool called Webflow to build her site and a client-management tool to let customers order services. Airtable, an online spreadsheet, let her store details about each job. And she glued many of these pieces together by cleverly using Zapier, a service that uses if-then logic to let one online app trigger another. (Whenever Bell creates a new task for one of her contractors, for example, Zapier automatically generates a Google doc for it, then pings her on Slack when the work is done.) Nineteen months later, her company—Scribly.io—had around 23 clients and was doing $25,000 a month in recurring business. ■ In essence, Bell built a startup without writing a line of code. She did it all her-

self, aided by advice from folks building the same scrappy systems. Sure, it's a bit of a Rube Goldberg machine. "They're a patchwork," Bell admits. But overall, it's "good enough, and usually good enough is perfectly OK." In the long run, she might get big enough to hire a coder to make a custom system. But, for now, it works.

Behold the trend known as "no code" (or "low code"). In the past few years there's been a flowering of tools like those Bell used, all aimed at the nonprogramming masses.

**"I code. But it's tedious. I feel like it's not reasonable to expect, you know, the vast majority of the population to be careful with their commas."**

It neatly inverts the cultural logic around programming and its unique value. A decade ago the rallying cry "Learn to code" emerged. The key to tech-fueled entrepreneurship—and its promise of independence and possible riches—was in learning to sling JavaScript or Python. Boot camps bloomed.

Nuts to that, say the proponents of no-code. "Coding sucks," laughs Emmanuel Straschnov, cofounder of Bubble, a service that offers a suite of tools for nontechies to build apps. "I mean, I code. But it's tedious. I feel like it's not reasonable to expect, you know, the vast majority of the population to be careful with their commas." Indeed, one measure of social progress is how well we automate complex skills for normies, he argues. We became competent photographers not by honing our skills at hand-developing film but by using iPhones with filters.

The emergence of no-code is, in a sense, the ur-pattern of software. We've been drifting this way for years. Websites at first were laboriously hand-coded, until blogging CMSs automated it—and blogging exploded. Putting video online was a gnarly affair until YouTube rendered it frictionless—and vlogging exploded. As no-code advances, "the amount of products is just going to skyrocket," argues Nate Washington, an Atlanta entrepreneur who used the Bubble tool to help create the first version of Qoins, an app that helps people pay off debt by automatically rounding up on purchases and sending the money to creditors. Four years later, Qoins has helped users pay off $11 million in debt.

As with all plenitude, we'll get a flood of silly startup ideas and only a few great ones. But no-code could be an even bigger deal for more mature firms. For example, Eric Astor, founder of the vinyl-album-pressing company Furnace, has long run his business on FileMaker Pro (an early no-code tool, really). Lately he's started outfitting his presses with IoT sensors, then using a new low-code tool called Claris Connect to autoreport their conditions. "We're capturing data that only big companies used to be able to afford," Astor tells me. "We're still a ragtag shop; we don't have the budget to go and hire consultants."

One could criticize no-code for not offering the flexibility and nuance you can get by writing your own code, line by line. But the truth is, for all the hoopla about Silicon Valley's innovative genius, a huge number of apps don't do much more than awfully simple things. Seriously: Silicon Valley's *main trick* is just shoving things into a database and pulling them out again. I'm exaggerating, but only a bit.

The success of no-code startups may thus be a useful corrective to the cult of the Brilliant Tech Dude. If nearly anyone can do this, some of the magic dies. And some new magic, possibly, is born.

CLIVE THOMPSON *(@pomeranian99) is a* WIRED *contributing editor. Write to him at clive@clivethompson.net.*


## NOT YOUR DAD'S APOCALYPSE

**The shock itself is shocking. Shouldn't we have been more prepared for the end of the world? Culture has been drenched in catastrophe porn for decades. *The Day After Tomorrow. 28 Days Later. The Road. Children of Men. Zombieland. I Am Legend. World War Z.* Though the heroes of these movies—straight boy-men with nuclear families to defend—are cut off from the rest of society, part of the fantasy is relief: Marauding biker gangs in bondage gear might want to murder you for half a tank of diesel and a sandwich, but at least you don't have to worry about your credit history anymore. Or your college debt. Or your neighbors. Well, exactly none of that infantile psychology predicted the reality of Covid-19. For one thing, the world feels larger now, not smaller. We're all frantic to connect and touch. For another, the people on the front line are not fighters. They are healers, caregivers, deliverers. (Turns out the very people whose work is rarely paid in proportion to its importance are the ones we need most when the dung hits the Dyson.) Still, you hear the same gleeful, muscular, Hollywoodized anticipation everywhere from alt-right forums to the rhetoric of "dark green" eco-fundamentalists: The coronavirus is nature's revenge on humanity! It's a cleansing Armageddon! If you are really so keen to be punished, there are websites for that. If you find yourself eager to see the whole species punished, that's not a fetish, that's fascism. In the end, what we're doing looks less like butchery and a good deal more like bakery—dry active yeast is suddenly the bartering commodity du jour. So let's be kind, pass around our gummy homemade bread, and survive this time of monsters.**

ILLUSTRATION / ELENA LACEY

# ZOOM WINDOW

**A viral close-up, thanks to electrons.**

BY LAURA MALLONEE

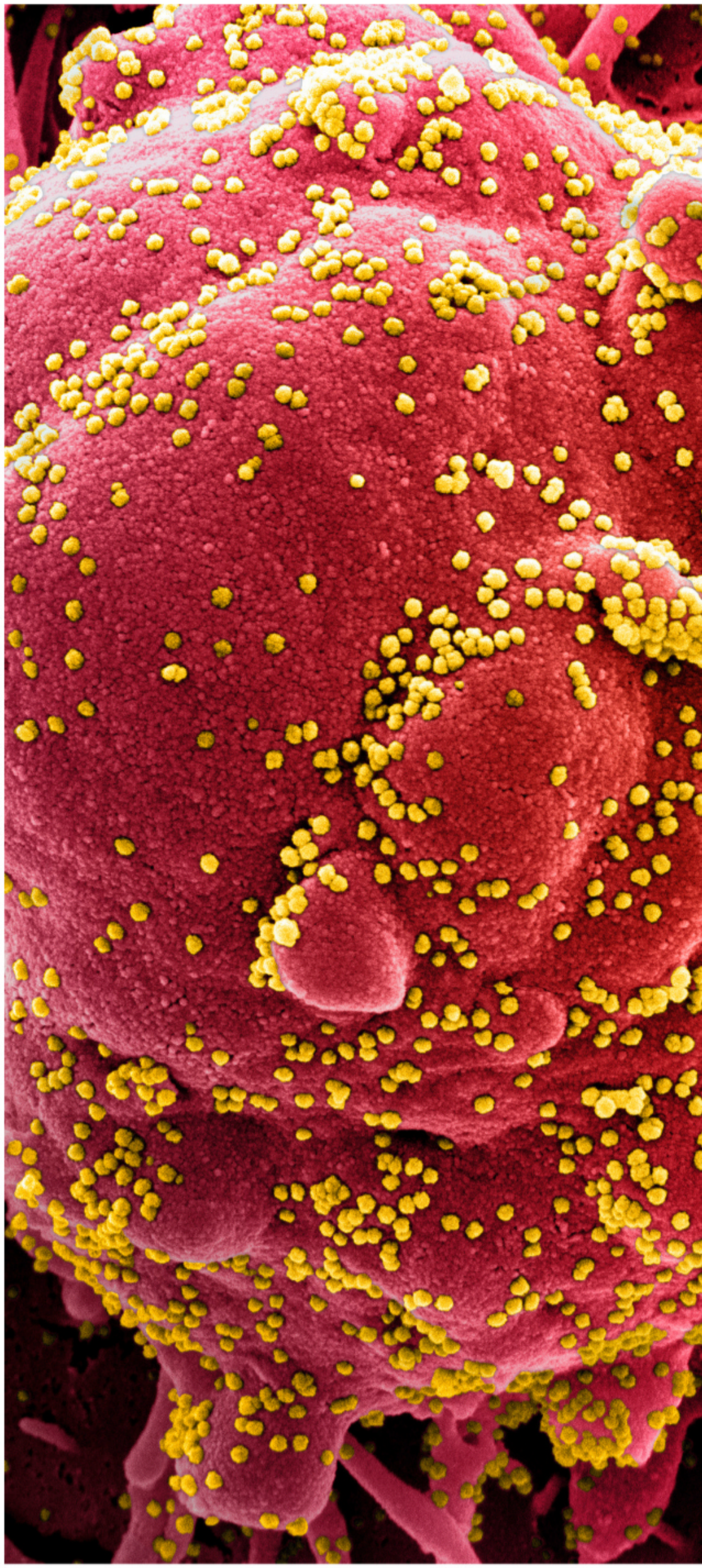
The president calls SARS-CoV-2 the "invisible enemy." Sure, at some 0.000003 inches across, the virus evades the naked eye. But luckily for us, virologists have a tool to render the pathogen quite visible, thanks to British physicist Joseph John Thomson. In 1897, Thomson discovered the electron, a particle too teensy to be measured. Just over 30 years later, scientists proved it's also a wave that magnets can bend, just as lenses deflect light. Those discoveries birthed the electron microscope and fuzzy pictures, or micrographs, of the virosphere.

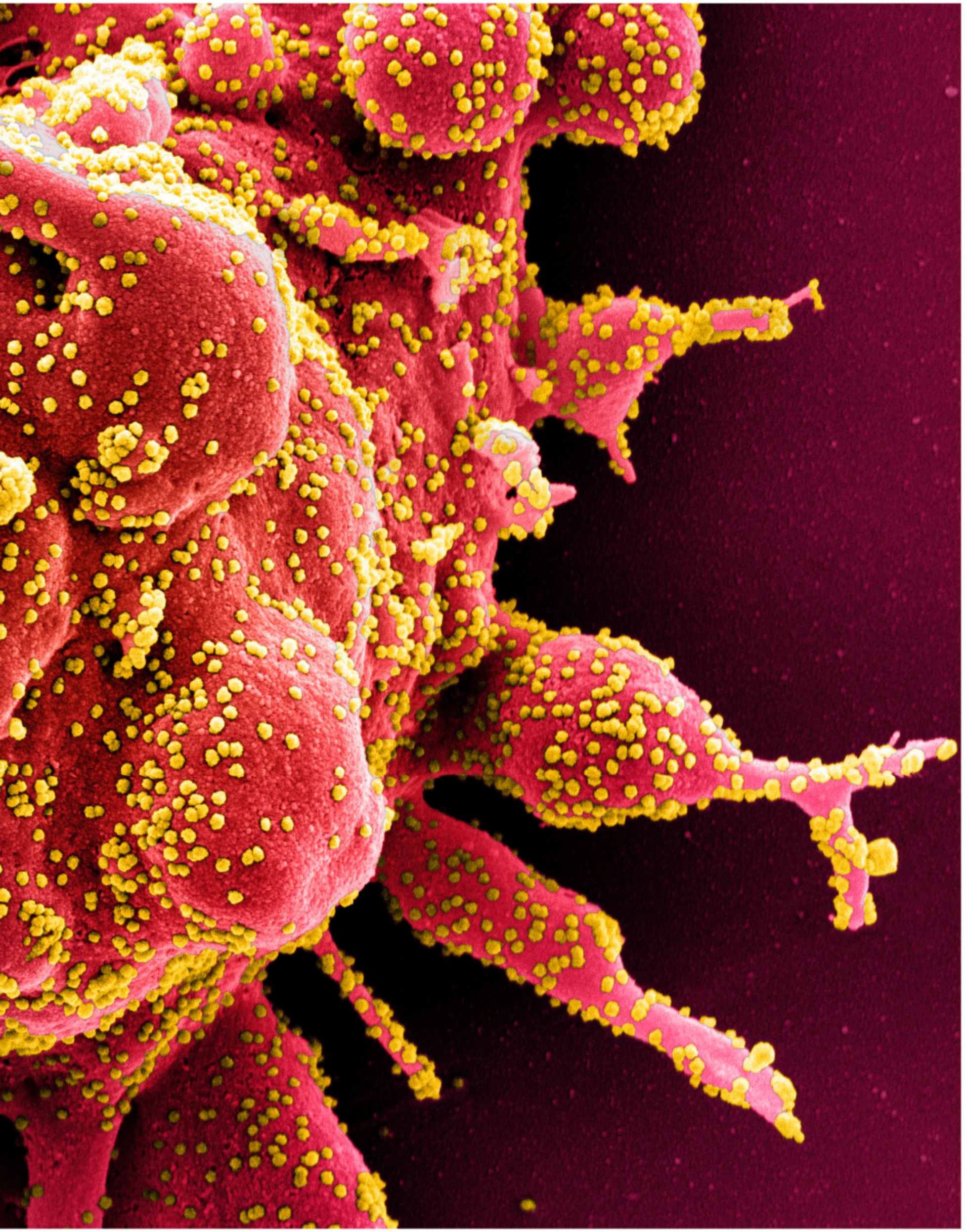
Today virologists can watch pathogens attack cells. That's what those yellow dots (aka SARS-CoV-2) are doing in this 30,000X magnification of vervet monkey cells. "People think we're trying to make them look scary," says microscopist John Bernbaum, whose team at the National Institute of Allergy and Infectious Diseases captured and colorized this image in March to better understand the virus. "But we just try to come up with pleasing color combinations."

Bernbaum used a scanning electron microscope, known for creating sculptural, 3D views. A field emission gun fires electrons down a vacuum chamber and past electromagnets that focus them into a beam. Some bounce back up into a detector, which lets Bernbaum follow along on his computer screen. He snaps pictures when he sees something important—or just plain wild. "It's like being in a car, just driving and looking at the landscape." The cells in this specimen were mostly flat, so when he noticed them forming blobby outgrowths called blebs, he perked up. Blebs signal cell suicide; when stressed cells start chopping up their own proteins, their membranes distend. "You start having these projections coming off the main body, with viruses heavily attached." That, he says, suggests the viruses were trying to reach other cells.

In February, a team at the University of Texas at Austin used a fancier electron microscopy technique, freezing specimens at temperatures colder than Pluto to create a 3D model of the spike protein that SARS-CoV-2 employs to latch onto cells. It was used to design a vaccine now in trials (page 58), says lab director Jason McLellan. "Knowing what the enemy looks like helps us fight it."

LAURA MALLONEE *(@LauraMallonee) writes about photography for* WIRED.





PHOTOGRAPH / NIAID

# THE FUTURE OF HEALTH **TODAY**

At Abbott, we're creating a future of better health and better opportunity. It's a future of stronger bodies through science-based nutrition, deeper insights through advanced diagnostics, new technologies that master diabetes, and cardiovascular breakthroughs that give life more heart.

For over 130 years Abbott has developed life-changing technologies that tackle tomorrow's greatest health challenges today — building a fuller and healthier future for us all.

**DIAGNOSTICS | MEDICAL DEVICES | NUTRITION**

*life. to the fullest.®*

**Abbott**

# Key Change

**To learn to play music while staying socially distanced, just follow the rainbow. —Boone Ashworth**

FETISH

$250

## ROLI LUMI KEYS

When you have no option but to stay inside, it's a great time to take up a hobby that educates *and* entertains. Roli Lumi teaches you the basics of playing piano while brightening the mood with a light show. The keys are 85 percent the size of those on a regular piano, and all 24 of them are illuminated in a rainbow of hues—each note is a different color. Play the pressure-sensitive plastic ivories as they flash to guide you through the lessons in the companion app. A larger device makes it easier to follow notes scrolling down the screen; the app is available for iOS and Android, but it's best on an iPad. The selection is a bit lacking (I can only play that Imagine Dragons tune so many times), but Roli plans to add a steady stream of songs, provided you pay $10 a month for Lumi Premium. Still, basic Lumi has over 200 songs to learn, from "Old MacDonald" to the maximalist cheese of "The Final Countdown." Just wear headphones so your fellow quarantine inmates don't throw your new gadget out the window.

PHOTOGRAPHS / AMANDA RINGSTAD

# Quiet Riot

**Kids' Zoom parties, the roar of delivery trucks, and neighbors yelling to each other across the street are no match for our favorite noise-canceling headphones. —Parker Hall**

LEVEL UP

$229

## ECONOMY

### PANASONIC RP-805N

With stellar sound, these headphones punch well above their modest price tag. Three levels of noise abatement outwit any external audio distraction, and 20 hours of battery life guarantees you a lot of uninterrupted jams. My favorite feature is the sensor on the right earpiece. Cup your hand over your ear to pause your tunes and pipe in sound from the real world—perfect for quick conversations with your family during the work-from-home day or late-night listening sessions.

$595

## FIRST CLASS

### MONTBLANC MB-01

Montblanc might be best known as a premium pen company, but its first noise-canceling headphones are more than a pretty set of over-ears for deal-signing executives. These are the best noise-canceling headphones you can buy—and for almost six Benjamins they ought to be. The leather-swathed aluminum skeleton makes the headphones feel practically weightless, and they're the quietest model I've ever tested. Sound is wide and revealing, with every layer of music in its own place. I also like the giant rubbery play/pause button on the right ear cup; my fingers never have to search for it.

$350

## BUSINESS

### SONY WH-1000XM3

Like the Panasonics, these also have a nifty feature where you can touch the earpiece to hear the outside world, but these headphones add even more impressive noise reduction, better sound quality, and other bells and whistles that make them some of my favorites right now. You'll get a third more battery life—more than 30 hours—and Sony's companion mobile app lets you fine-tune everything that comes out of the speakers. The noise cancellation even adjusts to compensate for the change in air pressure when ascending in an airplane. (You remember flying, right?)



Sunscreeen Reminder Sunscreeen Reminder

# HERE WE GORV!

If you like nature and you like going places, you will most likely like one of these cool fellas. By cool fellas, I mean super nice towables and go-ables that can hold all of your things, blings, and clings. Some of them even have a toilet. Cha-ching!

WE'VE GOT ONE OF THOSE WORLDWIDE WEBSITES! GORVEXCLAMATIONPOINT.COM

SCREEN TIME

# Ready, One Player

**Things get lonely fast under quarantine. Here's a selection of videogames that will keep you feeling social. —Cecilia D'Anastasio**

## FINAL FANTASY XIV

*Windows, Mac, PS4*
Massive multiplayer games aren't as intimidating as they look, and *FFXIV*'s community can't wait to prove it. Design a character using the game's super-detailed character generator, engage in quests, go bop some slimes on the head, and make a couple of friends in the big city. Soon you'll be traversing psychedelic worlds and fighting fantastical beasts alongside friendly strangers (or actual friends).

## DON'T STARVE TOGETHER

*Windows, Mac, PS4, Xbox One*
In this beloved survival game, players chop down trees, mine for gold, cook campfire dinners, make tools, and build structures—all in an effort to not die. Wander the gloomy yet cartoony world with up to five other players, exploring the natural realm and pooling resources until you eventually earn protective clothing and magic spells. The game is equal parts relaxing and punishing, offering plenty of time to chat between gathering sticks and fleeing the ghosts of players who've croaked.

## JACKBOX

*Windows, Mac, PS4, Xbox One, Nintendo Switch, and many more*
*Jackbox*'s ultimate group game offers six "party packs," each featuring hilarious and endlessly replayable microgames. Favorites include *Tee K.O.*, in which you and your friends take turns designing horrible T-shirts, and *Fibbage*, a trivia game that you win by writing the most convincing lie masquerading as an answer. *Jackbox* is playable on basically every device, and although it's built for local play, you can easily set up a remote session with friends and family.

## OVERWATCH

*Windows, PS4, Xbox One, Nintendo Switch*
This rabidly competitive game bends the rules of first-person shooters by including several character classes, like healers and tanks, with avatars that might not even use guns. Some "heroes" rely on deft reflexes and precise aim, while others wrangle the health, shielding, and power-ups their teammates need to survive. *Overwatch*'s diverse roster of heroes offers a play style for everyone—even casual gamers.

## ANIMAL CROSSING: NEW HORIZONS

*Nintendo Switch*
When the game begins, you have just purchased a getaway package to an uninhabited island. There, among fruit trees and native fauna, you make a life for yourself: mining materials, crafting tools, catching fish, building a house. It's not all about escapism, though. Players find immense joy in expressing themselves through creative outfits, home decor, and gardening, and friends can visit each other's islands. Alone, it's an entrancing life-sim that takes your mind off things; together, it's a great way to stay in touch.

## DIVINITY: ORIGINAL SIN 2

*Windows, PS4, Xbox One, Nintendo Switch*
Excellent writing and acting make *Divinity: Original Sin 2* so much more than a superior tactics game. Although it's most popular as a single-player endeavor, its multilevel plot and environments accommodate parties of up to three. Think of it as a high-brow RPG with a no-holds-barred ethos. Players can use nearby objects to their advantage when combating foes—say, by creating an electric force field to flummox the enemy or lighting a vat of oil on fire to set a trap.

## STARDEW VALLEY

*Windows, Mac, PS4, Xbox One, Nintendo Switch*
As anxious tweets and Facebook posts fill your feeds, *Stardew Valley* is the bucolic fantasy you need now. You play as a city person who moves to the valley to farm Grandpa's plot of land. The goal: Make the farm as beautiful and productive as possible. You can go on forever earning money and buying new tools, as long as your character doesn't get overly exhausted from all the work. It's methodical and relaxing, and there's a cooperative multiplayer mode where you and up to three friends can build your farms alongside one another.

## WORLD OF WARCRAFT CLASSIC

*Windows*
If you've always been curious about the cultural phenomenon that is *World of Warcraft* but were intimidated by the heap of content that's been piling up since 2004, try *World of Warcraft Classic*. It's the game as it was before the first expansion: hardcore fantasy with sword-and-sorcery combat. Organize a band of hooligans and share experience points, weapons, and crafts. It's a hoot with friends; plus, with a party, you'll level up faster to reach the more intense raid content.

Product images courtesy of Roli, Panasonic, Sony, Montblanc, Pyle USA, Ultimate Ears, Apple, Epson, Nintendo, Play Neat Games, and Tubi; Getty Images (Dinosaur)

XPS

# EVERY LITTLE THING IS EVERYTHING.

10th Gen Intel®
Core™ i7 processor

**The new XPS 13.**
To learn more, call a Dell Technologies Advisor at 855-341-5261
Dell.com/SB/XPS


# Break Free

**You may not have heard of these no-cost streaming services, but they're the perfect cure for subscription fatigue. —Brian Barrett**

## PLEX

Plex is widely recognized for its excellent media-server software. But the company has also partnered with big-name studios like MGM, Lionsgate, and Warner Bros. to build a decently stocked streaming larder focused on classics. For starters: *The Right Stuff*, *Raging Bull*, and *Apocalypse Now*. It also carved out international licensing deals that allow content to be streamed in multiple countries; unlike many services, the Plex library should remain accessible when you get to travel again.

## IMDB TV

To access IMDb's streaming library, you'll need to create an account or use your Amazon credentials. Current options are decent but not great; the most popular movie appears to be *Fury*, although bonus points for carrying *Sing Street*. Your best binge bet is probably the sci-fi series *Fringe*, and not just because it rhymes. Even though it's getting a deluge of new content, IMDb TV will likely never catch up to its Prime Video sibling, so manage those expectations accordingly.

## THE ROKU CHANNEL

Yes, we agree, this seems confusing, since Roku's hardware streams thousands of "channels," including majors like Hulu and HBO Now. But the same company operates the Roku Channel, which offers a smorgasbord of classics like *Groundhog Day* and *Tombstone*, along with slightly newer fare like *Spotlight*. But the more interesting reason to take a look is that the Roku Channel offers free live-streams, including news reports from ABC and indie movies and classic TV from Filmrise.

## KANOPY

Do you have a library card? Then you have Kanopy! Well, sort of. You still have to sign up for a Kanopy account and connect it to your local public branch. Individual libraries set their own limits; mine allows for 10 movies a month, with three days to watch from the time you press Play. Your credits refresh on the first of each month, and there are apps available for Android, iOS, Apple TV, Fire TV, and Roku. The selection leans toward indies, but it includes lots of Criterion Collection flicks like *The 400 Blows* and *Rashomon*, making it a cinephile's dream. Also? No ads. Libraries!

## TUBI

Tubi lacks the name recognition of some of its peers, but its library outpaces most, with thousands of ad-supported TV and movie titles. You don't even need an account to watch. It also arranges its haul into helpful categories—including a Not on Netflix collection to help you better appreciate what you're not paying for. There's a lot of junk to sift through, but it doesn't take long to turn up rewatchable classics like *Ronin*, art-house hits like *Nebraska*, and underappreciated gems like *The Host*.

## PLUTO TV

Most of the streaming services on this list specialize in on-demand content. Not so the Viacom-owned Pluto TV, which replicates a traditional cable viewing menu, but with specialized channels serving up nonstop *Doctor Who*, *Antiques Roadshow*, and even *The Hills.* It also has traditional networks, like CNN and Fox Sports. Surf hundreds of channels in all, in addition to a slightly anemic on-demand selection of movies and TV shows. If you've already wasted an hour riding the Netflix carousel, unable to decide what to watch, Pluto might be the elixir you're looking for.

## CRACKLE

Sony's Crackle has been around in one form or another since 2004. That's three years before Netflix started streaming. The head start may not have won it a massive following, but Crackle does feature some gems, particularly in the realm of cult and classic TV. Binge the entirety of *News Radio* and *Parker Lewis Can't Lose*, plus early seasons of *All in the Family* and *Bewitched*. Rare for a free streaming service, Crackle also has original shows like *Rob Riggle's Ski Master Academy* and the much less ridiculous *The Oath*. There are plenty of movies too, spanning decades but with a heavy focus on '90s classics.

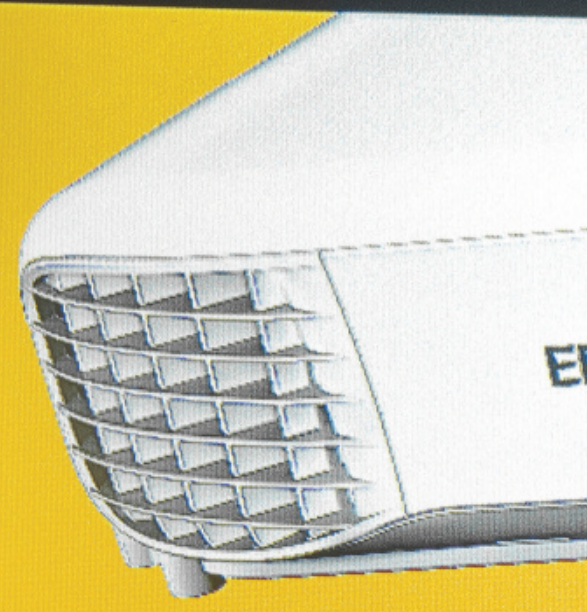
## VUDU

In April, Walmart sold its Vudu streaming service to ticketing company Fandango, but the free movies and TV shows will continue to flow uninterrupted. The selection isn't appreciably better than the other options here. But keep an eye on Vudu; it's investing in original programming, which includes a sci-fi drama called *Albedo* starring Evangeline Lilly and directed by Brad Peyton, who has directed the actor known as the Rock in three feature films. Impossible to say if it'll be any good. But at least it'll be free.

# Auto Tune

**Throw a house karaoke party—or just practice solo—using gear you already have or can pick up at a big-box store. —Michael Calore**

SING ALONG



### SPEAKER UP

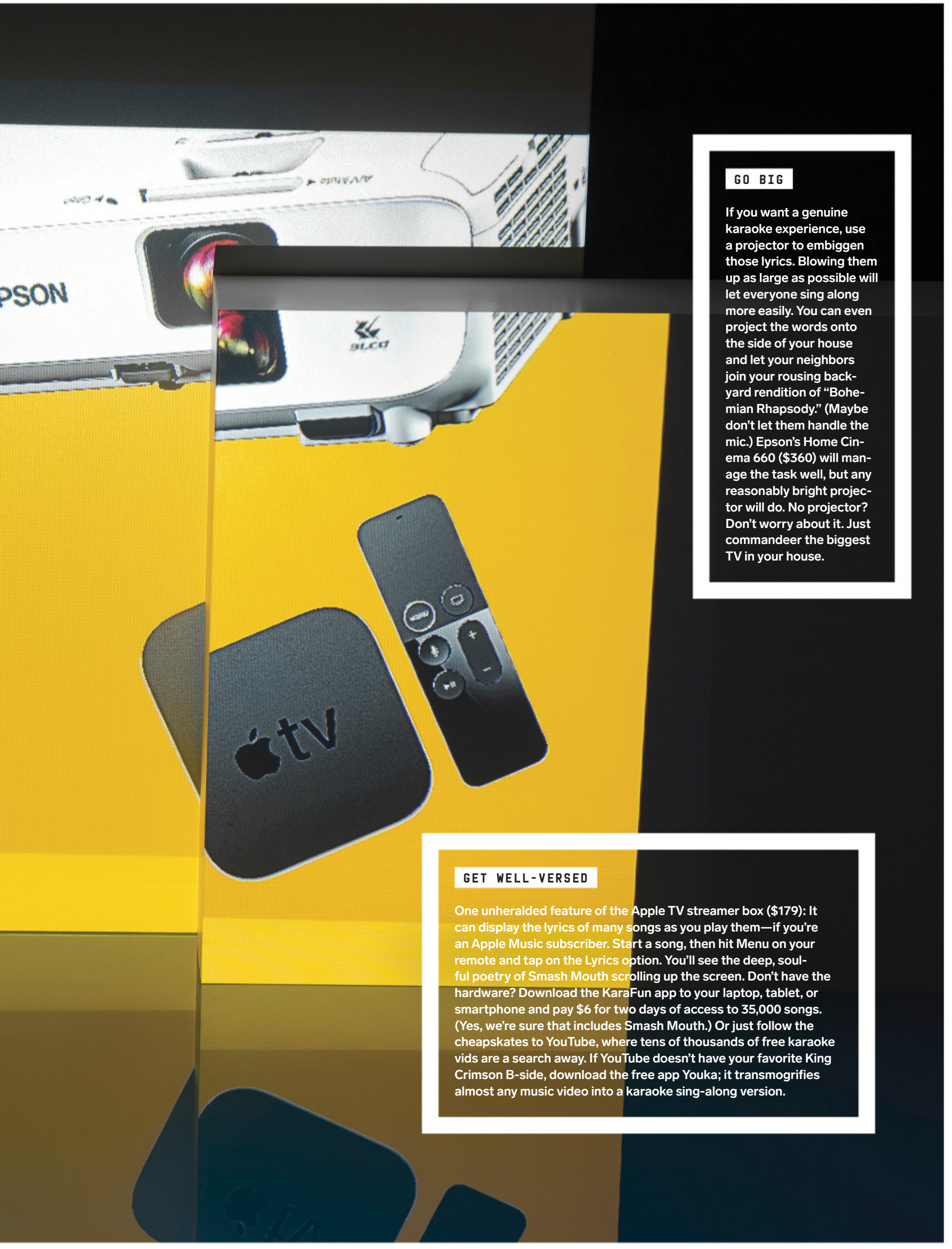
Choose a speaker that can make your voice as loud as the tune you're singing along to. A powerful Bluetooth model like the $399 UE Hyperboom would work perfectly. You'll likely need an adapter to plug in your microphone, so check the speaker's available inputs. (The Hyperboom has a 3.5-mm auxiliary jack.) Don't want to buy a speaker right now? Plugging into a guitar amp is the best solution, but the RCA inputs on a home stereo system will work in a pinch too.

### CHECK THE MIC

Karaoke just isn't karaoke without a microphone. But you're not Rosalía, and your living room isn't a recording studio—all you need is something simple. There are dozens of inexpensive options; just be sure it's a "high-output" microphone that can plug directly into a speaker without any additional (expensive) harware. Try the $23 Pyle PDMIC59, which comes with a cable.

## WE ARE PROJECTING

Given shelter-in-place orders, we had to find an alternative to shooting these gadgets in our San Francisco offices. Director of photography Anna Alexander came up with the idea of projecting images of the products onto colorful sets. Photo editor Lauren Joseph got images from the companies and found the perfect photographer: Amanda Ringstad. Ringstad has a studio in her home *and* a kick-ass projector. She was able to do the shoot all by herself—no health risks required.




### GO BIG

If you want a genuine karaoke experience, use a projector to embiggen those lyrics. Blowing them up as large as possible will let everyone sing along more easily. You can even project the words onto the side of your house and let your neighbors join your rousing backyard rendition of "Bohemian Rhapsody." (Maybe don't let them handle the mic.) Epson's Home Cinema 660 ($360) will manage the task well, but any reasonably bright projector will do. No projector? Don't worry about it. Just commandeer the biggest TV in your house.

### GET WELL-VERSED

One unheralded feature of the Apple TV streamer box ($179): It can display the lyrics of many songs as you play them—if you're an Apple Music subscriber. Start a song, then hit Menu on your remote and tap on the Lyrics option. You'll see the deep, soulful poetry of Smash Mouth scrolling up the screen. Don't have the hardware? Download the KaraFun app to your laptop, tablet, or smartphone and pay $6 for two days of access to 35,000 songs. (Yes, we're sure that includes Smash Mouth.) Or just follow the cheapskates to YouTube, where tens of thousands of free karaoke vids are a search away. If YouTube doesn't have your favorite King Crimson B-side, download the free app Youka; it transmogrifies almost any music video into a karaoke sing-along version.

# Beyond Monopoly

GAME NIGHT

**Those old board games were fun for the first two months. Here are four fresh options to enjoy while you wait for the world to reopen. —Jess Grey and Louryn Strampe**


## TOO MANY POOPS

Easy to learn and tough to master, this card game (shown above) encourages you to collect adorable cats, which deposit tiny plastic "pooples" into their owner's litter box every round. To win, you need to hoard felines, but not too many—just like in real life, having more than 10 poops in the litter box means you lose. With each turn, you can acquire more cats or offload your pooples into someone else's litter box for some truly catty backstabbing.
(2 to 6 players, ages 7+) $20

## PANDEMIC LEGACY: SEASON 1

The classic 2008 board game Pandemic used whole-world, Risk-like mechanics. This sequel offers a twist that puts players closer to the action. It's structured like a TV series, starring tireless health care workers trying to quell a deadly global pandemic. (Too soon?) Each round of play follows an episode that's part of a larger "season." Changes to your characters' mental states and the disease's behavior help shape subsequent episodes. Pandemic Legacy is entertainment you can consume in segments or binge in a day-long marathon—just like your favorite Netflix drama.
(2 to 4 players, ages 13+) $70

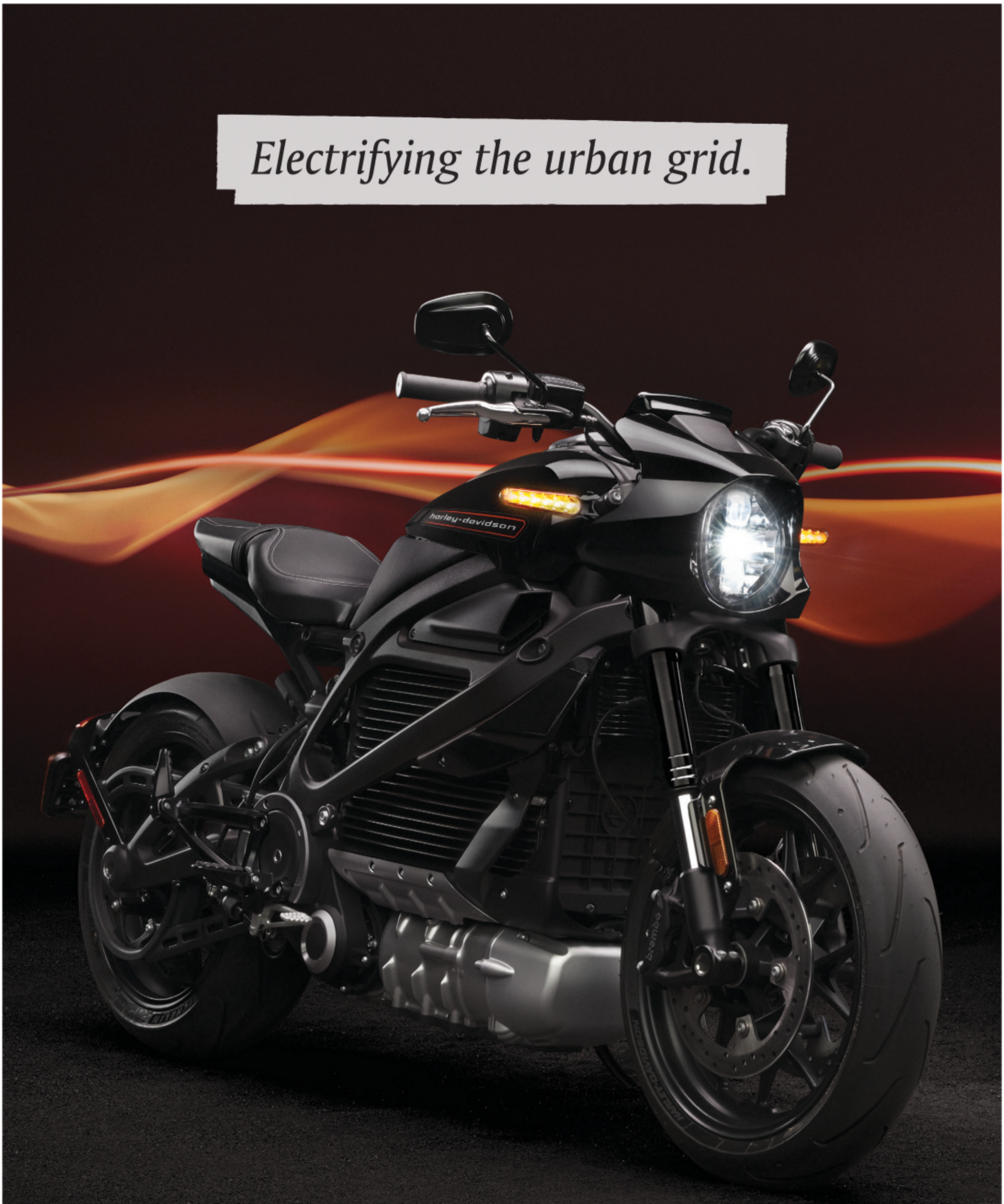
## BLUEBEARD'S BRIDE

This role-playing game goes well beyond the typical dungeon delving. Bluebeard's Bride explores sex, trauma, murder, and mystery from the perspective of the just-married wife of the monstrous Grimm's fairy tale character. Each player inhabits a different aspect of her psyche—Animus, Fatale, Mother, Virgin, and Witch. Together, the team works to keep the Bride alive (and sane) as it wanders room to room in her murderous new husband's mansion. Surprises and horrors lurk behind every door.
(3 to 5 players, ages 18+) $50

## THORNWATCH

Welcome to the endless deep of the haunted forest Eyrewood. Together players explore its murky vales as the party is beset by ancient evils, forbidden magic, and giant crows. Thornwatch is a rich and sprawling experience with role-playing elements like characters that level up and collect inventory items. Each session is its own quest that's part of a longer story arc. The board isn't just a board; you lay it out differently for each quest, using tiles illustrated like panels in a graphic novel. They're beautifully drawn but take up quite a bit of space as you get further into the campaign. An average Thornwatch session can fill up one to three quarantine hours.
(3 to 6 players, ages 14+) $75

*Electrifying the urban grid.*




Experience the LIVEWIRE® and bolt into the electric future—a future that goes 0 to 60 in 3 seconds with a twist of the throttle. No clutch, no shifting, just pure exhilaration. Learn more at H-D.com.

MOTOR HARLEY-DAVIDSON CYCLES®

# Why STEAM Learning in Middle School is So Critical

**A LESSON FROM AN EDUCATOR ON HOW LEGO® EDUCATION SPIKE™ PRIME HELPS MIDDLE SCHOOLERS**

**THIS IS AN UNPRECEDENTED TIME**, one that we are all learning to navigate together. With the disruptions, along with the uncertainties in the academic year ahead, teachers and parents are continuing to innovate to keep children engaged and learning. It's hard to find an educator who doesn't agree that STEAM (Science, Technology, Engineering, Arts, and Math) is a vital part of their education—in and out of school—that can help set them up for success in the future. It is particularly important for middle-school aged children, who are going through a transitional time as they evolve from concrete to abstract thinking processes. This means that in addition to discussion-based learning, lessons for middle schoolers should include hands-on learning activities.

Joey Tanaka is the EdTech and Robotics Specialist for Bertschi School in Seattle and a LEGO® Education Master Educator. He understands that STEAM-led education is essential for today's students in order for them to compete on the world stage in the future. So for his school, he works to combine the very best technology with innovative learning techniques that excite and spark curiosity in his students. In particular, he focuses on exploring the rapidly developing areas of research in robotics, bringing back his findings and integrating them into his curriculum.

Last summer, he was invited to go to MIT's Media Lab to meet with—and hear from—the best and brightest in the robotics field. "I spent the week at the game lab and really what I wanted to do in terms of an integration approach was something maker-esque for kids to iterate a solution because if you look at the world right now, there are these big questions/problems that we don't have answers to," says Tanaka. "I was looking for a platform for kids to build a solution and test it out and see if it works. And along came LEGO® [Education] SPIKE™ Prime—it is perfect; it was what I was looking for."

SPIKE™ Prime is a new STEAM solution from LEGO® Education that is designed specifically with middle schoolers in mind. Combining colorful LEGO building elements, easy-to-use hardware, and an intuitive drag-and-drop coding language, the solution engages students through playful learning activities—encouraging them to think critically and solve complex problems. One lesson, *Automate It!*, challenges students to build a model (without building instructions!) using LEGO bricks, motors, and sensors. This model serves as an "automated helper" that can identify and ship the correct package based on color. In another lesson, *Rain or Shine?*, students build and code a model that displays real-time weather forecasts for different cities, based on qualitative cloud data.

For educators, one of the most appealing parts of SPIKE™ Prime is that it provides a very easy getting-started experience, but also offers a high ceiling when it comes to building complex creations and exploring more advanced coding. "The coding initially is approachable," says Tanaka. "For most of my students, it's something they are familiar with, but as you jump in, especially for older kids, you begin to realize that there is a lot more complexity to it." Tanaka notes that he has used a lot of what he calls "pre-packaged" robots that you can assemble and re-assemble into different shapes and configurations but at the end of the day, they are still limiting. "Kids tend to have their own ideas and ways to solve things," says Tanaka.

**"It's important to elevate student creativity and expression through all kinds of digital platforms."**

Like all LEGO solutions, SPIKE™ Prime fosters hands-on learning both inside and outside of the classroom. This approachability factor that Tanaka talks about is also very beneficial for parents who may be new to coding, but looking for ways to facilitate hands-on, STEAM learning at home with their kids. "It's important to elevate student creativity and expression through all kinds of digital platforms," says Tanaka. SPIKE™ Prime taps into students' passion, creating an open environment for them to let their imagination run free and their problem-solving capabilities excel.

**To learn more, visit LEGOeducation.com**

LEGO education™

# Build. Code. Experiment. Repeat.

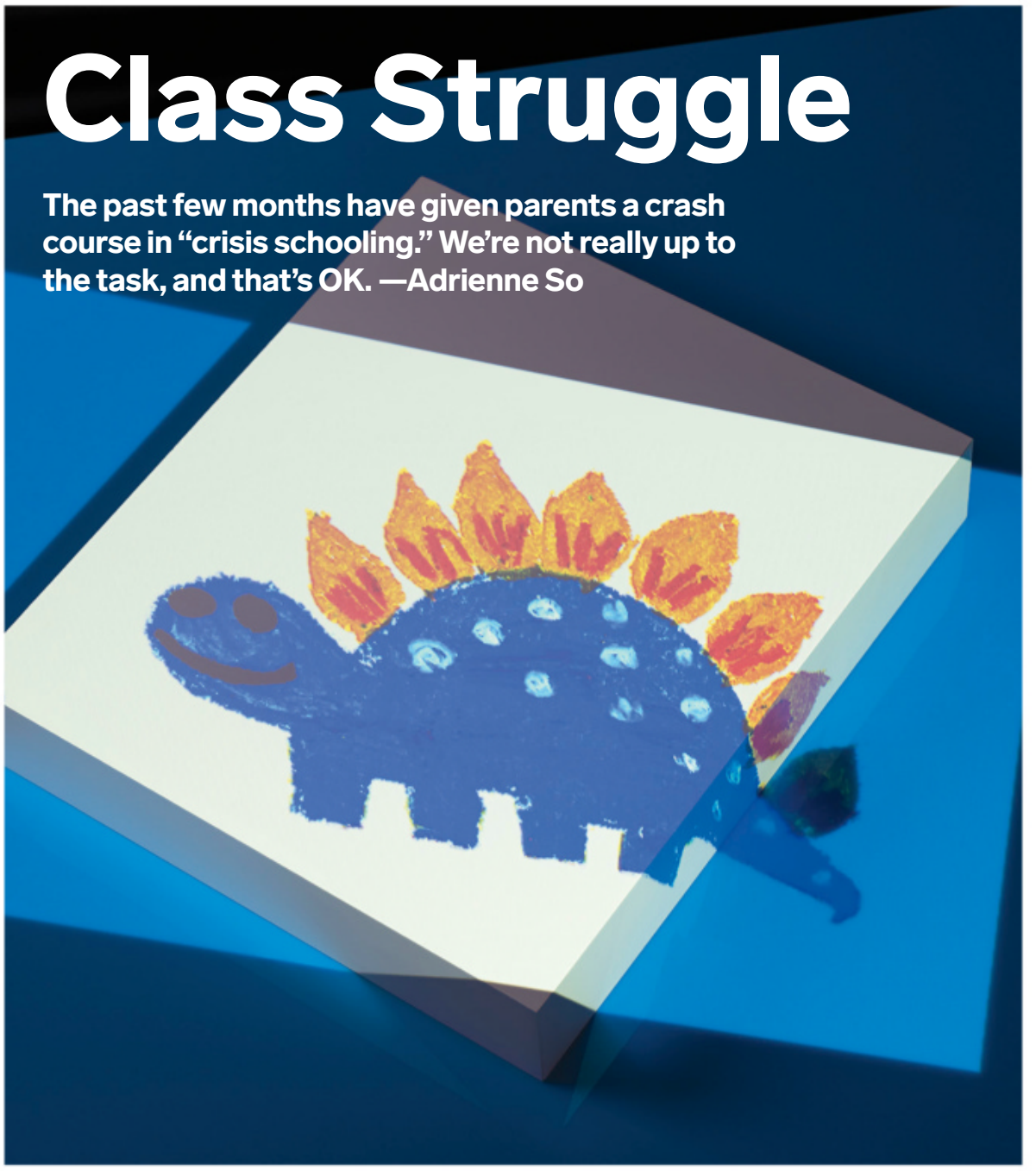
LEGO® Education SPIKE™ Prime is the go-to STEAM learning tool for middle schoolers, whether at school or at home. Help your students develop critical thinking skills, expand their creativity and build confidence in STEAM learning through playful, hands-on activities.

**LEGOeducation.com/MeetSPIKEprime**

#LEGOeduSPIKEprime

# Class Struggle

**The past few months have given parents a crash course in "crisis schooling." We're not really up to the task, and that's OK. —Adrienne So**



**"Mom, can you** fill up my water-keeper?" I looked down from making meatballs. My 5-year-old was holding a contraption that appeared to consist of several crayon drawings inside a large Ziploc that was suspended—via various forks and drinking straws—in a mixing bowl. "Sure," I said. I washed my hands and poured water in the bowl. She nodded and walked away.

Like many working parents, I never anticipated having to keep my kids home for months. Though my husband and I already work from our home and are both lucky enough to stay employed, the orders to shelter in place filled us with dread. Neither of us are teachers. The other adult commitments we have—earning an income, doing the laundry—don't disappear just because we're all now trapped inside, hiding from microbes.

At first, I started panic-hopping into every online homeschooling forum. A couple of days in, I ruefully acknowledged that becoming a teacher overnight was a lost cause. I can't run into an ER and defibrillate a patient just because I saw someone do it on *House, MD*. Likewise, downloading Starfall's reading app does not turn me into an experienced educator. Nevertheless, I tried to keep the kids up to speed with lessons and activities. In those first few weeks, the hours passed in dribs and drabs, and I was counting down the minutes until I handed the kids to my husband so I could turn my attention to my work.

Along the way, though, we realized that homeschooling is a misnomer in these circumstances. Homeschoolers don't stay home *all the time*. Those kids take field trips, have meetups, and do co-op classes. Isolation is an adjustment for them too.

"This is not homeschooling, this is crisis schooling," says Jamie Heston, a board member of the Homeschool Association of California. "It's very different. That parents make sure their families are taken care of, that everyone's mental and physical health is taken care of, and that everyone comes through this alive—literally—takes precedence over academics."

That helped us realize that learning doesn't have to look the way we think it should—how it looked at my kid's preschool. We don't have color-coded schedules, photocopied worksheets, or educational (or even organized) toys. And that is OK. Now, used to life without pickups, drop-offs, play dates, or lessons, my family seems to have found its rhythm.

Because of my job, I spend a lot of time staring at a screen, and so my kids do too. I'm fine with that. "Now is not the time to worry about screen time," Heston says. Whether my kids' screens are filled with online drawing classes with children's book artist Mo Willems, video chatting with their friends on Facebook's Messenger Kids, or taking a group yoga class through Zoom, this is how they keep in touch with one another and the world.

Since we're spending most of every day at home, learning can also take place anytime. My kids don't have to be at their "school" desks from 9 am to 2 pm. If the one success we have on a particular morning is we all got out the door for a 20-minute walk, that's pretty good. We can make banana bread later, or build a water-keeper (whatever it is), or write notes to the grandparents. The other afternoon I taught the 5-year-old how to wash windows. Our windows are now clean, and like the Karate Kid, she got a good arm workout.

Last week I turned on an hour-long episode of *Walking With Dinosaurs*, because I couldn't summon the energy for anything else. If you'd told me that my 3-year-old would be able to pronounce "quetzalcoatlus" flawlessly a day later, I wouldn't have believed you. But now we argue about—and research—whether "swimmy-saurs" are real dinosaurs or just marine reptiles, and how fast different dinos could run. We also now have a hand-drawn, hand-colored dinosaur garden in our hallway.

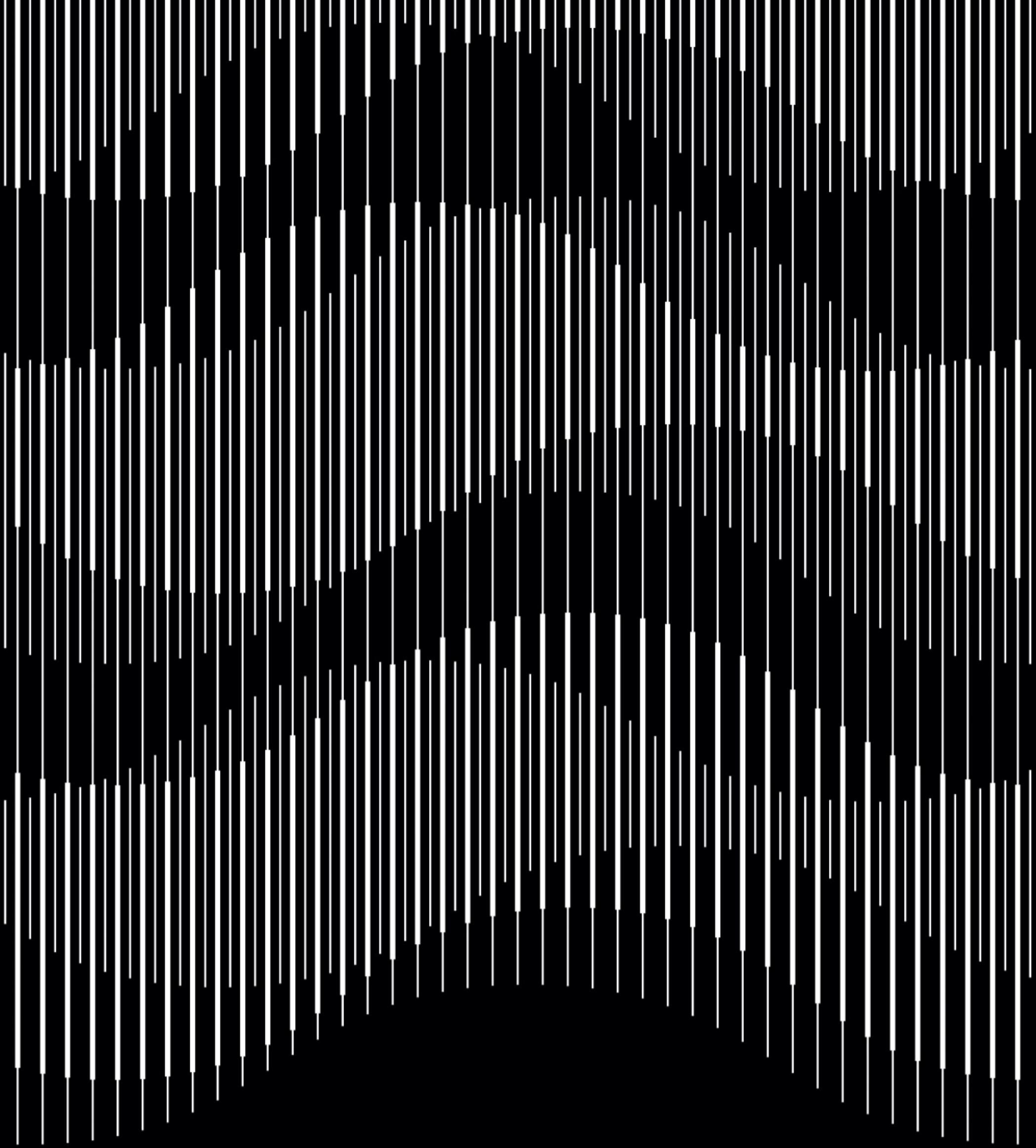
When my oldest daughter was an infant, when we had no reference points for this parenting thing, days became nights, nights became days. A 5-minute crying spell felt like 15 years. Back then, I spent hours texting friends or searching Google for advice, anything to help us calm her down and get some sleep. Then one day I looked up, and my kid was smiling.

Someday this will all be over. In the course of a lifetime, a few months is a blip. My kids don't have to learn their multiplication tables or how a jet engine works. If all they take away from this time is that we were safe and together, that's going to be enough.

---

*Senior writer* ADRIENNE SO *(@adriennemso) covers consumer tech.*

PHOTO-ILLUSTRATION / SEAN FREEMAN & EVE STEBEN, THERE IS STUDIO



# FLYING FISH IS LISTENING

BY MARA HVISTENDAHL

Alexa can tell you the weather.
Siri knows a few jokes.

China’s voice-computing giant iFlytek built similar chatty assistants beloved by users. But its technology is also enabling the surveillance state to identify citizens by the sound of their voice.

**In 1937,** the year that George Orwell was shot in the neck while fighting fascists in Spain, Julian Chen was born in Shanghai. His parents, a music teacher and a chemist, enrolled him in a school run by Christian missionaries, and like Orwell he became fascinated by language. He studied English, Russian, and Mandarin while speaking Shanghainese at home. Later he took on French, German, and Japanese. **In 1949,** the year Mao Zedong came to power and Orwell published *1984*, learning languages became dangerous in China. In the purges of the late 1950s, intellectuals were denounced, sent to labor camps, and even executed. Chen, who by then was a student at prestigious Peking University, was banished to a Beijing glass factory.

ART BY JOHN BURGESS

Chen's job was to cart wagons full of coal and ash to and from the factory's furnace. He kept his mind nimble by listening to his coworkers speak. At night, in the workers' dormitory, he compiled a sort of linguistic ethnography for the Beijing dialect. He finished the book around 1960. Soon after, Communist Party apparatchiks confiscated it.

His fortunes improved after Mao's death, when party leaders realized that China's economy needed intellectuals in order to develop. Chen went back to school, and in 1979, at the age of 42, his test scores earned him a spot in the first group of graduate students to go abroad in decades. He moved to the US and earned a PhD in physics at Columbia University. At the time, America offered more opportunity than China, and like many of his peers, Chen stayed after graduation, getting a job with IBM working on physical science research. IBM had developed some of the world's first speech recognition software, which allowed professionals to haltingly dictate messages without touching a keyboard, and in 1994 the company started looking for someone to adapt it to Mandarin. It wasn't Chen's area, but he eagerly volunteered.

Right away, Chen realized that in China speech recognition software could offer far more than a dictation tool for office workers; he believed it stood to completely transform communication in his native tongue. As a written language in the computer age, Chinese had long posed a unique challenge: There was no obvious way to input its 50,000-plus characters on a QWERTY keyboard. By the 1980s, as the first personal computers arrived in China, programmers had come up with several workarounds. The most common method used pinyin, the system of romanized spelling for Mandarin that Chinese students learn in school. Using this approach, to write *cat* you would type "m-a-o," then choose 猫 from a drop-down menu that also included characters meaning "trade" and "hat," and the surname of Mao Zedong. Because Mandarin has so many homophones, typing became an inefficient exercise in word selection.

To build his dictation engine, Chen broke Mandarin down into its smallest elements, called phonemes. Then he recruited 54 Chinese speakers living in New York and recorded them reading articles from *People's Daily*. IBM's research lab in Beijing added samples from an additional 300 speakers. In October 1996, after he had tested the system, Chen flew to China to display the resulting software, called ViaVoice, at a speech technology conference.

In a packed room festooned with gaudy wallpaper, Chen read aloud from that day's newspaper. In front of him, with a brief delay, his words appeared on a large screen. After he finished, he looked around to see people staring at him, mouths agape. A researcher raised her hand and said she wanted to give it go. He handed over the microphone, and a murmur ran through the crowd. ViaVoice understood her too.

ViaVoice debuted in China in 1997 with a box that read, "The computer understands Mandarin! With your hands free, your thoughts will come alive." That same year, President Jiang Zemin sat for a demonstration. Soon PC makers across China—including IBM's rivals—were preinstalling the software on their devices. The era of freely conversing with a computer was still a long way off, and ViaVoice had its limitations, but the software eased the headache of text entry in Chinese, and it caught on among China's professional class. "It was the only game in town," Chen recalls.

But for some scholars who had stayed in China, it stung that a researcher working for an American company had been the one to make a first step toward conquering the Chinese language. China, they felt, needed to match what Chen had done.

Among those motivated by IBM's triumph was Liu Qingfeng, a 26-year-old PhD student in a speech recognition lab at the prestigious University of Science and Technology of China, in Hefei. In 1999, while still at USTC, Liu started a voice computing company called iFlytek. The goal, it seemed, was not just to compete with IBM and other foreign firms but to create products that would recoup Chinese pride. Early on, Liu and his colleagues worked out of the USTC campus. Later they moved elsewhere in Hefei. It was a second-tier city—USTC had been relocated there during the Cultural Revolution—but staying in Hefei meant iFlytek was close to the university's intellectual talent.

When Liu explained his business concept to Kai-Fu Lee, then the head of Microsoft Research Asia, Lee warned that it would be impossible to catch up with American speech recognition giants. In the US, the industry was led by several formidable companies in addition to IBM and Microsoft, including BellSouth, Dragon, and Nuance Communications, which had recently spun off from the nonprofit research lab SRI International. These companies were locked in a slog to overcome the limitations of early-2000s computing and build a voice-computer interface that didn't exasperate users, but they were far ahead of Chinese competitors.

Liu didn't listen to Lee's warnings. Even if voice-interface technology was a crowded, unglamorous niche, Liu's ambition gave it a towering moral urgency. "Voice is the foundation of culture and the symbol of a nation," he later said, recounting iFlytek's origin story. "Many people thought that they"—meaning foreign companies—"had

MARA HVISTENDAHL *(@marahvistendahl) is the author of* The Scientist and the Spy. *She last wrote about a murder-for-hire website in issue 27.05.*

us by the throat." When some members of his team suggested that the company diversify by getting into real estate, Liu was resolute: Anyone who didn't believe in voice computing could leave. Nuance was building a healthy business helping corporate clients begin to automate their call centers, replacing human switchboard operators with voice-activated phone menus ("To make a payment, say 'payment' "). iFlytek got off the ground by doing the same sort of work for the telecommunications company Huawei.

iFlytek went public in 2008 and launched a major consumer product, the app iFlytek Input, in 2010. That same year, Apple's iPhone began to carry Siri, which had been developed by SRI International and acquired by Apple. But while Siri was a "personal assistant"—a talking digital concierge that could answer questions—iFlytek Input was far more focused. It allowed people to dictate text anywhere on their phones: in an email, in a web search, or on WeChat, the super app that dominates both work and play in China.

Like any technology trained on interactions with human speech, Input was imprecise in the beginning. "With the first version of that product, the user experience was not that good," said Jun Du, a scientist at USTC who oversaw technical development of the app. But as data from actual users' interactions with the app began to pour in, Input's accuracy at speech-to-text transcription improved dramatically.

As it happened, Siri and Input were relatively early arrivals in a coming onslaught of mature voice-interface technologies. First came Microsoft's Cortana, then Amazon's Alexa, and then Google Assistant. But while iFlytek launched its first generation of virtual assistant, Yudian, in 2012, the company was soon training much of its AI firepower on a different challenge: providing real-time translation to help users understand speakers of other dialects and languages. Later versions of Input allowed people to translate their face-to-face conversations and get closed captioning of phone calls in 23 Chinese dialects and four foreign languages. When combined with China's large population, the emphasis on translation has allowed the company to collect massive amounts of data.

Americans might tap Alexa or Google Assistant for specific requests, but in China people often use Input to navigate entire conversations. iFlytek Input's data privacy agreement allows it to collect and use personal information for "national security and national defense security," without users' consent. "In the West, there are user privacy problems," Du says. "But in China, we sign some contract with the users, and we can use their data." Voice data can be leaky in China. The broker Data Tang, for example, describes specific data sets on its website, including one that includes nearly 100,000 speech samples from 3- to 5-year-old children.

In 2017, *MIT Technology Review* named iFlytek to its list of the world's 50 smartest companies, and the Chinese government gave it a coveted spot on its hand-picked national "AI team." The other companies selected that year were platform giants Baidu, Alibaba, and Tencent. Soon after, iFlytek signed a five-year cooperation agreement with MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a leading AI lab. The company's translation technology is used by the Spanish football club RCD Espanyol, and it signed an exclusive deal to provide automated translation for the 2022 Beijing Winter Olympics. As of mid-April, iFlytek was valued on the Shenzhen Stock Exchange at $10.8 billion, and it claims to have 70 percent of the Chinese voice market, with 700 million end users. Nuance was valued at $5.3 billion during the same time. In China, the company's other major competitors in voice computing are mainly platforms like Alibaba and Baidu.

Two decades after Julian Chen intuited that voice computing would revolutionize how people interact with computers in China, its impact there is indeed dramatic. Every day, WeChat users send around 6 billion voice texts, casual spoken messages that are more intimate and immediate than the typical voicemail, according to 2017 figures. Because WeChat caps the messages at one minute, people often dash them off in one long string. iFlytek makes a tablet that automatically transcribes business meetings, a digital recorder that generates instantaneous transcripts, and a voice assistant that is installed in cars across the country.

Consumer products are important to iFlytek, but about 60 percent of its profits come from what is described in the company's 2019 semiannual report as "projects involving government subsidies." These include an "intelligent criminal investigation assistant system," as well as big data support for the Shanghai city government. Such projects bring access to data. "That might be everything that's recorded in a court proceeding, call center data, a bunch of security stuff," says Jeffrey Ding, a scholar at Oxford University's Future of Humanity Institute who studies AI governance in China. Liu, iFlytek's founder and CEO, is a delegate to the National People's Congress, China's rubber-stamp parliament. "He has a very good relationship with the government," Du says.

Liu has a vision that voice computing will someday penetrate every sphere of society. He recently told an interviewer for an online state media video channel: "It will be everywhere, as common as water and electricity." That's a dream that aligns neatly with the Chinese Communist Party's vision for a surveillance state.

One day this past fall, I tested out a recent model of the Translator, an instant translation device made by iFlytek, with a man I'll call Al Cheng. The Translator, a device powered by a Qualcomm Snapdragon chip, works offline for major world languages. Cheng and his wife live in a congested city in southern China, but every other year they travel to the Midwest to visit family. To get exercise, they walk half a mile each morning to the mall. But Cheng, who likes to hold forth on art and culture in Mandarin, Cantonese, and Hakka, does not speak any English. Much of the time while in the US, he is unhappily silent. He is exactly the sort of person who needs a Translator.

I met Cheng one morning in the mall's central atrium, near an antique Chevrolet pickup truck that held hay and flowers. ("Chrysanthemums," Cheng noted, approvingly.) When I told him the price of the Translator (around $400), he was skeptical. "Too expensive," he said, shaking his head. But as we sat down outside Caribou Coffee to play around with it, his skepticism gave way to admiration. We held the device alongside the Baidu Translate app on his phone, taking turns speaking phrases in various languages in an attempt to stump it. In Mandarin, the Translator understood that Cheng's accented "mingnisuda" was Minnesota. It got my name, despite Cheng pronouncing it "Mala." When I spoke English, both translation tools could handle the metaphor "I'm feeling blue," but only the Translator got that "I got up on the wrong side of the bed" was about my mood, not where I placed my feet. The most magical moment came when Cheng recited a couplet from the eighth-century poet Zhang Jiuling. Baidu translated the lines, nonsensically, as "At sea, the moon and the moon are at this time." The Translator offered up an accurate and genuinely poetic translation:

> As the bright moon shines over the sea;
> From far away you share this moment with me.

When Cheng switched to Cantonese, the results were more mixed. (The Translator understood an idiom for the "English language" as "chicken farm.") But the mere fact that the device supported the language impressed him.

iFlytek's translation mission goes far beyond helping travelers, business people, and urban elites. It has developed products for ethnic minorities and people in rural

**When I spoke English, both Baidu Translate and iFlytek's Translator could handle the metaphor "I'm feeling blue," but only the Translator got that "I got up on the wrong side of the bed" was about my mood, not where I placed my feet.**

areas where many people do not speak Mandarin, and it is constantly improving its handling of dialects. In 2017 it launched what it calls the Dialect Protection Plan. When I first came across a news report about it, I laughed out loud at the Orwellian name. The Chinese Communist Party has spent decades attacking language noun by noun, verb by verb—censoring terms it deems dangerous, undermining dialects and minority languages, and bludgeoning Mandarin with ideological drivel. (The Chinese cultural critic Li Tuo dubbed such clunky phrasing Maospeak, in reference to the Newspeak of *1984*.) Tech companies have aided in the assault on language.

An iFlytek spokesperson said in an email that the goal of the company's work on dialects was to "protect our ways of communication." iFlytek has devoted special attention to Uighur and Tibetan, which are spoken by ethnic minorities that have been singled out for persecution by Beijing. *China Daily* reported that in one promotion for the Dialect Protection Plan, executives encouraged users of iFlytek Input to record themselves speaking their native language, in exchange for a chance to win an iPhone.

I

Flytek's campus sits far outside Hefei's city center, on a street lined with drab apartment buildings. Nearly half of the company's 11,000 employees work in a guarded compound spanning 31 acres. The rest are scattered at offices throughout China, with a few in other parts of the world. Like Silicon Valley tech companies, iFlytek buses in staff, provides food and entertainment, and projects a lofty mission. Everywhere on the campus—on walls, merchandise, and the stall doors in the squat toilets—is the slogan "Empower the world with artificial intelligence." When I arrived there last spring, I was greeted by a photograph of Xi Jinping.

A spokesperson led me to a café on the campus for a chat over bubble tea. iFlytek does not list any media contacts on its website, and I had managed to arrange this visit only after spending several hours cold-calling the company's customer service lines. After a few dead ends, an agent took pity and connected me with the spokesperson, who accepted my request to visit. (Another spokesperson later responded to a list of questions sent to Chartwell Strategy Group, a DC-based lobbying firm that iFlytek engaged to manage its communications in the US.)

Surrounded by blond wood, I slurped up tapioca balls as my host explained the company's consumer products. She wore a flouncy shirt with a sewn-on vest, dangly earrings, and platform shoes—an outfit that reflected iFlytek's aesthetic, which is cute, whimsical, and even silly. One version of its child companion robot, the Alpha Egg, has polka dots and little antennae and speaks in a cartoonish alien voice. Its virtual assistant for drivers, Flying Fish, is depicted in ads as a cuddly shark in a scuba mask. The robot it markets to hospitals to assist with patient queries looks like the love child of C-3PO and EVE, the machine in the animated film *WALL-E*. ("Perhaps more than any people in the world," says Chen Xiaoping, the director of USTC's Center for Artificial Intelligence Research, the lab that helped develop the medical assistant, Chinese people "really like robots.") As the spokesperson explained it, iFlytek's products were all in service of convenience and fun.

Fun is also a means of subversion in China, especially when it comes to language. In the early 2000s, as online censors banned certain characters, computer users got around the state by switching to homophones. To mock the notion of a "harmonious society," a Maospeak phrase popularized during Hu Jintao's rule, they joked about crustaceans—*hexie*, river crab, is pronounced similarly to *hexie*, harmony. "Serve the people" became "smog the people." Both contain the sound *wu*. The characters were neighbors in an input drop-down menu.

Alarmed by the proliferation of online sarcasm, the central government went so far as to ban homophones and other wordplay. So dissidents turned to other means of dissemination. "Activists saw new opportunities in video as it became easier and cheaper on cameras and phones to record, view, and also distribute," said Dechen Pemba, a Tibetan human rights activist in London who edits the site High Peaks Pure Earth. But by the late aughts, the Communist Party had embarked on a quest to master speech technologies—one that ran in parallel with iFlytek's growth as a consumer voice company.

In 2009, Meng Jianzhu, the head of China's Ministry of Public Security, traveled to Hefei and visited iFlytek's headquarters. According to a report posted on the central government's website, he spoke there of the need for "public security organs to closely cooperate with technology companies" to create "prevention and control systems." As the CCP has amped up its surveillance capabilities over the past decade, it has installed millions of cameras, introduced electronic ID cards and real-name registration online, and built tech-driven "smart" cities. iFlytek's technology has helped the government to integrate audio signals into this network of digital surveillance, according to Human Rights Watch.

The company is emblematic of a broader Chinese government effort called "military-civil fusion," which aims to harness advances in China's tech sector for military might. "iFlytek is contributing to military-civil fusion quite actively," says Elsa Kania, a fellow at the Center for a New American Security in Washington, DC, who studies artificial intelligence in China. "There are elements of the company that pursue consumer applications, but the public security, policing, and defense-oriented applications appear to be significant as well." The company has promoted its products to the People's Liberation Army, according to testimony that Kania presented to Congress last year. She adds, "It's not clear that there are firewalls or divisions" between consumer and other state-oriented applications. (The spokesperson reached through Chartwell Strategy Group said that iFlytek does not develop military technologies and would not comment on the company's security work or on whether data gathered through iFlytek's consumer products is firewalled from its government projects. )

For the CCP, monitoring speech appears to be about more than censorship. "The collection of voice and video data assists with

WIRED

# SUBSCRIBERS NOW HAVE UNLIMITED ACCESS TO WIRED.COM

To ensure that our new paywall does not interrupt your experience, register or sign in at:
**wired.com/account/sign-in**

Not yet a subscriber? To see your options, visit:
**wired.com/subscription**


# Get More A.I.
# Get More Robots
# Get More Ideas
# Get More Rockets
# Get More Crispr
# Get More Blockchain
# Get More Informed
# Get More at WIRED.com

**Subscribers get unlimited access to all WIRED stories online.**

To authenticate your subscription, go to WIRED.com/register. Not a subscriber but want to get the best daily news and analysis of the biggest stories in tech? Subscribe at WIRED.com/subscribe.

WIRED

Christie Hemm Klok

identifying people, networks, how people speak, what they care about, and what are the trends," says Samantha Hoffman, an analyst at the Australian Strategic Policy Institute's Cyber Centre in Canberra.

iFlytek has patented a system that can sift through large volumes of audio and video in order to identify files that have been copied or reposted—part of an operation that the patent explains as "very important in information security and monitoring public opinion." iFlytek responded that "analyzing audio and video data can have a number of potential applications, including identifying popular songs, detecting spam callers, etc."

But iFlytek does enable security work. In 2012 the Ministry of Public Security purchased machines from iFlytek focused on intelligent voice technology. The ministry chose Anhui province, where iFlytek is headquartered, as one of the pilot locations for compiling a voice-pattern database—a catalog of people's unique speech that would enable authorities to identify speakers by the sound of their voice.

The project relies on an iFlytek product called the Forensic Intelligent Audio Studio, a workstation that includes speakers, a microphone, and a desktop tower. The unit, which according to a 2016 local government procurement announcement sells for around $1,700, can identify people based on the unique characteristics of their voices. An iFlytek white paper uploaded online in 2013 touts voiceprint or speaker recognition as the "only biometric identification method that can be operated remotely," noting that "in the defense field, voiceprint identification technology can detect whether there are key speakers in a telephone conversation and then track the content of the conversation." The workstation can take a snippet of audio, compare it against the voices of 200 speakers, and pick out the person talking in under two seconds, according to the white paper.

Other countries also use voiceprint recognition for intelligence purposes. According to classified documents leaked by Edward Snowden, the National Security Agency has long used the tool to monitor terrorists and other targets. NSA analysts used speaker recognition, for example, to confirm the identities of Saddam Hussein, Osama bin Laden, and Ayman al-Zawahiri in audio files, and the FBI has a research arm devoted to the technology. Nuance once sold a system called Nuance Identifier, which it said allowed law enforcement to "perform searches against millions of voiceprints within seconds." The US Bureau of Prisons reportedly collects and stores prisoners' voiceprints in order to monitor their phone calls.

In 2017, Human Rights Watch published a report detailing iFlytek's government work. Maya Wang, a researcher with the rights group, says that the company's tools are an essential part of the party's plan to "build a digital totalitarian state"—a charge the company calls "baseless and absurd." iFlytek's voice biometric technologies make "tracking and identifying individuals possible," Wang says. At some point, the noble effort to reclaim the Chinese language and ease communication became indistinguishable from one to control it.

The company, like many US tech firms, maintains that its technology is "end-use agnostic."

iFlytek's work has come under particular suspicion in regions that pose a threat to the party's rule. One focus is greater Tibet, the culturally distinct part of western China where people have long fought for sovereignty. In Lhasa, iFlytek cofounded a lab at Tibet University that focuses on speech and information technology. The company says the goal of the lab is "the preservation and greater understanding of minority dialects and to help protect Tibetan culture." The company also makes a Tibetan input app called Dungkar, which means "conch shell," an auspicious symbol in Tibetan Buddhism.

According to Human Rights Watch, iFlytek's technology appears to enable surveillance in Xinjiang, a region in northwest China populated by the predominantly Muslim Uighur minority group. In recent years, the Chinese government has tightened its grip on Uighurs, interning more than a million people in camps and farming out others to factories as forced labor. Residents have been made to install nanny apps on their phones, give biometric data at regular security checkpoints, and host cultural inspectors in their homes. In official materials, these inspectors are called, with no apparent hint of irony, "big sisters and big brothers."

The crackdown is perhaps most intense in Kashgar, an ancient city on the Silk Road that was once a major destination for tourists and is now home to at least a dozen internment camps. In 2016 police in Kashgar contracted with an iFlytek subsidiary to purchase 25 voiceprint terminals. According to the procurement agreement, the technology would be used to collect speech samples for biometric dossiers that also include photos, fingerprints, and DNA samples. The same subsidiary helped Kashgar University integrate big data on its campus for the purpose of ensuring its "safe and stable operation" in a "multiethnic" environment, according to the subsidiary's website.

In May 2016, iFlytek signed a strategic cooperation agreement with the agency that operates prisons in Xinjiang. It is unclear exactly how iFlytek's technology is used in this context, but a post on Sohu, a Chinese platform, stated that iFlytek's work would "ensure the security and stability of prisons."

A group of US scholars met with a member of iFlytek's leadership in Beijing last summer and pushed him on the company's work in Xinjiang: "He characterized it as, 'We're helping the government to better understand Uighurs through providing those language capabilities,'" one security analyst who was there told me.

Wang, of Human Rights Watch, says

the fact that iFlytek builds "both benign, commercial applications as well as surveillance applications is precisely what makes them very problematic." iFlytek's data from government projects is likely used to improve its consumer products—and vice versa. "They can train and perfect their AI systems on lots of samples, collected through not only their commercial but also through their military and policing applications," she says. Every time a traveler speaks into the Translator, their words feed an algorithmic black box. All told, iFlytek's technologies promise to dramatically reshape life for people in China and elsewhere, by turning an individual's voice into both a crucial time-saver and an inescapable marker of their identity.

**In the United States, companies like Apple have fought hard against the perception that their devices are always listening. In China, though, it was a selling point. A Flying Fish sales rep said: "You only have to wake it up one time, and then it's awake."**

In recent years, iFlytek entered a stage of international expansion, brokering research partnerships with universities in Canada, New Zealand, and the United States. On the occasion of its agreement with MIT's CSAIL, lab director Daniela Rus said the partnership would focus on addressing "the biggest challenges of the 21st century" by "finding ways to better harness the strengths of both human and artificial intelligence." Critics of the partnership had a more cynical view: iFlytek gave an undisclosed sum of money in return for the prestige of the MIT brand.

The announcement came eight months after Human Rights Watch exposed iFlytek's work in Xinjiang, and as awareness of the indoctrination camps spread, some MIT researchers grew alarmed. Alan Lundgard, a graduate student at CSAIL, told me that he learned his work would be funded by iFlytek only after he started his position at the lab. When he emailed a CSAIL administrator to explain that he had moral objections to receiving money from the company, the administrator responded that he could find other funding for his work. If he didn't, he said, Lundgard would have to return the payments that he had already received.

Last summer, after press reports revealed that sex offender Jeffrey Epstein and the Saudi state had funded other labs at MIT, students and staff staged a series of protests, and CSAIL's agreements with Chinese tech companies were thrust into the spotlight. "The concerns about surveillance activities in China are very real," says Roger Levy, the director of MIT's Computational Psycholinguistics Laboratory.

"MIT needs to take very seriously that, when we enter into an engagement with another entity, we are lending it a kind of credibility."

In October, the Department of Commerce placed iFlytek on the US government's Entity List of companies subject to export restrictions. In response, Liu Qingfeng posted a defiant missive on iFlytek's site, in Chinese, that did little to dispel perceptions of close government ties. "Without the revolutionary martyrs giving their blood, today there would be no modern China," it read. "Without the prosperity and development of modern China, iFlytek could not have debuted on the industrial stage … There is no force that can stop our confidence and pace in building a beautiful world with artificial intelligence!" The next day, US secretary of state Mike Pompeo touched on the crackdown in Xinjiang in a speech. "The pages of George Orwell's *1984* are coming to life there," he said.

Last fall, in response to emailed questions, a CSAIL spokesperson said that the addition of iFlytek to the Entity List had triggered a review by MIT, but that in the interim CSAIL would continue with the partnership. In April, after WIRED sent more inquiries, MIT announced that it had terminated the relationship in February. The university would not disclose the rationale. As for Lundgard's funding, a spokesperson responded that "the Institute must strike a balance between the funding available to carry out research and the individual preferences of researchers."

When I mentioned iFlytek's work to a friend in Shanghai, she said it reminded her of the story "City of Silence," by the Chinese science fiction writer Ma Boyong. The story is set in a future society where speech is tightly controlled. The people are clever at adapting to each new limit, turning to homonyms and slang to circumvent censors, and in time the authorities realize that the only way to truly control speech is to publish a List of Healthy Words, forbid all terms not on the list, and monitor voice as well as text. Anytime the protagonist leaves the house, he has to wear a device called the Listener, which issues a warning whenever he strays from the list of approved words. The realm of sanctioned speech dwindles day by day.

Eventually the protagonist discovers the existence of a secret Talking Club, where, in an apartment encircled by lead curtains, members say whatever they want, have sex, and study *1984*. Feeling alive again, he realizes that he has been suppressing "a strong yearning to talk." This brief encounter with hope is squelched when the authorities develop radar dishes that can intercept signals through lead curtains. By the end of the story, there are no healthy words left, and the hero walks the city mutely, alone with his thoughts. "Luckily, it was not yet possible to shield the mind with technology," Ma writes.

The Chinese surveillance state has sometimes involved what the scholar Jathan Sadowski calls "Potemkin AI"—technology that seems all-powerful but is not. But on a practical level, whether the technology is as accurate as advertised makes little difference. When people have the impression that the state can locate them using just a few seconds of intercepted audio, they begin to self-censor. Big Brother is internalized.

I reflected on this last April, while visiting Shanghai. One day I took the metro to the massive National Exhibition and Convention Center, at the city's western edge, to attend the Shanghai Auto Show. iFlytek was one of the exhibitors, and when I reached its booth a video was playing on a large screen. It showed a clean-cut young man getting behind the wheel of a red sedan. "Hi Peter!" a voice said, as a screen attached to the dashboard flashed his picture. Peter beamed as if he had been waiting his whole life for his car to recognize him.

White characters flashed across a neon background in rapid succession, so fast as to be almost subliminal. *Understands your needs. Establishes your feelings. The intelligent interactive auto system of the future.*

A sales associate named Xing Xiaoling led me to a small station to try out the auto assistant for myself. We put on headphones. "Flying Fish, hello!" she said, and the screen woke up.

"I want to listen to a song," Xing said, and a saccharine pop number blasted into my ears. She showed me how to buy airplane tickets to Beijing with a few simple voice cues, a feature available to users who connect their Alipay or WeChat Pay mobile payments accounts. Xing added that Flying Fish was always at the ready.

iFlytek's virtual assistants are often called "China's Siri," but Xing thought that comparison did the company a disservice. "With Siri, you have to say 'Hey, Siri' every time," she told me. "It's very mechanical." In the US, companies like Apple have fought hard against the perception that their devices are always listening. In China, though, it was a selling point. "You only have to wake it up one time, and then it's awake," Xing said of Flying Fish.

I captured the conversation with my digital recorder and took notes as she spoke. When I glanced back at the screen I saw that I wasn't the only one who had made a recording. Right there, on the intelligent interactive auto system of the future, was a complete record of all our words.

ARTIFICIAL INTELLIGENCE IS LEARNING FASTER BY THE MOMENT.
HOW WILL HUMANS KEEP UP?

Now is the time to think about the future of

# Thinking Machines

# Is the brain a useful model for AI?

BY KELLY CLANCY

**In the summer** of 2009, the Israeli neuroscientist Henry Markram strode onto the TED stage in Oxford, England, and made an immodest proposal: Within a decade, he said, he and his colleagues would build a complete simulation of the human brain inside a supercomputer. They'd already spent years mapping the cells in the neocortex, the supposed seat of thought and perception. "It's a bit like going and cataloging a piece of the rain forest," Markram explained. "How many trees does it have? What shapes are the trees?" Now his team would create a virtual rain forest in silicon, from which they hoped artificial intelligence would organically emerge. If all went well, he quipped, perhaps the simulated brain would give a follow-up TED talk, beamed in by hologram.

Markram's idea—that we might grasp the nature of biological intelligence by mimicking its forms—was rooted in a long tradition, dating back to the work of the Spanish anatomist and Nobel laureate Santiago Ramón y Cajal. In the late 19th century, Cajal undertook a microscopic study of the brain, which he compared to a forest so dense that "the trunks, branches, and leaves touch everywhere." By sketching thousands of neurons in exquisite detail, Cajal was able to infer an astonishing amount about how they worked. He saw that they were effectively one-way input-output devices: They received electrochemical messages in treelike structures called dendrites and passed them along through slender tubes called axons, much like "the junctions of electric conductors."

Cajal's way of looking at neurons became the lens through which scientists studied brain function. It also inspired major technological advances. In 1943, the psychologist Warren McCulloch and his protégé Walter Pitts, a homeless teenage math prodigy, proposed an elegant framework for how brain cells encode complex thoughts. Each neuron, they theorized, performs a basic logical operation, combining multiple inputs into a single binary output: true or false. These operations, as simple as letters in the alphabet, could be strung together into words, sentences, paragraphs of cognition. McCulloch and Pitts' model turned out not to describe the brain very well, but it became a key part of the architecture of the first modern computer. Eventually, it evolved into the artificial neural networks now commonly employed in deep learning.

These networks might better be called neural-*ish*. Like the McCulloch-Pitts neuron, they're impressionistic portraits of what goes on in the brain. Suppose you're approached by a yellow Labrador. In order to recognize the dog, your brain must funnel raw data from your retinas through layers of specialized neurons in your cerebral cortex, which pick out the dog's visual features and assemble the final scene. A deep neural network learns to break down the world similarly. The raw data flows from a large array of neurons through several smaller sets of neurons, each pooling inputs from the previous layer in a way that adds complexity to the overall picture: The first layer finds edges and bright spots, which the next combines into textures, which the next assembles into a snout, and so on, until out pops a Labrador.

Despite these similarities, most artificial neural networks are decidedly un-brainlike, in part because they learn using mathematical tricks that would be difficult, if not impossible, for biological systems to carry out. Yet brains and AI models do share something fundamental in common: Researchers still don't understand why they work as well as they do.

What computer scientists and neuroscientists are after is a universal theory of intelligence—a set of principles that holds true both in tissue and in silicon. What they have instead is a muddle of details. Eleven years and $1.3 billion after Markram proposed his simulated brain, it has contributed no fundamental insights to the study of intelligence.

Part of the problem is something the writer Lewis Carroll put his finger on more than a century ago. Carroll imagined a nation so obsessed with cartographic detail that it kept expanding the scale of its maps—6 yards to the mile, 100 yards to the mile, and finally a mile to the mile. A map the size of an entire country is impressive, certainly, but what does it teach you? Even if neuroscientists can re-create intelligence by faithfully simulating every molecule in the brain, they won't have found the underlying principles of cognition. As the physicist Richard Feynman famously asserted, "What I cannot create, I do not understand." To which Markram and his fellow cartographers might add: "And what I *can* create, I do not *necessarily* understand."

It's possible that AI models don't need to mimic the brain at all. Airplanes fly despite bearing little resemblance to birds. Yet it seems likely that the fastest way to understand intelligence is to learn principles from biology. This doesn't stop at the brain: Evolution's blind design has struck on brilliant solutions across the whole of nature. Our greatest minds are currently hard at work against the dim almost-intelligence of a virus, its genius borrowed from the reproductive machinery of our cells like the moon borrows light from the sun. Still, it's crucial to remember, as we catalog the details of how intelligence is implemented in the brain, that we're describing the emperor's clothes in the absence of the emperor. We promise ourselves, however, that we'll know him when we see him—no matter what he's wearing.

---

KELLY CLANCY *(@kellybclancy) is a neuroscientist at University College London and DeepMind. She wrote about fatal familial insomnia, a rare disease, in issue 27.02.*

# Why didn't AI save us from Covid-19?

BY GREGORY BARBER

**In late January,** more than a week before Covid-19 had been given that name, hospitals in Wuhan, China, began testing a new method to screen for the disease, using artificial intelligence. The plan involved chest CTs—three-dimensional scans of lungs displayed in finely detailed slices. By studying thousands of such images, an algorithm would learn to decipher whether a given patient's pneumonia appeared to stem from Covid-19 or something more routine, like influenza.

In the US, as the virus spread in February, the idea appeared to hold promise: With conventional tests in short supply, here was a way to get more people screened, fast. Health professionals, however, weren't so sure. Although various diagnostic algorithms have won approval from the US Food and Drug Administration—for wrist fractures, eye diseases, breast cancer—they generally spend months or years in development. They're deployed in different hospitals filled with different kinds of patients, interrogated for flaws and biases, pruned and tested again and again.

Was there enough data on the new virus to truly discern one pneumonia from another? What about mild cases, where the damage may be less clear? The pandemic wasn't waiting for answers, but medicine would have to.

In late March, the United Nations and the World Health Organization issued a report examining the lung CT tool and a range of other AI applications in the fight against Covid-19. The politely bureaucratic assessment was that few projects had achieved "operational maturity."

The limitations were older than the crisis, but aggravated by it. Reliable AI depends on our human ability to collect data and make sense of it. The pandemic has been a case study in why that's hard to do mid-crisis. Consider the shifting advice on mask wearing and on taking ibuprofen, the doctors wrestling with who should get a ventilator and when. Our daily movements are dictated by uncertain projections of who will get infected or die, and how many more will die if we fail to self-isolate.

As we sort out that evidence, AI lags a step behind us. Yet we still imagine that it possesses more foresight than we do.

Take drug development. One of the flashiest AI experiments is by Google-affiliated DeepMind. The company's AlphaFold system is a champion at the art of protein modeling—predicting the shape of tiny structures that make up the virus. In the lab, divining those structures can be a months-long process; DeepMind, when it released schematics for six viral proteins in March, had done it in days. The models were approximations, the team cautioned, churned out by an experimental system. But the news left an impression: AI had joined the vaccine race.

In the vaccine community, however, the effort elicited a shrug.

"I can't see much of a role for AI right now," says Julia Schaletzky, a veteran drug discovery researcher and head of UC Berkeley's Center for Emerging and Neglected Diseases. Plenty of well-defined protein targets have been confirmed in labs without the help of AI. It would be risky to spend precious time and grants starting from scratch, using the products of an experimental system. Technological progress is good, Schaletzky says, but it's often pushed at the expense of building on what's known and promising.

She says there's potential in using AI to help find treatments. AI algorithms can complement other data-mining techniques to help us sift through reams of information we already have—to spot encouraging threads of research, for example, or older treatments that hold promise. One drug identified this way, baricitinib, is now going to clinical trials. Another hope is that AI could yield insights into how Covid-19 attacks the body. An algorithm could mine lots of patient records and determine who is more at risk of dying and who is more likely to survive, turning anecdotes whispered between doctors into treatment plans.

But again, it's all a matter of data—what data we've already gathered, and whether we've organized it in a way that's useful for machines. Our health care system doesn't give up information easily to train such systems; privacy regulations and balkanized data silos will stop you even before the antiquated, error-filled health databases do.

It's possible this crisis will change that. Maybe it will push us to rethink how data is stored and shared. Maybe we'll keep studying this virus even after the chaos dissipates and the attention wanes, giving us solid data—and better AI—when the next pandemic arrives. For now, though, we can't be surprised that AI hasn't saved us from this one.

---

GREGORY BARBER *(@GregoryJBarber) is a* WIRED *staff writer. He wrote about energy-saving AI in issue 28.04.*

# As machines get smarter, how will we relate to them?

BY TOM SIMONITE

**Bicycling in a hilly,** busy city like San Francisco provides a cognitive as well as a physical workout. I survive in traffic by flexing not only my quadriceps but my theory of mind, the capacity to imagine the thoughts and intentions of others: Will the guy riding a Bird scooter swerve to avoid that pothole? Will the UPS driver try to run that yellow light? But self-driving cars stump me.

Last year, when General Motors stepped up testing of its Cruise autonomous vehicles, I began to encounter the sporty white hatchbacks with rooftop sensors once or more each day. At first the cars were overcautious and twitchy, earning angry honks from human drivers for unnecessary braking and hesitant turns. With time, I felt able to read and even exploit these timorous robots. If I strayed from the bike lane, they would hang back, giving me extra room to maneuver. At four-way stops, they tended to dither, allowing me to dart ahead.

Then a couple of Cruise vehicles surprised me one week with displays of more confident driving. Rather than meekly waiting behind bikes, they zipped past. My theory of robot mind was vaporized, replaced by a feeling of unease: As AI grows more capable and assertive, how will we relate to it?

Generally speaking, people adapt well to new technologies. We steer hunks of speeding metal and communicate via tiny icons with élan. But more complex and dynamic AI systems, like robot cars, will challenge us in new ways. Millennia of biological and cultural evolution have given us brains and societies primed to read the behaviors, quirks, and transgressions of other people. With thinking machines, says Iyad Rahwan, director of the Max Planck Institute for Human Development in Berlin, "we're sort of stumbling in the dark."

Our tendency is to assume, perhaps without realizing it, that AI systems have minds somewhat like ours. In the 1960s, MIT professor Joseph Weizenbaum created the world's first chatbot, ELIZA, and programmed it to parody a therapist by responding to typed statements by rephrasing them into questions. To Weizenbaum's shock, his human subjects sensed humanlike intelligence and emotion in the bot. "What I had not realized is that extremely short exposures to a relatively simple computer program could induce powerful delusional thinking in quite normal people," he wrote.

The hazards of not thinking clearly about AI have grown since then; soon, they will become momentous. The perky feminine-coded personas of virtual assistants like Amazon's Alexa divert us from considering the risks of allowing large corporations to record in our intimate spaces. The way that drivers, cyclists, and pedestrians understand and react to robot vehicles is a matter of life or death.

Even when there's more than a split second to mull an AI system's decisions, its behavior may be impossible to fully explain. The machine-learning algorithms behind many recent AI milestones can't be programmed or reverse-engineered in the same way as conventional software. Experts call these systems black boxes, because even their creators cannot fully explain how they work. You may one day have to make a life-changing medical decision based on advice from a doctor that was in turn based on advice from an AI system built on methods and resources no human or regulatory body could check. Artificial intelligence is alien intelligence, perceiving and processing the world in ways fundamentally different from the way we do.

Misjudging AI systems may lead us to misjudge people. Madeleine Clare Elish, an anthropologist at Data & Society, a research institute, has studied accidents involving automation, and says moral blame for system failures often lands unfairly on humans who didn't create them. After an Uber self-driving car killed a jaywalking pedestrian in Arizona in 2018, police focused public attention on the safety driver, who appeared to be distracted in video from the car. Federal investigators later found that Uber had disabled the car's emergency braking system and programmed its algorithms to look for pedestrians only at crosswalks. Uber stepped up safety features and can no longer test in Arizona, but it has been cleared of criminal liability; the safety driver may yet face charges.

People may find it even harder to clearly see the functions and failings of more sophisticated AI systems that continually adapt to their surroundings and experiences. "What does it mean to understand what a system does if it is dynamic and learning and we can't count on our previous knowledge?" Elish asks. As we interact with more AI systems, perhaps our own remarkable capacity for learning will help us develop a theory of machine mind, to intuit their motivations and behavior. Or perhaps the solution lies in the machines, not us. Engineers of future AI systems might need to spend as much time testing how well they play with humans as on adding to their electronic IQs.

---

**TOM SIMONITE** *(@tsimonite) covers intelligent machines for* WIRED.

# Are killer robots inevitable?

BY PAUL SCHARRE

**In war, speed kills.** The soldier who is a split second quicker on the draw may walk away from a firefight unscathed; the ship that sinks an enemy vessel first may spare itself a volley of missiles. In cases where humans can't keep up with the pace of modern conflict, machines step in. When a rocket-propelled grenade is streaking toward an armored ground vehicle, an automated system onboard the vehicle identifies the threat, tracks it, and fires a countermeasure to intercept it, all before the crew inside is even aware. Similarly, US Navy ships equipped with the Aegis combat system can switch on Auto-Special mode, which automatically swats down incoming warheads according to carefully programmed rules.

These kinds of defensive systems have been around for decades, and at least 30 countries now use them. In many ways, they're akin to the automatic braking systems in newer cars, intervening only under specific emergency conditions. But militaries, like automakers, have gradually been giving machines freer rein. In an exercise last year, the United States demonstrated how automation could be used throughout the so-called kill chain: A satellite spotted a mock enemy ship and directed a surveillance plane to fly closer to confirm the identification; the surveillance plane then passed its data to an airborne command-and-control plane, which selected a naval destroyer to carry out an attack. In this scenario, automation bought more time for officers at the end of the kill chain to make an informed decision—whether or not to fire on the enemy ship.

Militaries have a compelling reason to keep humans involved in lethal decisions. For one thing, they're a bulwark against malfunctions and flawed interpretations of data; they'll make sure, before pulling the trigger, that the automated system hasn't misidentified a friendly ship or neutral vessel. Beyond that, though, even the most advanced forms of artificial intelligence cannot understand context, apply judgment, or respond to novel situations as well as a person. Humans are better suited to getting inside the mind of an enemy commander, seeing through a feint, or knowing when to maintain the element of surprise and when to attack.

But machines are faster, and firing first can carry a huge advantage. Given this competitive pressure, it isn't a stretch to imagine a day when the only way to stay alive is to embrace a fully automated kill chain. If just one major power were to do this, others might feel compelled to follow suit, even against their better judgment. In 2016, then deputy secretary of defense Robert Work framed the conundrum in layperson's terms: "If our competitors go to Terminators," he asked, "and it turns out the Terminators are able to make decisions faster, even if they're bad, how would we respond?"

Terminators aren't rolling off the assembly line just yet, but each new generation of weapons seems to get us closer. And while no nation has declared its intention to build fully autonomous weapons, few have forsworn them either. The risks from warfare at machine speed are far greater than just a single errant missile. Military scholars in China have hypothesized about a "battlefield singularity," a point at which combat moves faster than human cognition. In this state of "hyperwar," as some American strategists have dubbed it, unintended escalations could quickly spiral out of control. The 2010 "flash crash" in the stock market offers a useful parallel: Automated trading algorithms contributed to a temporary loss of nearly a trillion dollars in a single afternoon. To prevent another such calamity, financial regulators updated the circuit breakers that halt trading when prices plummet too quickly. But how do you pull the plug on a flash war?

Since the late 19th century, major military powers—whether Great Britain and Germany or the United States and the USSR—have worked together to establish regulations on all manner of modern killing machines, from exploding bullets to poison gas to nuclear weapons. Sometimes, as with anti-satellite weapons and neutron bombs, formal agreements weren't necessary; the parties simply engaged in tacit restraint. The goal, in every case, has been to mitigate the harms of war.

For now, no such consensus exists with fully autonomous weapons. Nearly 30 countries support a complete ban, but none of them is a major military power or robotics developer. At the United Nations, where autonomous weapons are a subject of annual debate, China, Russia, and the United States have all stymied efforts to enact a ban. (The US and Russia have objected outright, while China in 2018 proposed a ban that would be effectively meaningless.) One of the challenging dynamics at the UN is the tug-of-war between NGOs such as the Campaign to Stop Killer Robots, whose goal is disarmament, and militaries, which won't agree to disarm unless they can verify that their adversaries will too.

Autonomous weapons present some unique challenges to regulation. They can't be observed and quantified in quite the same way as, say, a 1.5-megaton nuclear warhead. Just what constitutes autonomy, and how much of it should be allowed? How do you distinguish an adversary's remotely piloted drone from one equipped with Terminator software? Unless security analysts can find satisfactory answers to these questions and China, Russia, and the US can decide on mutually agreeable limits, the march of automation will continue. And whichever way the major powers lead, the rest of the world will inevitably follow.

---

PAUL SCHARRE *(@paul_scharre) is a senior fellow at the Center for a New American Security and the author of* Army of None: Autonomous Weapons and the Future of War.

# What exactly *is* intelligence?

BY WILL KNIGHT

**Elizabeth Spelke,** a cognitive psychologist at Harvard, has spent her career testing the world's most sophisticated learning system—the mind of a baby.

Gurgling infants might seem like no match for artificial intelligence. They are terrible at labeling images, hopeless at mining text, and awful at videogames. Then again, babies can do things beyond the reach of any AI. By just a few months old, they've begun to grasp the foundations of language, such as grammar. They've started to understand how the physical world works, how to adapt to unfamiliar situations.

Yet even experts like Spelke don't understand precisely how babies—or adults, for that matter—learn. That gap points to a puzzle at the heart of modern artificial intelligence: We're not sure what to aim for.

Consider one of the most impressive examples of AI, AlphaZero, a program that plays board games with superhuman skill. After playing thousands of games against itself at hyperspeed, and learning from winning positions, AlphaZero independently discovered several famous chess strategies and even invented new ones. It certainly seems like a machine eclipsing human cognitive abilities. But AlphaZero needs to play millions more games than a person during practice to learn a game. Most tellingly, it cannot take what it has learned from the game and apply it to another area.

To some members of the AI priesthood, that calls for a new approach. "What makes human intelligence special is its adaptability—its power to generalize to never-seen-before situations," says François Chollet, a well-known AI engineer and the creator of Keras, a widely used framework for deep learning. In a November research paper, he argued that it's misguided to measure machine intelligence solely according to its skills at specific tasks. "Humans don't start out with skills; they start out with a broad ability to acquire new skills," he says. "What a strong human chess player is demonstrating isn't the ability to play chess per se, but the potential to acquire any task of a similar difficulty. That's a very different capability."

Chollet posed a set of problems designed to test an AI program's ability to learn in a more generalized way. Each problem requires arranging colored squares on a grid based on just a few prior examples. It's not hard for a person. But modern machine-learning programs—trained on huge amounts of data—cannot learn from so few examples. As of late April, more than 650 teams had signed up to tackle the challenge; the best AI systems were getting about 12 percent correct.

It isn't yet clear how humans solve these problems, but Spelke's work offers a few clues. For one thing, it suggests that humans are born with an innate ability to quickly learn certain things, like what a smile means or what happens when you drop something. It also suggests we learn a lot from each other. One recent experiment showed that 3-month-olds appear puzzled when someone grabs a ball in an inefficient way, suggesting that they already appreciate that people cause changes in their environment. Even the most sophisticated and powerful AI systems on the market can't grasp such concepts. A self-driving car, for instance, cannot intuit from common sense what will happen if a truck spills its load.

Josh Tenenbaum, a professor in MIT's Center for Brains, Minds & Machines, works closely with Spelke and uses insights from cognitive science as inspiration for his programs. He says much of modern AI misses the bigger picture, likening it to a Victorian-era satire about a two-dimensional world inhabited by simple geometrical people. "We're sort of exploring *Flatland*—only some dimensions of basic intelligence," he says. Tenenbaum believes that, just as evolution has given the human brain certain capabilities, AI programs will need a basic understanding of physics and psychology in order to acquire and use knowledge as efficiently as a baby. And to apply this knowledge to new situations, he says, they'll need to learn in new ways—for example, by drawing causal inferences rather than simply finding patterns. "At some point—you know, if you're intelligent—you realize maybe there's something else out there," he says.

A self-driving car cannot intuit from common sense what will happen if a truck spills its load.

WILL KNIGHT *(@willknight) is a senior writer for* WIRED*, covering artificial intelligence.*

# Please, let us be lucky.

BY
Brooke Jarvis

**The quest to find a vaccine for Covid-19 has become a worldwide race of unprecedented scope and speed. The first contender entered human trials—and Neal Browning's arm—on March 16. Inside the early days of what might, just might, be the world's fastest vaccine.**

ILLUSTRATION BY
Heads of State

# Monday

**morning, 8 am.** Neal Browning walked into the waiting room. He took in the reception desk, the play area for kids, the table full of magazines that he was too cautious to touch. There was another patient waiting, a woman in her forties with brown, chin-length hair. Browning wasn't sure whether she was here for the same historic reason that he was, so he decided to follow standard waiting-room procedure and sat quietly—no conversation, no eye contact. After a few minutes, a nurse called the woman back and he watched her disappear behind a door. Another few minutes passed and it was his turn.

First, there were questions: Still no fever? Still no contact with anyone who's been sick? Then there was a round of blood draws. Browning, a 46-year-old network engineer, had taken the morning off from his job at Microsoft, where he'd been unusually busy for weeks: His team was following the spread of a deadly new virus around the world, preparing firewalls and VPNs to allow a global workforce to suddenly start working from home. The engineers trailed the virus from Wuhan to the rest of China, to Europe, and to his own doorstep in Washington state.

Eighteen days before he walked into the waiting room, a teenager who lived 10 miles from Browning's house in Bothell, Washington, had tested positive for the new virus. The teen hadn't traveled abroad or had known contact with anyone with a positive case. Browning wrote on Facebook that Pandora's box had been opened. The next day, officials announced that the first person in the United States had died from the virus, at a hospital just 5 miles from Browning's house. (Earlier deaths would later be uncovered.) A few days later, when a friend texted Browning with news that a group of researchers were looking for volunteers to test a possible new vaccine, he marveled at how quickly the vaccine had appeared but didn't hesitate to sign up.

The researchers got in touch, asking to check his blood work and his medical background. (For the earliest phase of trials, they were looking for participants with a clean bill of health, so it would be simpler to trace any changes caused by the vaccine.) Browning started Googling. Viruses, vaccines, RNA, DNA—so many details of his own biology to which he hadn't spared a thought since an introductory science class back in college. He talked with his fiancée and his mother, both of whom are registered nurses, about the risks of offering himself as a test subject. There was the chance he'd have a bad reaction to the shot; the theoretical possibility that the vaccine might make his body produce antibodies that actually made the virus worse; and simply the inherent risk of unknowability associated with the brand-new. Still, to Browning, the risks seemed low when compared with the known danger. On the news, he watched as deaths mounted at a nearby nursing home, as the governor shut down concerts and then schools and then businesses. Now the moment was here, and he had no doubts. Only hopes.



Browning watched as his veins filled vial after vial, each of them a viscous red record of what his body was like now, in its "before" state. Then it was time for the shot. It took a few awkward tugs for the pharmacist to get the sleeve of Browning's blue collared shirt above his deltoid, but that was the only drama visible for anyone to see. The needle slid in, the needle slid out. A news camera clicked. Twenty-five micrograms of fluid, the first and fastest hope for stopping a pandemic that had been officially declared just five days before, diffused into the muscle of his right arm.

To Browning, it felt like "a big nothing." That's what it looked like too. He pulled his sleeve back down. The pharmacist disposed of the syringe. From this moment on, any action would be invisible, hidden away inside Browning's body, where the dramatis personae were proteins and cytokines, T cells and B cells.

In the exam room, where he was asked to wait an hour to make sure there was no immediate adverse reaction, Browning sent some texts, messed around on his phone, and tried to imagine what might be going on inside him. Right now, as far as he could tell, the answer seemed to be not much out of the ordinary. It was entirely possible that this would prove true—that nothing much *would* happen. This very first human trial of a vaccine designed to fight SARS-CoV-2, the newly emerged coronavirus that was disrupting the world, could lead to disappointment, just like so many trials for so many other vaccines for so many other diseases. To make a successful vaccine, to test its safety and effectiveness, and to get it licensed for widespread use in healthy humans, is usually a long and arduous process. Development commonly takes a decade or more; historically, for any given attempt, the statistical chance of failure is 94 percent.

But Browning was an optimist. He knew that the vaccine candidate now in his arm had made it there in record time. Instead of years, the timescale was measured in days: Just 66 of them had passed since the genome of the virus had first been published. Maybe more records were possible. He lay on the exam table and hoped, fervently, that at the gates of his cells something big was beginning.

Across a panicked world, anybody who saw the day's news—that the first four human beings had been injected with a vaccine meant to fight a virus that seemed to be changing everything—had to hope the same. Please, we pleaded, as businesses shuttered and families stayed apart and ambulance sirens wailed. Please, as people risked their lives in ERs and grocery stores. Please, as we tried to imagine a future that

could safely return to what we had once been so bold as to think of as normal life. Please, let us be lucky, and please, down in the microscopic battlefield of Neal Browning's immune system, let some drama be starting.

**For the great hope** against a 21st-century virus, inoculation is a surprisingly old technology. As early as the 10th century, the Chinese were known to put material from the lesions of people infected with smallpox on the nostrils of the healthy, in an attempt to give them a less virulent course of the disease; by the 1600s, people in the Ottoman Empire were letting pus be grafted under the skin of their arms and legs. In the 1720s, an updated version of the practice was so accepted that Caroline of Ansbach, the Princess of Wales, had it performed on her two young daughters. (Still, the death rate for those inoculated was as high as 3 percent.) Edward Jenner, the English doctor who proved that exposure to a different virus, cowpox, protected people from getting smallpox at all, started shipping what are considered the very first vaccines (the word derives from the Latin word for "cow") to his medical colleagues in the same decade in which Eli Whitney invented the cotton gin.

Since then, the process of vaccine creation has changed dramatically. In the 19th century, scientists discovered that they could teach people's immune systems to fight off viruses by exposing them to versions inactivated with heat or chemicals. As methods advanced, they found they could breed less virulent versions of viruses in labs. They could also make effective vaccines by exposing human cells to only a small part of a virus, such as the protein structures that actually irritate the immune system, or even to synthetic structures, convincing enough to be thoroughly confused for the real thing. They could circulate those structures by attaching them to other, less dangerous viruses; they could even, theoretically, instruct human cells to make the structures themselves. What mattered was simply that the body could meet a convincing enough threat that it would prepare its own specially designed resistance in advance, before it ever encountered the real thing. The strategies changed, but their basic principle stayed the same: For all our technology, our best defense is still to activate the ancient protections that are already waiting inside us.

When something unfamiliar and possibly dangerous enters your body, the first response is from what's known as your innate immune system. This is your fastest, oldest (evolutionarily speaking), and certainly bluntest response to invasion, with one basic arsenal of weapons to use against whatever it meets. For its signature move, the innate immune system leans heavily on inflammation—which can manifest as everything from redness around a small cut to classic cold and flu symptoms such as fever and coughs to swelling in and around vital organs—as a way of calling in white blood cells to attack invaders. What we perceive as symptoms are often our bodies' own, cruder defenses, mobilizing to kill germs where they are and keep them from spreading through the body. "When this process works correctly," says Angela Rasmussen, a virologist at Columbia University's Mailman School of Public Health, "inflammation is very tightly controlled."

That's because the innate immune system is also responsible for calling in your next, and more sophisticated line of defense—your adaptive, or acquired, immune system. This is the smart system, the one that can change and adjust, build new defenses to deal with specific threats, and then hold those protections in reserve in case their corresponding threats return. It also regulates the innate immune system. Peptides called cytokines serve as messengers, letting your immune responses know when it's time to accelerate or pull back.

Benjamin Neuman, a virologist at Texas A&M who has been studying coronaviruses for more than two decades, compares the innate immune system to a baby having a tantrum. It doesn't learn, and it can't recognize what it's actually mad at; it mostly just screams and shouts and throws things. (Because its tantrums can be dangerous, Neuman also compares it to Rambo, firing its ammunition indiscriminately in all directions.) Still, its reaction protects you, somewhat, while the adaptive immune system, the adult in the room, hears the yelling, tells the baby to calm down, and figures out what to do.

This is where your B cells and T cells, the problem-solvers and soldiers of the adaptive immune system, come in. Each day, these cells are undergoing their own form of natural selection: developing and recombining at random to create billions of antibodies and receptors in different patterns, each of them a possible match for dangers your body has never actually encountered. (T and B cells, thanks to this random development, are some of the only cells that are different from one identical twin to the next.) All that variation creates a vast, always rotating repertoire of potential immune responses. When a new virus comes along, wielding a new shape of protein that it can use like a crowbar to break into your healthy cells, some of your B and T cells, simply because there are so many of them, will be able to neutralize it. (The name for the specific molecular structure that your immune system targets is "antigen.") Immune cells are "circulating in your blood, all the time, just waiting to bind

AP Photo/Ted S. Warren

**Browning gets his shot of the first Covid-19 vaccine to make it to human trials.**

with their specific form," Rasmussen says. "They're out there, looking for their one. And for a very small percentage of those, that one is going to be SARS-CoV-2."

Once the match is made, the cells that can make the right antibodies start replicating like mad. This, plus something called immunological memory, is why vaccines work: B and T cells, like a sports team learning the playbook of a rival, gradually become better and faster at counteracting the new intruder. When the adversary (or, in the case of a vaccine, the imitation of the adversary) is gone, the immune system hangs on to copies of the playbook, in the form of clones of those more "experienced" cells. If the antigen returns, they can skip the whole process; they already know how to win.

Every vaccine, explains Shane Crotty, a virologist in the Center for Infectious Disease and Vaccine Research at La Jolla Institute for Immunology, depends on this scattershot genius of the immune system: "Boy, are you glad that you have those rare cells that could actually recognize the rare germ."

**Inside your body, the** arrival of a new virus starts the clock on a frantic race—but a strange one, where the runners are full of tricks and schemes to try to trip each other up. The virus, unable to survive on its own, wants to hijack your cells and use them to replicate itself. For your adaptive immune system, the challenge is to find and create enough of the right antibodies before the virus spreads too far—but also before the screaming baby Rambo that is your innate immune system does too much damage.

With SARS-CoV-2, the competition is a particularly difficult one. Some viruses are made up of only the bare minimum genetic material necessary to get inside a host cell and make copies of themselves. But coronaviruses, says Neuman, "are the biggest RNA viruses that we know, and so they've got more of these little bells and whistles"—by which he means clever tricks to bias the race, to confound and hobble and outrun the immune system. "They've got the gold package," he says. The novel coronavirus is as much as 10 times better than the first SARS virus at binding to a cell. Once inside, it twists the structure of human cells, turning them into super-efficient virus factories. It has a camouflage strategy that lets it sneak past cell receptors. And it has an enzyme that Neuman likens to a paper shredder: It destroys the messenger RNA that the cell uses to call for help once it does realize that something has gone wrong.

Scientists are still scrambling to understand the details of how the novel coronavirus affects us and why different people, once infected, have such different outcomes. But the patients who do best, Rasmussen says, seem to have ongoing, solid communication between the parts of their immune systems: a quick inflammatory response, but one that is turned off once it has served its purpose. When patients die, it appears to be because the virus has managed to spread widely by sneaking past or disabling the alarms. The body responds, belatedly, with "an immuno-pathological response"—so much unregulated inflammation that it damages its own cells and organs. Doctors are seeing what are called "cytokine storms," surges of uncontrolled activity by the innate immune system, in the lungs but perhaps also in the liver and kidneys, the heart and the brain. "It's chaos," says Rasmussen. "Every cell is yelling these pro-inflammatory messages." If no one comes to hush the angry Rambo baby, and it keeps screaming and shooting, the damage can be widespread. "The innate immune system buys you time," says Neuman, "but it will also kill you if left to its own devices."

Some hospitals have begun taking plasma from people who have recovered from the virus and transfusing it into people who are still fighting it. This is meant to give a struggling immune system a breather, a chance to catch up. But the break is only temporary; plasma can't teach your body to actually beat the virus. It has to learn on its own. So for now, the outbreak is this: millions of infected people whose immune systems are running their own individual sprints, some of them desperate and dangerous, against an opponent trying to fill the course with potholes and trip wires. We've separated ourselves from each other in an attempt to keep our champions from ever getting on the track, so that most racers will at least have access to the doctors and nurses and medicines and ventilators that will give them the best chance of winning. But in the meantime, we're stuck. We can't relax our social distancing without sending more racers into a deadly arena.

Unless, that is, one of the candidate vaccines that researchers are developing is successful in giving our adaptive immune systems a major head start against the virus. Neuman described vaccines as a fitting rejoinder to a sneaky opponent, a way to re-bias the rules of the race in the other direction—tilting them, decisively, in our own favor. Crotty used the same metaphor but continued it a little differently. "That's the brilliant thing about a vaccination," he says. "You get rid of the race."

**The record for the** fastest path to a licensed vaccine, depending on how you clock it, is held by the mumps vaccine—developed in just four years in the 1960s—but the process is usually far slower. In February, years after an outbreak that caused more than 11,000 deaths, four African countries finally licensed an Ebola vaccine that had been in development since at least 2003. "The international response was too late," Norway's prime minister, Erna Solberg, said in 2017, as the vaccine inched forward. "But now we know how to respond faster the next time."

Solberg was announcing the formation of a new international organization with a goal of underwriting and coordinating accelerated development for vaccines when they were most needed, during outbreaks. The Coalition for Epidemic Preparedness Innovations, or CEPI, would focus on a short list of priority diseases. One was Middle East respiratory syndrome, or MERS, a disease caused by a coronavirus that emerged in Saudi Arabia in 2012. (It wasn't easily spread, but of those who got sick, about a third died.) The coalition would also start planning to respond to a theoretical disease, which the World Health Organization referred to as "Disease X." It was likely to emerge suddenly, just as MERS and its predecessor, a coronavirus that caused severe acute respiratory syndrome, had. And it might be deadlier or more easily transmissible. Disease X might belong to any number of virus families, says Melanie Saville, CEPI's director of vaccine development, but coronaviruses were "one of the ones that we thought was a prime candidate." Whatever it turned out to be, a deeply interconnected planet could find itself desperate for the fastest possible vaccine. "What happens in Lagos will affect Davos tomorrow," Jeremy Farrar, director of the Wellcome Trust in the UK, said when CEPI was announced. "The world is incredibly vulnerable."

Some of the slowest parts of the vaccine development process are the necessary rounds of safety and efficacy testing: Because vaccines are given to people who aren't already sick, their rewards must be proven to dramatically outweigh their risks. And clinical testing depends on waiting long enough for human bodies to reveal success or problems; for that part, Saville says, "there's no shortcut." So CEPI officials, as they began investigating other ways to speed things up, started investing in what they called "rapid-response platforms," new and experimental methods of vaccine development that they hoped could move to clinical trials in record time.

In the US, Barney Graham and John Mascola, leaders at the Vaccine Research Center, and their boss, Anthony Fauci, the director of the National Institute of Allergy and Infectious Diseases, were thinking along similar lines. In 2018 they wrote that traditional vaccine development methods, using whole viruses or even proteins, were hindered by their need to be uniquely designed to fit different viruses. Newer technologies, including those that used either DNA or messenger RNA to move through the body, could potentially work for multiple viruses, with only parts of their designs swapped out. With more research, these platforms might herald a new era of far quicker vaccine deployment. Since 2003, they noted, the institute had developed candidate DNA vaccines to target SARS, two influenza outbreaks, and Zika, and had seen the time it took to go from a sequence of a new virus to the first phase of human trials shorten from 20 months to just over three.

Rather than introduce killed or weakened viruses as the antigens to activate the immune system, DNA vaccines are meant to work by convincing the body to become its own antigen factory. The vaccine delivers a carefully designed DNA sequence, which enters a cell and instructs it to create a protein that imitates part of the virus. If all goes as planned, the body starts producing both an ersatz attacker and the defenses it needs to stop it. Crucially, if a new virus comes along, the same platform can be used to target a different antigen.

The institute was also working, in collaboration with Moderna, a relatively small biotech company based in Massachusetts, on a new vaccine to prevent MERS. This vaccine would essentially skip a step and directly inject messenger RNA encoded with the genetic blueprint that instructs a cell to build a version of the spike protein that MERS uses to penetrate cells. Like a DNA vaccine, this platform could be rapidly repurposed and redeployed, without waiting for a lab to modify and grow a bunch of viruses. (More traditional vaccines rely on cells grown in giant bioreactors; the machines that Moderna uses "look more like little beermaking kits," says Ray Jordan, Moderna's head of corporate affairs.) All that was needed to get started was a genetic sequence. And then, Jordan says, "instead of the bioreactor, you use the human body."



Saville says these mRNA vaccines are "an early but very promising platform." Still, there are lots of ways trial vaccines can fail; in the worst cases, they can actually make the immune response more unregulated, the disease's damage worse. With RNA vaccines, though, a common concern has been the opposite: There's no actual virus replicating in the body, which means that these vaccines are believed to be safe, but they might not trigger the complex chain of immune responses. Even if the vaccine works as planned, and the immune system creates antibodies that target the chosen antigen, those antibodies may not be sufficient to actually make the recipient immune. But the technology has been rapidly improving. Moderna's first crack at a Zika vaccine, for example, didn't create much of an immune response. A second try was at least 20 times more potent, according to an article in *Nature*.

By the winter of 2019, Moderna had eight mRNA vaccines, for a variety of viruses, in some stage of development: Six were in Phase 1 trials, which primarily test the safety, not the effectiveness, of a vaccine candidate, while one was just preparing to enter a Phase 2 efficacy trial. According to the company, all had shown some form of immune response—not proven effectiveness, yet, but signs that are correlated with it. Still, Moderna had not yet brought a single vaccine all the way through human trials and into the market. Nor had any other company created a DNA or mRNA vaccine of any kind that had been approved for use in humans. It was still a hope waiting to be verified.

**Late last December, fewer** than three months before Neal Browning and the three other first vaccine trial participants offered their arms for injection, Jason

**If no one comes to hush the angry Rambo baby, and it keeps screaming and shooting, the damage can be widespread.**

McLellan, who runs a molecular biosciences laboratory at the University of Texas at Austin, started hearing about a new respiratory pathogen that had just emerged in Wuhan, China. Given the symptoms, he wondered if it might be a coronavirus.

McLellan had done his postdoc at the Vaccine Research Center, working with Barney Graham. When he finished in 2013, shortly after the emergence of MERS, he talked to Graham about what he should do next. They agreed there was a family of viruses calling out for further study: "We thought it was clear that there would be additional coronavirus outbreaks."

McLellan started his own lab, which focused on understanding the protein structures of just two families of RNA viruses: *Pneumoviridae*, such as respiratory syncytial virus, which widely infects infants and children, and *Coronaviridae*, whose spike-shaped proteins are now infamous. The spike, his team found, operated similarly across all the coronaviruses they studied. The lab members began to create three-dimensional maps of the spikes, so detailed that they showed the location of each atom. (They used a technique called cryo-electron microscopy: essentially using liquid nitrogen to freeze molecules in place, and then using a bombardment of electrons to capture their structure.) They knew that blueprints of the structures that the adaptive immune system would have to learn to neutralize could be invaluable for future efforts to make vaccines.

But there was a complication: The spikes kept transforming. It was their nature. They needed to be one shape to bind to a cell and then another to enter it; once this fusion began, what started out looking like a mushroom changed—losing its cap, elongating, and twisting into something new. It might do little good for the immune system to learn to recognize this post-fusion structure, so McLellan's lab started researching ways to stabilize the protein, locking it into the shape that it actually used to break into cells. They mapped which parts of the structure changed and which didn't, and they found that they could use carefully engineered genetic mutations as if they were staples, locking down regions of the spike that wanted to move around by binding them to regions that did not.

In early January, McLellan was snowboarding with his family in Utah when he got a call from Graham. He was calling about the disease circulating in Wuhan: "It looks like this is a coronavirus," Graham said. "Are you ready to put everything together and race on this?"

"Yes," McLellan replied. "We're ready."

On January 10, one day before China announced its first death from the new disease—at that point it was known to have sickened just 41 people—a consortium of researchers published a draft sequence of the genome of the new virus. Labs across the world got to work. In Texas, it was Friday night, but McLellan and his team didn't wait. SARS-CoV-2 was a new version of a familiar problem; they could apply the stabilizing mutations they'd been developing right away. McLellan messaged Daniel Wrapp, a grad student, on WhatsApp. The next morning, Wrapp and Kizzmekia Corbett, the scientific lead of the Vaccine Research Center team that studies coronaviruses, got to work using mutations their colleague Nianshuang Wang had already identified. Within an hour or two, they had a genetic sequence for a stabilized version of the new virus's spike protein.



**As their MERS** collaboration continued, scientists at the Vaccine Research Center and Moderna had been exploring whether it would be possible, if a viral epidemic were to break out, to work together and use Moderna's mRNA platform to make a rapid vaccine. Within a day of getting the sequence of the new virus, they decided to try. In those early days, the outbreak was still widely expected to be contained. Rather than a world-changing pathogen, says Moderna's president, Stephen Hoge, the virus at first seemed like an interesting opportunity to test the potential of their collaboration and their technology.

The scientists adapted their previous work to target the specific spike of SARS-CoV-2. "Plug and play," Corbett calls it. First, they had to choose which protein to express. The teams considered whether to use the wild form of the new virus's spike protein or the stabilized, pre-fusion one, but they agreed that the latter was more likely to make the best antigen. ("The point of a vaccine is to do better than natural infection," Corbett would later explain on CNN. "The point of a vaccine is to create an immune response that is very potent, so, high-level immunity for an extended period of time.")

Then it was up to Moderna to decide how to encode that protein in mRNA—a problem with an overwhelming number of possible solutions, but one that the company had prepared for, by using machine learning to train algorithms to pick sequences best able to express a given protein. From those possibilities, they manually selected the most promising. (They also planned backups, in case their selection wasn't supported by new data, but the alternatives didn't prove necessary.) By January 13, the scientists had finalized the genetic sequence of a vaccine they called mRNA-1273, which would enter Neal Browning's arm two months later. The process was incredibly fast, says Jordan, but only if you ignored all the work that came before. "You're able to do this in a few weeks, but it's a few weeks plus 10 years."

Even with the head start, beginning the trials so quickly required a sprint. The news about the virus's spread, and its effects on those it infected, kept getting scarier. It was soon clear that more was riding on the vaccine than anyone had initially realized. Within two weeks, scientists at Moderna, without being asked, were staying late, working weekends. Corbett's team started growing spike proteins and stocking freezers

with vials. They immunized mice with the vaccine, then tested their blood for antibodies. A clinical batch was ready by February 7, tested and shipped by February 24, and green-lit for human testing by March 4. (It was a coincidence that the human trials began in what had, by March, become the first hot spot in the US; Kaiser Permanente Washington Health Research Institute had been selected to conduct them in late January.) There was never a singular moment, says Hoge, when he realized the researchers had begun an 18-month marathon. Instead, "it felt like every day, can you run faster, can you run faster, can you run faster?"

Even after trials began in record time, that remained a key question. Were there other ways to speed up development? Usually, a vaccine moves through phases sequentially, proving itself before its producers are willing to invest in the next step. By the end of January, CEPI selected mRNA-1273, along with three other vaccine candidates, for emergency funding, allowing the researchers to start preparing extra vaccine material for future phases of testing. In April the US government approved nearly half a billion dollars for Moderna from the Biomedical Advanced Research and Development Authority (Barda)—money that would allow for more staff, more equipment, and more space to produce large quantities of a vaccine that was still months from being proven (or disproven) to work. (Barda also supported other companies, including Johnson & Johnson and Sanofi.) Instead of the normal sequential process, Jordan says, Moderna was "shingling": preparing everything it could, as soon as it could, in the hope that all the work wouldn't turn out to be wasted. "This is not normal times," explained Hoge. The company is now preparing to produce a million doses a month by the end of this year, and tens of millions of doses a month in early 2021. All of a vaccine that has not yet entered an efficacy trial.

On the same day Neal Browning got his shot of Moderna's first-out-of-the-gate vaccine, another candidate from the company CanSino Biologics in China became the second SARS-CoV-2 vaccine to officially move into human trials. Within a few weeks, three other vaccines—two from Chinese labs and a DNA-based one pioneered by the Pennsylvania-based company Inovio—also got the green light. The list of projects for vaccines targeting SARS-CoV-2 expanded and expanded and then expanded some more; as of mid-April, the WHO listed 78 active efforts and 37 others for which statuses weren't public. CanSino announced that one of its vaccines was ready to move onto efficacy testing.

The candidates could be used to teach a course on the history of vaccine strategies—on the growing diversity of methods, on their different strengths and drawbacks, on our continued reliance, no matter what, on our own immune response. Including Moderna's and Inovio's, there were some 20 vaccines using nucleic acids, split almost evenly between RNA and DNA platforms. Some vaccines used the real virus, either attenuated or inactivated; some used viruslike particles, or recombinant protein, or peptides, or replicating or nonreplicating viral vectors. When asked which approach she found most promising, Rasmussen replies that it's still much too early to make more than a pure guess about which of the vaccines, if any of them, might be the one the world is waiting for. "I'm most interested," she says, "in the vaccine that works."

Still, the flowering of options reminded her of something. The growing list was a bit like a bunch of B cells, each floating around with a possible solution locked inside, each one part of a system that works simply by throwing answer after possible answer at a vexing new problem. In trying to help the ancient, adaptive defense system inside us prepare for a brand-new challenge, our scientific response had come to resemble it.

**On March 23, seven** days after his injection, Neal Browning returned to the office to have his blood drawn again: the first record of his immune system's "after" state, though it was likely still too soon for any antibodies his body might be creating to be detectable. (The researchers didn't expect to have results about immune response to share until late June.) In the waiting room, he saw the same brown-haired woman he'd noticed the week before. This time, they smiled and, from a safe distance, greeted each other. "You're Neal," she said. "You're Jennifer!" he answered—Jennifer Haller, the world's very first coronavirus vaccine recipient. Browning was the second. They recognized each other from being interviewed on TV.

Haller reported that she'd experienced no problems with the vaccine, and Browning agreed: "a feeling of underwhelming normalcy," he called it.

In a few weeks, they'd return for another injection—a booster to juice their immune systems. By then, to calibrate the body's response, two other cohorts of volunteers would have received their doses: injections of four and 10 times more vaccine that Haller and Browning received. The trial would have expanded to include volunteers considered both "older" and "elderly," the ones who would need a vaccine the most.

Later, there would be more volunteers, more trials. If everything perfectly followed the desperate hopes of a watching world, a vaccine might really be ready for widespread deployment 12 to 18 months after Anthony Fauci, standing next to the president, had proposed that record-setting timeline. Under emergency protocols, it might be ready for higher-risk groups, such as health care workers, even sooner.

But all that waited somewhere in the deeply uncertain future. For now, almost three weeks after getting his first shot, Browning sat on the deck behind his house, watching a parade of hummingbirds come and go from his feeders, their wings beating so fast he couldn't see them but still holding them aloft. He thought, yet again, about what his cells might be invisibly up to. There were a lot of possibilities. His B and T cells might be getting more efficient at fighting SARS-CoV-2 all the time; Crotty's research has shown that, after a month, new generations of immune cells might be 1,000 or even 10,000 times better at binding to a pathogen than they were on the day of the shot. Or, it was possible that even now, all that carefully constructed RNA could be degrading away, leaving behind no real sign that it had ever been introduced.

Browning continued to be an optimist. When he pictured his immune system, he imagined a cadre of his own personal armed guards, sentries out on patrol. Maybe their training against their newest adversary had gone exactly as the whole world hoped. "Maybe," he says, "my body saw it, and fought it off, and it's done."

---

**BROOKE JARVIS** *lives in Seattle. Her most recent feature for* WIRED*, in issue 28.04, was about the natural world and carbon sequestration.*

IN EARLY FEBRUARY, THE

*DIAMOND PRINCESS*

CAPTIVATED THE WORLD AS IT DOCKED IN YOKOHAMA, HARBORING THE NEW CORONAVIRUS.

HERE'S HOW THE 3,711 PEOPLE ON BOARD BECAME RELUCTANT SUBJECTS IN A LIFE-AND-DEATH QUARANTINE EXPERIMENT.

# 27 DAYS IN TOKYO_




BY LAUREN SMILEY


# -BAY

# *Before dawn*

on the 5th of February, Captain Gennaro Arma sipped espresso in his tidy office, wondering how bad the news would be. He wore a crisp black uniform with shiny brass buttons and lifted the tiny cup with fingers swathed in cheap latex gloves. The passengers on the *Diamond Princess* were mostly asleep, and Arma, not long awake himself, brooded over the possibilities. He hoped for a Return to Normal: He would thunder up the engines and glide the *Diamond* from its anchored stillness out in Tokyo Bay into the port of Yokohama. Passengers would trudge down the gangway, Samsonites rumbling, a little befuddled by their brush with calamity but on their way. Then there was That Other Option, less clear and more ominous. Hearing a knock—*there they are*—Arma strapped on a surgeon's mask, opened the door, and greeted two Japanese health officers who strode in, also wearing gloves and masks, ready to deliver the verdict.

Two weeks earlier, on January 20, Arma had sailed the *Diamond* southwest from Yokohama for a 14-day cruise to China, Vietnam, and Taiwan, then back to Japan. Three days into the voyage, news reports arrived that China had shut down all travel from and within Wuhan, an inland city of 11 million, in an attempt to squelch a new coronavirus. Then, in the predawn hours of February 2, Princess Cruises' vice president of maritime operations had awoken Arma with preliminary information that a passenger in his eighties who had left the ship in Hong Kong eight days earlier had since tested positive for the same virus. The captain was told to speed back early from Okinawa to Tokyo Bay, so that passengers and crew could be screened. Ferrying out


Emergency workers in protective gear exit the *Diamond Princess* on February 10. As the ship was parked at the port, supplies were brought in and sick passengers taken away to isolation on shore.

to meet the ship late on February 3, health workers boarded and spent that night and the next day walking cabin to cabin, asking if people were feverish or coughing, taking temperatures and swabbing throats.

Now the health officers were back with the first set of test results: The coronavirus hadn't disembarked with the elderly man in Hong Kong. Ten of the 31 results at that point were also positive. Nine passengers. One food worker.

While they spoke, the captain's thoughts went to the 2,666 passengers and 1,045 crew members. *Those 10 people probably had roommates. How far had it spread?*

Arma had spent more than 25 years at sea. Just five months earlier, in these same

Opener: Philip Fong/Getty Images; above: Carl Court/Getty Images

waters, he had faced his most arduous trial yet, white-knuckling the *Diamond*'s helm against Typhoon Faxai. He had held the bow straight into 100-mph winds, lest they catch the cruise liner's massive flank and fling it around like a toy boat in a Jacuzzi. He accepted the sea's hierarchy—"You can't beat Mother Nature, but you can come to a compromise"—so all night he negotiated, gunning the engines and thrusters to keep the 115,875-ton behemoth in place, the nautical version of running on a treadmill. You didn't hear about a Princess cruise ship slamming into a cargo vessel or capsizing last September, because he succeeded.

"We got through Faxai. We'll get through this," a staff captain told Arma upon hearing of the virus aboard the ship. Arma preferred Faxai. This new coronavirus wasn't something he knew how to navigate.

The legal authority for the ship's safety had shifted to the Japanese government. Those officials, in turn, had pondered a real-life version of the trolley problem: The ship was carrying 3,711 people, any one of whom could be harboring a potentially fatal disease to which no one had immunity. No option was good. A ham-handed disembarkation risked unleashing the virus within Japan, which at that point had only 20 known cases and was hosting the Summer Olympics in just five months' time. Send passengers to their home countries without ensuring they were healthy and Japan would be blamed for spreading the contagion. Yet the last choice—a quarantine, albeit in a glamorous prison—presented a danger, even an inevitability, of sickening many on board. And given that 60 percent of the cruisegoers were 60 years or older, with weaker immune systems, an infection could mean death.

That morning, the Japanese health officials delivered the government's decision. For all his nautical prowess and romantic seafarer bearing, Arma is also a polished company man. Accepting his role as a high-ranking messenger, he fired up the shipwide intercom at 8:12 that morning and announced in steady Italian-accented English:

*The Ministry of Health has notified us that 10 people have tested positive for coronavirus ...*

*The local public health official has requested all guests stay in their stateroom ... It has been confirmed that the ship will remain under quarantine in Yokohama.*

*The length of quarantine will be at least 14 days ...*

No one knew at that point how much damage the virus had already caused. For days, as passengers played bingo and drank mai tais in the Skywalker Lounge, it had invisibly hopscotched from one person to another. Now the ship would become the first big outbreak outside the Chinese epicenter and a mutating symbol: at first, a Fyre Festival–like joke, its buffed banisters, restaurants, casinos, and dance floors converted into beguiling on-ramps for infection. Over time, though, the luxury ship proved to be a microcosm of the world's battle with the novel coronavirus: the laggard response, the upstairs-downstairs inequality, the limitations of privilege against a pandemic, and how global interconnection allowed the virus to take over. By the time its crisis concluded, the *Diamond* would be less punch line than premonition.

.
.
.

**ARNOLD HOPLAND REACHED** for his cabin phone after hearing Arma's announcement. Hopland had people to call, but he hadn't sprung for the personal Verizon international plan, because, as he puts it, "I'm cheap." That's also the reason he and his wife, Jeanie, had opted for a cabin on Deck 5 on a ship that rose to 18. Hopland could have chosen a stateroom with a balcony and a soaring view; he'd done well for himself as a doctor and semiretired founder of three family practice clinics near Johnson

ARNOLD HOPLAND WENT INTO SHIN-KICKING MODE: UNTESTED, ASYMPTOMATIC CRUISE PASSENGERS MIGHT BOARD COMMERCIAL FLIGHTS AT THE END OF THIS COCKAMAMIE QUARANTINE, POTENTIAL TYPHOID MARYS IN THE SKIES.

*Additional reporting by Sherbien Dacalanio.*

City, Tennessee. But, he concluded, his cheap streak was for the best. "It was an absurd plan" to coop contagious humans on a ship, but at least he and Jeanie were sealed in their room, squeezing by each other between the flatscreen TV and two pushed-together twin beds. People in the more expensive quarters above were chatting on their balconies over thin dividers—as if that were safe to do.

The quarantine came as a shock to Hopland. He hadn't heard Arma's shipwide dispatch on the night of February 3, announcing that a passenger who had left the ship had tested positive for the coronavirus six days after disembarking. He'd caught something about a health inspection, which would delay the cruise's end, but dismissed it as a kitchen issue. Nothing on the ship tipped him off to the gravity of the impending emergency.

While Princess executives on two continents exchanged texts and calls about the infected passenger and flew to Tokyo to set up an incident command, on board the ship, a normal day's schedule with a Zumba class and Dance the Night Away party was handed out. Passengers only noticed small tweaks: A staffer seemed to be more serious about enforcing use of a hand-washing station at the buffet. The MC of a trivia match in the Explorers Lounge told players to pocket their pencils instead of handing them back. The crew sprayed disinfectant on surfaces and set out more hand sanitizer, but passengers said they didn't see out-of-the-ordinary efforts. On February 4, Arnold and Jeanie killed time playing Scrabble outside, never thinking trouble was coming for them while passengers were told over the PA to return to their cabins for screenings in shifts. Now they were on a floating petri dish.

Arma had docked the *Diamond* by the pier of Yokohama for the quarantine. Several times a day, the captain's luxuriant voice would fill the Hoplands' cabin to announce, like a bingo match of doom, the growing number of people who had tested positive for the new coronavirus: 10 infections the first day. Another 10 the next. Forty-one more the day after that. Then 66 three days later. During organized fresh air breaks, Hopland got a view of a brigade of ambulances parked in rows on the vast plain of the pier, as if on the side of a battlefield, ready to transfer those who tested positive to isolation rooms ashore. Hopland watched one ambulance take 45 minutes to load one person, concluding, "We're going to be here until June."

Up on Deck 10, a 57-year-old lawyer from Sacramento named Matt Smith had a balcony seat for the dockside action. He logged into his mostly dormant Twitter account—some 13 followers and a bio ("I'm too old for this s***")—and started posting photos: A crane lifting fresh linen on board. A phalanx of reporters lined up with cameras on tripods. One he captioned, "Frustrating to see a group of hazmat astronauts huddled around an ambulance … and have no way of finding out what's going on." Perusing the news online, Smith was amused to spot a picture of his wife, Katherine Codekas, standing forlornly on their balcony in her robe.

The World Health Organization wouldn't release a preliminary cruise ship protocol for handling the Covid-19 outbreak until two and a half weeks after the *Diamond*'s quarantine started; when it did, it recommended isolating people with suspected cases and then, as quickly as possible, getting them to an onshore facility for testing. In the meanwhile, the Japanese government had invoked a cordon sanitaire, a blunt-force disease control method dating to the 1500s in which authorities force everyone—infected, healthy, immune—to stay inside an area of suspected outbreak. China had used this method to lock down the city of Wuhan.

Precise protocols for contagions have been developed over time to care for the sick and prevent health care workers from contracting disease. Even in trying settings, like the plastic tents used during the Ebola outbreak, patients can be held in a "red zone," where medical personnel are clad in protective gear, which they shed in a "yellow zone," before stepping into the "green zone" free of contagion. On the *Diamond*, infection control experts trained medical staff on using protective gear, which they shed in a designated area apart from other working areas, the health ministry said; still, one Japanese expert boarding late in the quarantine publicly denounced what he viewed as "completely chaotic" and lax controls.

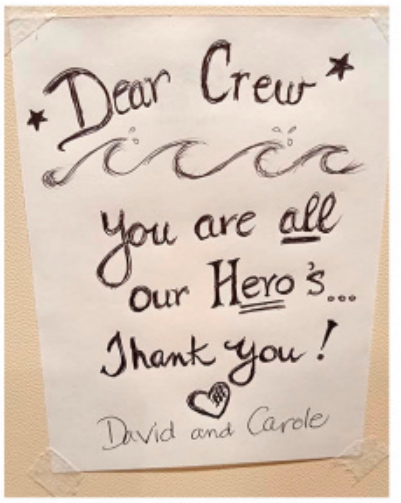
"In theory, a quarantine could be done" on a ship, says Arthur Reingold, a professor of epidemiology at UC Berkeley. "But in practice, I suspect it would be extraordinarily difficult." Without universal testing for sorting the infected from the healthy, he says, each person would need to be isolated in their own cabin—a virtual impossibility on a ship—and do an "exceptionally good job of preventing exposure to the crew, or the crew to each other."

Early on, the Japanese authorities suggested the US evacuate American cruisegoers, who made up the second largest passenger contingent after Japanese, according to state broadcaster NHK. But at the time, the US Centers for Disease Control and Prevention decided that keeping people inside their cabins was the "best approach" to limit spreading infection.

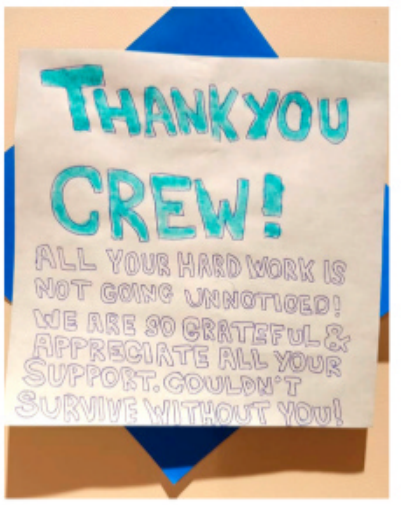
On board the *Diamond*, the crew, untested for the virus, delivered food, towels, and Amazon orders and picked up dirty dishes while walking through various floors of the ship, where untested passengers shared rooms with their travel partners. Japanese authorities handed out digital thermometers to everyone during the third day of the quarantine. Captain Arma urged passengers to take their own temperatures throughout the day; if it registered over 99.5 degrees Fahrenheit, they were to call the onboard fever center, and only then would they be tested for the new coronavirus. Such a system allowed asymptomatic virus carriers—which turned out to be about half of the *Diamond*'s cases—to unwittingly spread disease.

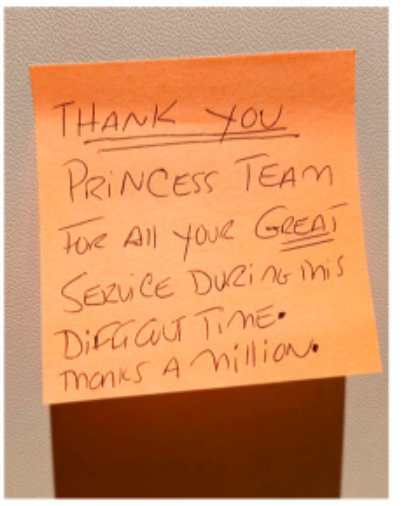
Princess Cruises, owned by the mega cruise company Carnival Corporation, hired crisis communications consultants to massage the optics of its ship paralyzed by a virus outbreak. The company wasn't happy with the onboard quarantine, says Ryan Mikolasik, one of the crisis consultants. "It quickly became obvious that this situation was not tenable," he says. At a meeting with about 15 Japanese officials at Carnival's Tokyo office, company representatives discussed isolating the passengers onshore. Officials told them there weren't 3,700 hospital rooms available. *Hotels?* Well, they would need 10. *The Olympic Village?* Not finished yet. (The government says it would have been preferable to isolate people on land, but that the difficulty finding accommodations for Japanese evacuees from Wuhan contributed to the decision to quarantine on the ship.)

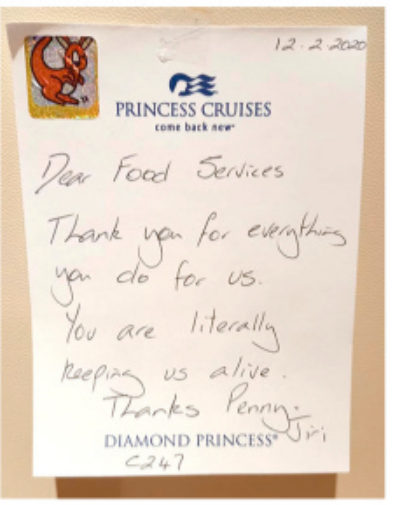
Several times a day, Captain Arma became

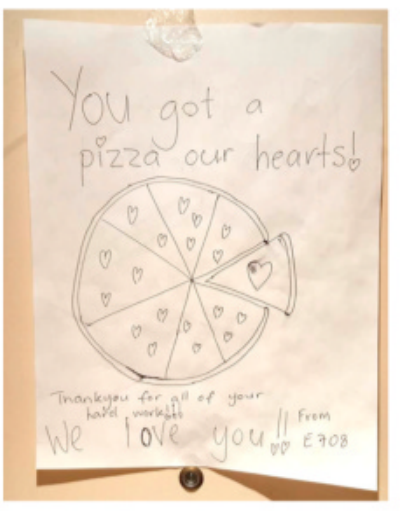




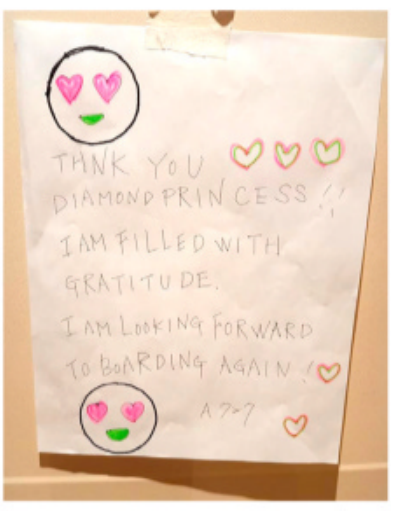








▲

**PASSENGERS TAPED THANK-YOU NOTES TO THE CREW ON THE OUTSIDE OF THEIR CABIN DOORS.**

"TV NEWS, SOCIAL MEDIA, WHATSAPP, ALL CORONAVIRUS! WE WERE GETTING SCARED, SCARED, SCARED," ONE CREW MEMBER SAID. "LIKE, WHY ARE THEY TRAPPING US IN THE SHIP?"

the voice of incoming decisions, piping through the PA system with lengthy updates: Prescription refills would be delivered as soon as possible. Passengers would now receive supplies to clean their own cabins, as the housekeepers could no longer enter. He added assurances—"A diamond is just a rock that did well under pressure"—and explained how to call the ship's help line, on which he sometimes spoke to passengers himself.

Hopland was not placated. Seventy-five but "physiologically in my fifties," he says, with a full head of white hair, Hopland wasn't worried for his own health. But pandemic preparedness had been his pet issue for decades. As a clinician, he proselytized for flu shots, advertised by a gigantic blow-up pink elephant named Fluzie in his clinics' parking lots. He would recount tales of the 1918 Spanish flu to Jeanie and fret that the country was woefully underprepared for the next outbreak. He'd even sent the Obama administration a letter urging it to prepare and offering his services as surgeon general. (He got a polite brush-off.)

When, on February 8, the CDC advised the US passengers aboard the *Diamond* to stay in their cabins, Hopland went into shin-kicking mode. He wanted US residents taken off the ship and tested. He was infuriated by the idea that untested, asymptomatic cruise passengers might board commercial planes at the end of this cockamamie quarantine, potential Typhoid Marys in the skies. He was convinced he had a smarter plan, and the connections to pull it off.

.
.
.

**DOWN ON DECK 4,** the first with windows, Alex sat in the crew cafeteria watching the news on TV. Onscreen he saw images of the ship he was inside. As soon as he heard about the outbreak of the new coronavirus on the *Diamond*, Alex started Googling. He read about social distancing and was eating apart from other workers who were sitting side by side at long tables. At one point he stood up to look out a porthole and saw boats gliding by, news cameras pointed his way. A security officer demanded that crew members shut the windows, Alex says, cutting off the view.

Alex isn't his real name, but unlike the passengers freely tweeting and appearing on TV, he was wary about discussing his experiences on the ship. The crew was barred from speaking to the media without approval, and although he said he was not telling me "anything wrong ... it's the truth," he asked to be identified only as "Asian hotel staff," for fear of being blacklisted for future jobs. On cruises, he says, the crew work "like machines" on temporary contracts. But it was a good job for a guy who had grown up, he told me, in a slum that "sounds ugly and is ugly." The gig came with free room and board and about $900 a month, enough for him to help family members and save up so that, one day, he and his wife could move into their own place.

On board, Alex noticed that, among the crew, the navigation team tended to come from Western countries. Their cabins were on higher decks. Some officers were allowed to eat in the passenger dining rooms and run on treadmills in the passenger gym. Housekeeping and food workers largely came from the Philippines, India, and Indonesia and most slept below the waterline in cramped cabins with roommates.

Throughout the quarantine, workers were required to cook and deliver food and linens to cabin-bound passengers, increasing their own chances of exposure. "So many people said that's wrong," Alex says. As workers commiserated, the shared language of English splintered into Tagalog, Hindi, and Indonesian. Alex and his immediate coworkers contemplated a work stoppage, but they feared that taking action would mean they'd never be hired again. The Princess contract states that in emergencies workers must show "immediate unquestioning obedience of orders; There can be no exception to this rule." In this case, Princess was also obeying the Japanese Ministry of Health, Labour, and Welfare, which had authority to say when everyone got to leave. "So we're not going to go against them," Alex says.

The health ministry distributed face masks and latex gloves to the crew. Letters signed "Yours in Health" from Princess' chief medical officer, Grant Tarling, at the corporate headquarters in Santa Clarita, California, were delivered to the crew's cabins. One read: "What is happening is unprecedented, but it is allowing health experts to learn about the virus and how it spreads. This will help all of you onboard, as well as people around world."

In short: guinea pigs. Because not everyone had been tested, Alex had no idea if his coworkers—or his sneezing roommate in their 6- by 9-foot cabin, or the other crew with whom they shared a bathroom—carried the virus. "TV news, social media, WhatsApp, all coronavirus! We were getting scared, scared, scared," he says. "Like, why are they trapping us in the ship?" More postings went up in crew quarters and were delivered to cabins: numbers for a counseling line, reminders to wash their hands frequently, recommendations for self-care apps. But crew members were still working next to each other, albeit in masks and latex gloves, chopping onions, stuffing dirty sheets into washers, scrubbing the passengers' grubby plates until the ship changed to disposable ones. A CDC study would later reveal that 15 of 20 workers who tested positive in the first week worked in food preparation, and 16 of them lived on the same deck. A Filipina cook who lived on that deck feared she would die. "Who would take care of my kids?"

Like the passengers, crew members were given thermometers and told to self-report fevers. Those with symptoms awaiting test results, or who had roommates who'd tested positive and been whisked away, were told to stay in their cabins and self-isolate. "That was pathetic," Alex says. Those people still had cabin- and bathroom-mates.

Then, on February 11, Japanese health workers rolled out a more comprehensive testing plan. First the passengers would be tested, starting with the oldest and working down. After all the passengers were tested, the crew without symptoms would get their turn. Meanwhile, there were a few half-hearted attempts at social distancing for the crew. Some chairs in the cafeteria were removed, and the ship's staff was told to keep a chair's space from the next person at meals. Eventually, they ate in smaller groups in shifts.

For the first few days of quarantine, Captain Arma had made separate announcements to the passengers and crew. But now he started broadcasting to the entire ship at once. "That was probably good for everyone, like a wake-up call," he explains, "to say yes, the crew is here to support and assist you, but we're all sharing the same problem." He called for them to stay "strong and united" against a common foe, "literally in the same boat."

Arma looks like a sea-weathered Patrick Dempsey, with blue eyes and hair that's graying at the temples. A carpenter's son, he grew up on Italy's Sorrento peninsula steeped in the region's seafaring lore and his mom's devotion to *Love Boat*. He enrolled in a nautical vocational school and then started "from the very bottom" as a deck boy on a chemical tanker, scrubbing dishes through a winter on the Baltic Sea. He worked as a senior officer on the *Diamond Princess*' maiden voyage from the Nagasaki shipyard in 2004 and returned as its charismatic 43-year-old captain in 2018.

That Baltic winter gave him perspective to appreciate his privileges and the experience to cajole his crew, whose duty he says was to continue serving the passengers. He had taken to calling them "my gladiators" in his PA announcements, which rallied even Alex. "This captain was beautiful," he says. "We could have stopped working, but we did not, because of the encouragement and those gladiator speeches."

On February 10, Arma announced 66 new cases of Covid-19, bringing the total to 136. This raised alarm among experts in the US. The next day, Eva Lee, an infectious disease specialist at the Georgia Institute of Technology, sent an email to health experts and government officials who were tracking the virus's spread. She called the *Diamond* a "quarantine nightmare with missing opportunities and missteps," especially with regard to testing. "The spread—no doubt—involves those without symptoms," she wrote; she was eager for Japanese authorities to test everyone on board. (The high-level email chain, obtained through a Freedom of Information Act request, was published in *The New York Times*.) Dr. Carter Mecher, an adviser at the Department of Veterans Affairs, called the 136 cases on the *Diamond* "unbelievable" and bemoaned the US lack of preparation: "We are so far behind the curve." (It would be 39 days before California became the first state to implement social distancing measures.)

The *Diamond*'s crew was starting to lose its composure. A crew member flung his ship access card from a deck onto the pier below in what the company called "an act of rebellion." A group of workers from India posted a video to Facebook pleading for Prime Minister Narendra Modi to evacuate them: "Please save us from this swamp." Three days later, a 24-year-old security officer named Sonali Thakkar appeared on CNN, saying she had a cough and fever and had been isolated but not tested; a Japanese vice minister of health conceded to the network that treatment between passengers and crew "is not all equal." The Filipina cook admired the Indian crew members for speaking out: "They have balls, unlike us. We are silenced by our fears of losing our jobs."

Trying to lighten things up, a Filipino galley crew, wearing face masks and kitchen uniforms, choreographed a group dance to Justin Bieber's "Yummy." Another cook named Mae Fantillo posted the video on Twitter with a buoyant message: "We all know that we're facing a crisis here … but hey we still managed to smile, laugh and dance." Company brass and other Princess ships wished the crew well in videos with the rallying cry #HangInThereDiamondPrincess. And there was something else giving hope to the shipbound: February 19, the day the quarantine would end. Crew members filled Facebook posts with the countdown: "We're halfway there!!! 7 days to go!"

After hours of conference calls and meetings, Arma would end each day in his solitary suite on Deck 12, with an expansive view off the bow. There, he would Skype with his wife on the Sorrento coast and pray to a picture of Madonna del Lauro, the patroness of seafarers. Looking out his window, he, too, fantasized about escape. To him, that meant steering the *Diamond Princess* from this stagnant port to the open sea.

.
.
.

**AT THE OUTSET** of week two, a punch-drunk tedium sank in among the passengers. Matt Smith listened behind his door for the rumble of the coffee cart each morning, ready to pounce. Someone unfurled a "Trump 2020" sign from their balcony for the TV cameras. Servers cheerily called "Bon appétit!" as they pushed the food down the hallway, one wearing a shark head hat for laughs. Dozens of passengers taped thank-

you notes to the crew on the outside of their cabin doors. "You're literally keeping us alive," one wrote. When Covid-negative medically vulnerable people were given the choice to move to an isolation facility onshore, more than 80 percent chose the devil they knew, staying on the *Diamond*.

Smith tweeted meal reviews to his followers, now up to a robust 14,000. "The beef was tender and well-seasoned." "Who doesn't like cake?" Arnold Hopland relished the fresh air breaks on an astroturfed deck, springing from his cabin like a terrier from a cage. He'd pump medical workers for details on how the quarantine was being run.

One day, Jeanie Hopland opened the cabin door to find that a new steward had replaced the Ukrainian who'd been bringing them fresh sheets and towels. "What happened?" Jeanie asked.

*He got sick.*

This got Arnold spun up all over again. After a week of wrangling to get his Verizon international plan rolling, Hopland started dialing reporters, convinced the virus was still actively being spread despite quarantine. On February 12 he finally reached the person he'd been trying to get ahold of since day one: an old doctor friend from Tennessee named Phil Roe, who also happened to be a member of Congress.

Hopland told Roe about the conditions on the ship, and Roe immediately saw the risk that the virus could still be spreading. Within hours, Hopland found himself on a conference call with "the top of the food chain," he says. On the call were Roe and Robert Kadlec, the assistant secretary for preparedness and response at the Department of Health and Human Services, and medical experts from the CDC and the National Institutes of Health. "It was a bunch of nerdy doctors like us talking," Roe says. "To have eyes on the ground was extremely helpful." Hopland lambasted the quarantine: the lack of testing, the honor system for reporting symptoms, the hospitality workers' thin gloves and surgeon's masks. He urged them to bring passengers back to the States for a legitimate isolation, as had been done for Americans in Wuhan earlier that month. Roe says he and Kadlec agreed: "I said, listen, we're the best in the world at evacuating people." Yet other voices on the line, Roe says, worried about the risk of bringing Covid-exposed people to the US, which had only 14 domestic cases at the time. They suggested the Japanese had the situation under control, a contention Hopland angrily countered. (Roe calls it a "robust discussion.") Jeanie patted her husband's head and told him to calm down.

The next day, February 13, a letter signed by Roe and eight other members of Congress was sent to three cabinet secretaries warning of "deteriorating conditions" on the ship. They urged that the 428 US citizens and permanent residents be tested, and those who tested negative be evacuated by air to US soil.



A passenger peers out of a bus evacuating people from the *Diamond* on February 20. Americans were the first to be taken off the ship.

Eugene Hoshiko/AP

.
.
.

**ALEX AWOKE WITH** a start. His body felt like a stove. He poked his thermometer under his armpit: still a normal 37.5 Celsius. Was it broken? He'd been unable to sleep for more than two hours at a time. His insomnia, like any new tic or sneeze, felt suspect. He visited the makeshift medical center on board, asking if his thermometer was broken. It worked fine, he says they told him.

On February 13, a total of 218 people on board the *Diamond* had tested positive for the coronavirus, and the WHO declared the ship the largest Covid cluster outside of Wuhan. Infections were cresting for crew members, while the case numbers among passengers had begun to ease. The company sent hand sanitizer, vitamins, bottled water, Cup Noodles, and chips to the crew. But Alex wanted the same thing Hopland did: to be taken off the ship and tested for Covid-19.

The Japanese Ministry of Health had distributed temporary iPhones to passengers and crew, preinstalled with an app for free calls along with a list of numbers to get medications, medical appointments, and counseling. Alex used the phone to contact a Japanese doctor onshore. In a video call, he confided his surging anxiety. Was insomnia a sign of the virus? What should he do? He says the doctor told him that he wasn't sick and just needed sunlight and air.

.
.
.

**AN EMAIL FROM** the US embassy in Japan appeared in the American passengers' inboxes on the afternoon of Saturday, February 15. The government was recommending that citizens come home, "out of an abundance of caution." Most *Diamond* passengers had been getting tested to determine their fate at the quarantine's end, and only those Americans who did not have Covid-19 could take charter flights to the US the following night. When they arrived, they would have to spend another 14 days in isolation. Anyone rejecting the evacuation could stay in Japan on their own dime after the ship's quarantine ended, until they were cleared by the CDC to fly home. Everyone needed to decide by 10 am the next morning.

Arnold Hopland rejoiced. His advocacy had worked. Matt Smith and his wife, Katherine, however, imagined a flight in close quarters with people whose Covid status was hazy. Even a negative test was just a snapshot of the moment the swab was taken. Most important, just four days stood between them and freedom in Tokyo. Going home guaranteed more isolation. Smith had read about Hopland's efforts in a Politico article and tweeted about them: Was this "rescue"—in scare quotes—"an honest humanitarian effort or political cronyism?"

Hopland packed his bags, unmoved by Smith's taunting. That Sunday, he and Jeanie waited for the call to board chartered buses, snapping a victorious selfie in the mirror. When the knock came, they stood up for their departure. They were greeted by a health worker who said Jeanie couldn't leave: She had tested positive for the virus. She felt fine, but Jeanie was headed for a Tokyo hospital isolation room. Hopland picked up Jeanie's phone and downloaded the Life360 tracking app so that he could see where she would be taken.

More than 300 Americans trundled out of their suites and onto charter buses, heading for the evacuation flights. Smith, one of 61 who stayed on the ship, recorded the moment from his balcony, drolly tweeting, "the Departure of the Americans."

En route to the airport, news reached US authorities in Japan handling the evacuation that not everyone who had newly tested positive had been culled from the group as Jeanie had: 14 people were sitting on the bus with Covid-19 at that very moment. For hours, as the buses sat parked on the airport tarmac, the CDC argued to the State Department that the Covid-positive travelers shouldn't be allowed on the flights, but, according to *The Washington Post*, the State Department pushed back. And won. Everyone ambled onto the Boeing 747 cargo planes. The Covid-positive group was seated in an area enclosed with hanging tarps. At least one passenger started feeling feverish on the flight and was moved into the sick warren midflight.

Arnold Hopland, who had pressed for the flights, stayed in Japan to be near his wife. Jeanie's infection deemed him a "close contact," so his quarantine clock would be reset. Ferried to a dorm room at an accounting college, he passed the hours talking to reporters via FaceTime and cold-calling other bored ship alumni also isolated in the dorms on the landline, hoping to reach someone who could chat in English.

.
.
.

**AROUND THE TIME** that US citizens were evacuated, Captain Arma got more news from the Japanese Ministry of Health. He braced himself to relay the message to the crew. Starting in four days, the rest of the passengers would disembark, but the workers would have to remain on board for another 14 days. Because they had worked and roamed the ship during the passenger quarantine, they'd continued to be exposed and needed a formal isolation period themselves.

So much for everyone being in the same boat. "That was the lowest moment for us," Alex says.

As scores of passengers from Hong Kong, Australia, and Canada filed onto evacuation flights, at least one person wanted to get onto the *Diamond Princess*: a punctilious infectious disease specialist named Kentaro Iwata. He had been involved in the response to Ebola in Sierra Leone and had been a clinician during the SARS outbreak in China, and he was alarmed by the growing number of coronavirus cases in his own country's port.

After much bureaucratic jockeying, Iwata was cleared to go on board the ship on February 18, a day before the passenger quarantine was to end. By that time, 531 passengers had tested positive for Covid-19 and most had been moved to an onshore hospital. He made his way to the dining room that had been repurposed as the medical staging area and saw what he thought looked like a perfect stew for viral spread. Crew, officers, and medical workers walked around freely. Some were eating lunch and using phones with gloves on. No enforced green and red zones. One medical officer told him she was probably infected by now, so she was giving up on protective gear. (Three Japanese responders contracted Covid-19.)

After leaving the ship, he checked into a hotel room to stay isolated. Once there, he filmed videos in Japanese and English and posted them to YouTube. Iwata, a middle-aged man wearing a zip-up yellow sweater, spoke to the camera with barely suppressed anger, precisely describing the "completely inadequate" infection control he'd seen. "I

cannot bear with it," he said in one video. "We have to help people inside the ship."

More than a million people watched Iwata's whistle-blowing video. The system wasn't perfect, the health ministry said. Still, it was too late to make much of a difference. Medical experts were calling the Japanese response a disaster. People who had finally been evacuated from the ship continued to test positive for Covid-19. On February 20 came another somber milestone: Two Japanese passengers in their eighties died, the *Diamond*'s first fatalities, but not its last.

The widow of one Japanese victim told a television interviewer how she and her husband had sailed on the *Diamond* to celebrate their wedding anniversary. She couldn't enter his hospital room to say goodbye. "The nurse took his hand and put it up to the window and I placed mine on the other side. That was the end."

Back in the US, experts were emailing about the quarantine's failure. The *Diamond*, wrote Lee of Georgia Tech, showed that timeliness was everything. "A delayed intervention," she wrote, "cannot reverse the course and can be catastrophic."

.
.
.

**TWO DAYS AFTER** Iwata boarded, Smith and Codekas finally stepped off the *Diamond*'s gangway. They checked into a Tokyo hotel, where the manager asked them not to tell anyone where they were staying. That night, Smith tweeted a photo of their celebratory martinis.

As the number of passengers on board dwindled, desperation grew among crew members. Ten Indonesian workers released a video to a news network pleading for an evacuation, as the group of Indian staffers had done 10 days earlier. "Dear Mr. President Jokowi, we are on the *Diamond Princess* in Yokohama, and we're afraid that we're being killed slowly," they wrote. Fantillo, the cook who'd posted the cheery dance video days earlier, tweeted an urgent note:

*Each day, the gravity of the situation only gets worse ... We dont know where the virus really is. But we know, its all over. With all due respect to our company, we appreciate all the effort keeping us high in hopes. But right now, all we need is to... get all the external support needed. #PhilEmbassy #PlsSendUsHome #WeAlsoWantToLiveLonger #WeAlsoNeedToBeProtected #WeAlsoHaveFamilies #OneWithDiamondCrew.*

.
.
.

**ON FEBRUARY 24,** at the Ministry of Foreign Affairs in downtown Tokyo, three Japanese infectious disease experts sat before rows of journalists. The press conference was conducted in English, and one reporter asked, if all other countries were isolating the *Diamond* evacuees, "what was the point of the quarantine on the ship except to waste two weeks in the lives of those people? Very simply put: What did the quarantine achieve?"

Omi Shigeru, the distinguished president of the Japan Community Health Care Organization, responded by referencing data. Much of the spread among passengers had happened before the infection was discovered, and certainly before the quarantine began on February 5. Passengers had mixed on board "for social enjoyment, movie watching, dining, dancing, sometimes they are drunk ... I admit the isolation policy was not perfect. A ship is a ship. A ship is not a hospital. Though isolation was somewhat effective, it was not perfect."

The mea culpas and rationalizations continued for more than an hour: Getting 4,000 people into hospitals or hotels immediately is very difficult. The crew had to keep working, and we're grateful. It was a tough decision. History will be the judge.

Some preliminary judgments came quickly. Calculations from Japanese and US researchers concluded that the quarantine, for all its flaws, had staved off a second ballooning of the virus among passengers. But a study from Swedish, British, and Ger-

"WHAT WAS THE POINT OF THE QUARANTINE ON THE SHIP EXCEPT TO WASTE TWO WEEKS IN THE LIVES OF THOSE PEOPLE? VERY SIMPLY PUT: WHAT DID THE QUARANTINE ACHIEVE?"

man researchers concluded that if everyone had been let off on February 3 and properly taken care of, only 2 percent of them—or 76 people, instead of 712—would have been infected.

A few days before the press conference, the health ministry had changed course and allowed workers to disembark. Before they could leave, the galley staff was told to sanitize the kitchen with chlorine, the Filipina cook says, though the large-scale disinfection of the ship would be done by a biohazard contractor once everyone left. Chartered flights shepherded hundreds of workers and a smattering of passengers home—445 to the Philippines, 113 to India, and, lastly, on March 1, 69 Indonesians walked off the ship.

Watching them go, Captain Arma realized the moment he'd been dreading had come. He paused before the bank of navigation panels. "Despite the fact that they are a giant piece of metal," Arma told me, "every ship has a soul. And there has been a special connection between me and the *Diamond*." They'd faced a typhoon and a disease outbreak watched around the world. He thanked the ship for pushing him, for working with him, for sparing him any mechanical breakdown that would have made a bad situation worse. Before leaving, he powered up the PA for a final salute to the empty decks: "Good night, *Diamond Princess*."

.
.
.

**THE *DIAMOND PRINCESS*** was the cruise industry's patient zero. Throughout the spring, new Covid-infested ships kept beaching in ports, more than 20 gleaming fail whales of public health. After a Californian who'd disembarked from the *Grand Princess* in San Francisco tested positive for Covid-19 and died, US authorities forced the ship to anchor off the coast of California for several days while passengers stayed in their cabins and crew brought food to their doors. Carnival and health officials had learned some things: Once the ship was allowed to dock in Oakland on March 9, the passengers disembarked and were shuttled straight into isolation. Princess paid for repatriation flights for hundreds of workers. Yet for the next month, 614 crew members remained on the ship while it was parked in San Francisco Bay, most undergoing an on-ship quarantine. A Filipino crew member who had contracted Covid-19 was evacuated but died in a San Francisco hospital. And one day before the CDC demanded it, Carnival Corporation canceled all cruises for the spring.

When the order came to halt cruises, many were already underway. The industry plowed ahead with missteps. The *Ruby Princess* and Australian border agents let 2,700 untested passengers disembark in Sydney on March 19, and the ship was linked to more than 600 infections and at least 21 deaths in Australia. In early April, Australian police, alleging that Carnival had informed local authorities that Covid-19 wasn't an issue on the ship, launched a criminal investigation. Crew members of a Celebrity Cruises ship sued Royal Caribbean, the parent company, for failing to protect them from Covid. A growing number of Carnival passengers did the same, filing suit for negligence in allowing cruises to continue after the *Diamond* debacle. (Princess says it is cooperating with Australian authorities and that it does not comment on pending litigation.)

The *Diamond* didn't beat Mother Nature. Of the 712 people infected on board, 14 passengers died. Jeanie Hopland stayed in a Tokyo hospital room with three other *Diamond Princess* alumni for two weeks before being cleared to go home. Arnold, holed up in the college dorms, finally arrived at the Knoxville, Tennessee, airport a week after Jeanie got there.

Princess refunded everyone's cruise expenses and offered each passenger a free cruise in the future. Hopland plans to take them up on it. He has no beef with the crew. "Trying to contain a quarantine is a tough medical problem, and they had no expertise and a facility not designed for it. They were given an impossible assignment." Smith, once cleared to fly back to Sacramento, continued tweeting his meals and his general skepticism of coronavirus shutdowns.

After his isolation onshore in Japan, Captain Arma flew back to Rome. On the ride to his coastal town of Sant'Agnello, Arma asked the driver to make a stop at the crisp white Basilica Pontificia Santa Maria del Lauro. It was after 11 pm, and Arma faced the door to pray for the sick still in Japan and for his own country, besieged by the same virus.

In April, I talked to Arma on the phone with two Princess crisis consultants listening in. How would the *Diamond* be remembered? I asked. Arma, both a company man and a romantic, returned to his favorite metaphor. "A diamond is a chunk of coal that did well under pressure," he responded. "I would like to think we'll be remembered as one big family that, under some very challenging times, remained united with sacrifice and went through these problems."

Some of his team, at least publicly, expressed the same conclusion. Back in their home countries, crew members stuck #PrincessProud logos over their Facebook profile pictures and #Gladiators on social media. WIRED reached out to dozens, but few wanted to talk. One wrote in an email, "In my view, at least we did well under a challenging and complicated situation. But I wish we could realize how dangerous that virus is. If so we could have controlled it more tightly." The Filipina cook thought the Japanese government had done the best it could. But she's struggling. The two months' wages that Princess paid the *Diamond* crew because sailings were canceled fall short of covering her expenses while the industry was on pause. "We all risked our lives. But that's the decision. We can't do anything. We're helpless." Alex told me that whatever indignities happened on the *Diamond*, he's broke and has no option but to sign up for the next cruise that will have him.

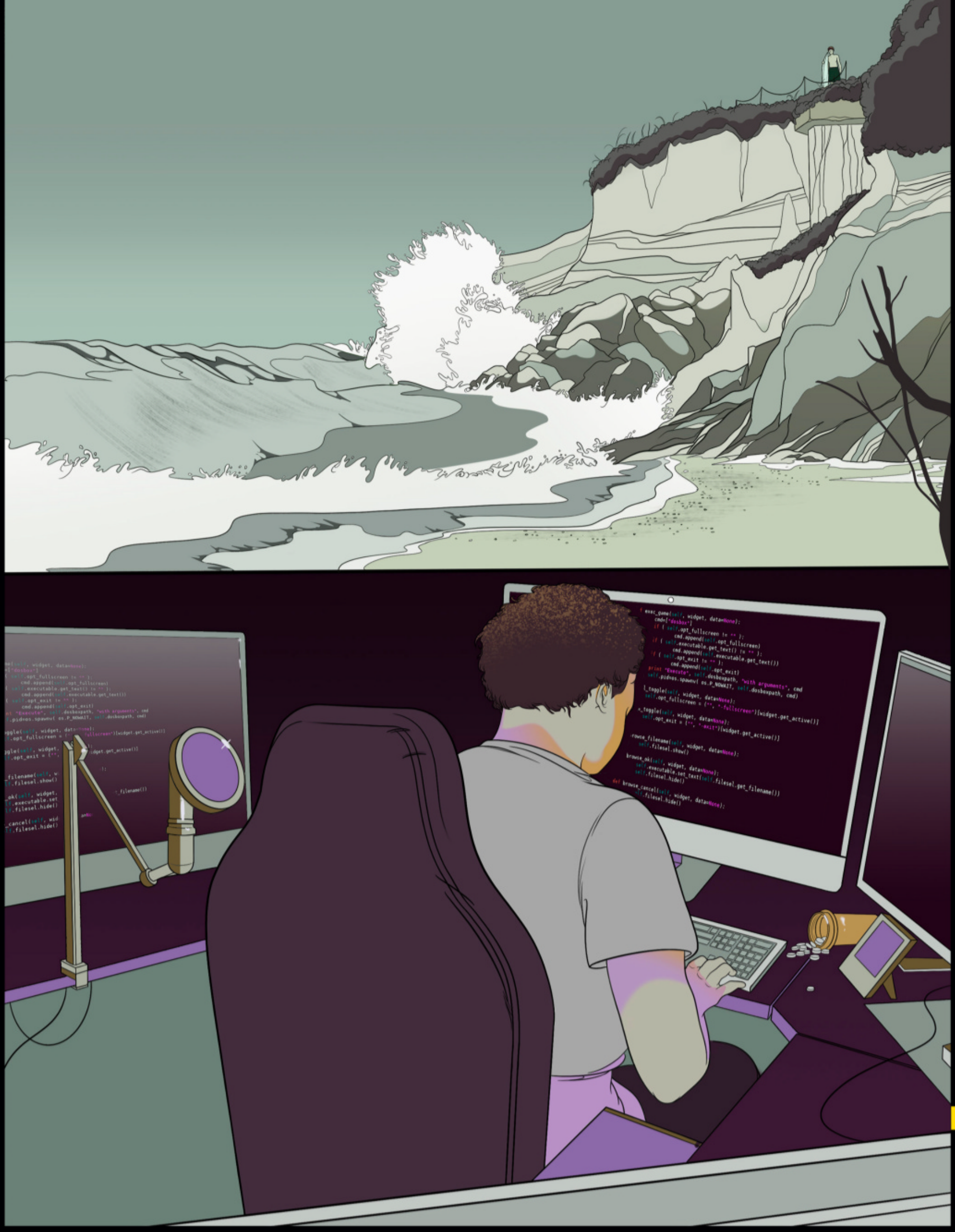
The world's attention soon swept to more urgent battles. In the US, the early response to Covid had been not unlike the *Diamond*'s. The country continued to cha-cha and play bingo while the virus ping-ponged among crowds. As the crisis swelled, Carnival offered up waylaid ships as overflow facilities to funnel non-coronavirus patients from overburdened ICUs. Turns out, the company said, the ships make excellent hospitals. Cleaning and meals courtesy of the crew.

---

**LAUREN SMILEY** *(@laurensmiley) is a regular contributor to* WIRED.

# THE CONFESSIONS OF MARCUS HUTCHINS

BY ANDY GREENBERG



**At 19, he was a security blogger with a mysteriously deep understanding of malware. At 22, he single-handedly put a stop to WannaCry, the worst cyberattack the world had ever seen. Then, just as he was being celebrated as the internet's savior, Marcus Hutchins was arrested by the FBI. This is his untold story.**

PHOTOGRAPH BY **RAMONA ROSALES** ILLUSTRATIONS BY **JANELLE BARONE**

# AT AROUND 7 AM ON A QUIET WEDNESDAY

**in August 2017,** Marcus Hutchins walked out the front door of the Airbnb mansion in Las Vegas where he had been partying for the past week and a half. A gangly, 6'4", 23-year-old hacker with an explosion of blond-brown curls, Hutchins had emerged to retrieve his order of a Big Mac and fries from an Uber Eats deliveryman. But as he stood barefoot on the mansion's driveway wearing only a T-shirt and jeans, Hutchins noticed a black SUV parked on the street—one that looked very much like an FBI stakeout.

He stared at the vehicle blankly, his mind still hazed from sleep deprivation and stoned from the legalized Nevada weed he'd been smoking all night. For a fleeting moment, he wondered: Is this finally it?

But as soon as the thought surfaced, he dismissed it. The FBI would never be so obvious, he told himself. His feet had begun to scald on the griddle of the driveway. So he grabbed the McDonald's bag and headed back inside, through the mansion's courtyard, and into the pool house he'd been using as a bedroom. With the specter of the SUV fully exorcised from his mind, he rolled another spliff with the last of his weed, smoked it as he ate his burger, and then packed his bags for the airport, where he was scheduled for a first-class flight home to the UK.

Hutchins was coming off of an epic, exhausting week at Defcon, one of the world's largest hacker conferences, where he had been celebrated as a hero. Less than three months earlier, Hutchins had saved the internet from what was, at the time, the worst cyberattack in history: a piece of malware called WannaCry. Just as that self-propagating software had begun exploding across the planet, destroying data on hundreds of thousands of computers, it was Hutchins who had found and triggered the secret kill switch contained in its code, neutering WannaCry's global threat immediately.

This legendary feat of whitehat hacking had essentially earned Hutchins free drinks for life among the Defcon crowd. He and his entourage had been invited to every VIP hacker party on the strip, taken out to dinner by journalists, and accosted by fans seeking selfies. The story, after all, was irresistible: Hutchins was the shy geek who had single-handedly slain a monster threatening the entire digital world, all while sitting in front of a keyboard in a bedroom in his parents' house in remote western England.

Still reeling from the whirlwind of adulation, Hutchins was in no state to dwell on concerns about the FBI, even after he emerged from the mansion a few hours later and once again saw the same black SUV parked across the street. He hopped into an Uber to the airport, his mind still floating through a cannabis-induced cloud. Court documents would later reveal that the SUV followed him along the way—that law enforcement had, in fact, been tracking his location periodically throughout his time in Vegas.

When Hutchins arrived at the airport and made his way through the security checkpoint, he was surprised when TSA agents told him not to bother taking any of his three laptops out of his backpack before putting it through the scanner. Instead, as they waved him through, he remembers thinking that they seemed to be making a special effort not to delay him.

He wandered leisurely to an airport lounge, grabbed a Coke, and settled into an armchair. He was still hours early for his flight back to the UK, so he killed time posting from his phone to Twitter, writing how excited he was to get back to his job analyzing malware when he got home. "Haven't touched a debugger in over a month now," he tweeted. He humblebragged about some very expensive shoes his boss had bought him in Vegas and retweeted a compliment from a fan of his reverse-engineering work.

Hutchins was composing another tweet when he noticed that three men had walked up to him, a burly redhead with a goatee flanked by two others in Customs and Border Protection uniforms. "Are you Marcus Hutchins?" asked the red-haired man. When Hutchins confirmed that he was, the man asked in a neutral tone for Hutchins to come with them, and led him through a door into a private stairwell.

Then they put him in handcuffs.

In a state of shock, feeling as if he were watching himself from a distance, Hutchins asked what was going on. "We'll get to that," the man said.

Hutchins remembers mentally racing through every possible illegal thing he'd done that might have interested Customs. Surely, he thought, it couldn't be *the thing*, that years-old, unmentionable crime. Was it that he might have left marijuana in his bag? Were these bored agents overreacting to petty drug possession?

The agents walked him through a secu-

rity area full of monitors and then sat him down in an interrogation room, where they left him alone. When the red-headed man returned, he was accompanied by a small blonde woman. The two agents flashed their badges: They were with the FBI.

For the next few minutes, the agents struck a friendly tone, asking Hutchins about his education and Kryptos Logic, the security firm where he worked. For those minutes, Hutchins allowed himself to believe that perhaps the agents wanted only to learn more about his work on WannaCry, that this was just a particularly aggressive way to get his cooperation into their investigation of that world-shaking cyberattack. Then, 11 minutes into the interview, his interrogators asked him about a program called Kronos.

"Kronos," Hutchins said. "I know that name." And it began to dawn on him, with a sort of numbness, that he was not going home after all.

## PART ONE
# DESCENT

**Fourteen years** earlier, long before Marcus Hutchins was a hero or villain to anyone, his parents, Janet and Desmond, settled into a stone house on a cattle farm in remote Devon, just a few minutes from the west coast of England. Janet was a nurse, born in Scotland. Desmond was a social worker from Jamaica who had been a firefighter when he first met Janet in a nightclub in 1986. They had moved from Bracknell, a commuter town 30 miles outside of London, looking for a place where their sons, 9-year-old Marcus and his 7-year-old brother, could grow up with more innocence than life in London's orbit could offer.

At first the farm offered exactly the idyll they were seeking: The two boys spent their days romping among the cows, watching farmhands milk them and deliver their calves. They built tree houses and trebuchets out of spare pieces of wood and rode in the tractor of the farmer who had rented their house to them. Hutchins was a bright and happy child, open to friendships but stoic and "self-contained," as his father, Desmond, puts it, with "a very strong sense of right and wrong." When he fell and broke his wrist while playing, he didn't shed a single tear, his father says. But when the farmer put down a lame, brain-damaged calf that Hutchins had bonded with, he cried inconsolably.

Hutchins didn't always fit in with the other kids in rural Devon. He was taller than the other boys, and he lacked the usual English obsession with soccer; he came to prefer surfing in the freezing waters a few miles from his house instead. He was one of only a few mixed-race children at his school, and he refused to cut his trademark mop of curly hair.

But above all, what distinguished Hutchins from everyone around him was his preternatural fascination and facility with computers. From the age of 6, Hutchins had watched his mother use Windows 95 on the family's Dell tower desktop. His father was often annoyed to find him dismantling the family PC or filling it with strange programs. By the time they moved to Devon, Hutchins had begun to be curious about the inscrutable HTML characters behind the websites he visited, and was coding rudimentary "Hello world" scripts in Basic. He soon came to see programming as "a gateway to build whatever you wanted," as he puts it, far more exciting than even the wooden forts and catapults he built with his brother. "There were no limits," he says.

In computer class, where his peers were still learning to use word processors, Hutchins was miserably bored. The school's computers prevented him from installing the games he wanted to play, like *Counterstrike* and *Call of Duty*, and they restricted the sites he could visit online. But Hutchins found he could program his way out of those constraints. Within Microsoft Word, he discovered a feature that allowed him to write scripts in a language called Visual Basic. Using that scripting feature, he could run whatever code he wanted and even install unapproved software. He used that trick to install a proxy to bounce his web traffic through a faraway server, defeating the school's attempts to filter and monitor his web surfing too.

On his 13th birthday, after years of fighting for time on the family's aging Dell, Hutchins' parents agreed to buy him his own computer—or rather, the components he requested, piece by piece, to build it himself. Soon, Hutchins' mother says, the computer became a "complete and utter love" that overruled almost everything else in her son's life.

Hutchins still surfed, and he had taken up a sport called surf lifesaving, a kind of competitive lifeguarding. He excelled at it and would eventually win a handful of medals at the national level. But when he wasn't in the water, he was in front of his computer, playing videogames or refining his programming skills for hours on end.

Janet Hutchins worried about her son's digital obsession. In particular, she feared how the darker fringes of the web, what she only half-jokingly calls the "internet boogeyman," might influence her son, who she saw as relatively sheltered in their rural English life.

So she tried to install parental controls on Marcus' computer; he responded by using a simple technique to gain administrative privileges when he booted up the PC, and immediately turned the controls off. She tried limiting his internet access via their home router; he found a hardware reset on the router that allowed him to restore it to factory settings, then configured the router to boot *her* offline instead.

"After that we had a long chat," Janet says. She threatened to remove the house's internet connection altogether. Instead they came to a truce. "We agreed that if he reinstated my internet access, I would monitor him in another way," she says. "But in actual fact, there was no way of monitoring Marcus. Because he was way more clever than any of us were ever going to be."

**Many mothers'** fears of the internet boogeyman are overblown. Janet Hutchins' were not.

Within a year of getting his own computer, Hutchins was exploring an elementary hacking web forum, one dedicated to wreaking havoc upon the then-popular instant messaging platform MSN. There he found a community of like-minded young hackers showing off their inventions. One bragged of creating a kind of MSN worm that impersonated a JPEG: When someone opened it, the malware would instantly and invisibly send itself to all their MSN contacts, some of whom would fall for the bait and open the photo, which would fire off another round of messages, ad infinitum.

Hutchins didn't know what the worm was meant to accomplish—whether it was intended for cybercrime or simply a spammy prank—but he was deeply impressed. "I was like, wow, look what programming can do," he says. "I want to be able to do *this* kind of stuff."

Around the time he turned 14, Hutchins

posted his own contribution to the forum—a simple password stealer. Install it on someone's computer and it could pull the passwords for the victim's web accounts from where Internet Explorer had stored them for its convenient autofill feature. The passwords were encrypted, but he'd figured out where the browser hid the decryption key too.

Hutchins' first piece of malware was met with approval from the forum. And whose passwords did he imagine might be stolen with his invention? "I didn't, really," Hutchins says. "I just thought, 'This is a cool thing I've made.'"

As Hutchins' hacking career began to take shape, his academic career was deteriorating. He would come home from the beach in the evening and go straight to his room, eat in front of his computer, and then pretend to sleep. After his parents checked that his lights were out and went to bed themselves, he'd get back to his keyboard. "Unbeknownst to us, he'd be up programming into the wee small hours," Janet says. When she woke him the next morning, "he'd look ghastly. Because he'd only been in bed for half an hour." Hutchins' mystified mother at one point was so worried she took her son to the doctor, where he was diagnosed with being a sleep-deprived teenager.

One day at school, when Hutchins was about 15, he found that he'd been locked out of his network account. A few hours later he was called into a school administrator's office. The staff there accused him of carrying out a cyberattack on the school's network, corrupting one server so deeply it had to be replaced. Hutchins vehemently denied any involvement and demanded to see the evidence. As he tells it, the administrators refused to share it. But he had, by that time, become notorious among the school's IT staff for flouting their security measures. He maintains, even today, that he was merely the most convenient scapegoat. "Marcus was never a good liar," his mother agrees. "He was quite boastful. If he had done it, he would have said he'd done it."

Hutchins was suspended for two weeks and permanently banned from using computers at school. His answer, from that point on, was simply to spend as little time there as possible. He became fully nocturnal, sleeping well into the school day and often skipping his classes altogether. His parents were furious, but aside from the moments when he was trapped in his mother's car, getting a ride to school or to go surfing, he mostly evaded their lectures and punishments. "They couldn't physically drag me to school," Hutchins says. "I'm a big guy."

Hutchins' family had, by 2009, moved off the farm, into a house that occupied the former post office of a small, one-pub village. Marcus took a room at the top of the stairs. He emerged from his bedroom only occasionally, to microwave a frozen pizza or make himself more instant coffee for his late-night programming binges. But for the most part, he kept his door closed and locked against his parents, as he delved deeper into a secret life to which they weren't invited.

**Around the** same time, the MSN forum that Hutchins had been frequenting shut down, so he transitioned to another community called HackForums. Its members were a shade more advanced in their skills and a shade murkier in their ethics: a *Lord of the Flies* collection of young hackers seeking to impress one another with nihilistic feats of exploitation. The minimum table stakes to gain respect from the HackForums crowd was possession of a botnet, a collection of hundreds or thousands of malware-infected computers that obey a hacker's commands, capable of directing junk traffic at rivals to flood their web server and knock them offline—what's known as a distributed denial of service, or DDoS, attack.

There was, at this point, no overlap between Hutchins' idyllic English village life and his secret cyberpunk one, no reality checks to prevent him from adopting the amoral atmosphere of the underworld he was entering. So Hutchins, still 15 years old, was soon bragging on the forum about running his own botnet of more than 8,000 computers, mostly hacked with simple fake files he'd uploaded to BitTorrent sites and tricked unwitting users into running.

Even more ambitiously, Hutchins also set up his own business: He began renting servers and then selling web hosting services to denizens of HackForums for a monthly


fee. The enterprise, which Hutchins called GhOsthosting, explicitly advertised itself on HackForums as a place where "all illegal sites" were allowed. He suggested in another post that buyers could use his service to host phishing pages designed to impersonate login pages and steal victims' passwords. When one customer asked if it was acceptable to host "warez"—black market software—Hutchins immediately replied, "Yeah any sites but child porn."

But in his teenage mind, Hutchins says, he still saw what he was doing as several steps removed from any *real* cybercrime. Hosting shady servers or stealing a few Facebook passwords or exploiting a hijacked computer to enlist it in DDoS attacks against other hackers—those hardly seemed like the serious offenses that would earn him the attention of law enforcement. Hutchins wasn't, after all, carrying out bank fraud, stealing actual money from innocent people. Or at least that's what he told himself. He says that the red line of financial fraud, arbitrary as it was, remained inviolable in his self-defined and shifting moral code.

In fact, within a year Hutchins grew bored with his botnets and his hosting service, which he found involved placating a lot of "whiny customers." So he quit both and began to focus on something he enjoyed far more: perfecting his own malware. Soon he was taking apart other hackers' rootkits—programs designed to alter a computer's operating system to make themselves entirely undetectable. He studied their features and learned to hide his code inside other computer processes to make his files invisible in the machine's file directory.

When Hutchins posted some sample code to show off his growing skills, another HackForums member was impressed enough that he asked Hutchins to write part of a program that would check whether specific antivirus engines could detect a hacker's malware, a kind of anti-antivirus tool. For that task, Hutchins was paid $200 in the early digital currency Liberty Reserve.

The same customer followed up by offering $800 for a "formgrabber" Hutchins had written, a rootkit that could silently steal passwords and other data that people had entered into web forms and send them to the hacker. He happily accepted.

Hutchins began to develop a reputation as a talented malware ghostwriter. Then, when he was 16, he was approached by a more serious client, a figure that the teenager would come to know by the pseudonym Vinny.

Vinny made Hutchins an offer: He wanted a multifeatured, well-maintained rootkit that he could sell on hacker marketplaces far more professional than HackForums, like Exploit.in and Dark0de. And rather than paying up front for the code, he would give Hutchins half the profits from every sale. They would call the product UPAS Kit, after the Javanese upas tree, whose toxic sap was traditionally used in Southeast Asia to make poison darts and arrows.

Vinny seemed different from the braggarts and wannabes Hutchins had met elsewhere in the hacker underground—more professional and tight-lipped, never revealing a single personal detail about himself even as they chatted more and more frequently. And both Hutchins and Vinny were careful to never log their conversations, Hutchins says. (As a result, WIRED has no record of their interactions, only Hutchins' account of them.)

Hutchins says he was always careful to cloak his movements online, routing his internet connection through multiple proxy servers and hacked PCs in Eastern Europe intended to confuse any investigator. But he wasn't nearly as disciplined about keeping the details of his personal life secret from Vinny. In one conversation, Hutchins complained to his business partner that there was no quality weed to be found anywhere in his village, deep in rural England. Vinny responded that he would mail him some from a new ecommerce site called Silk Road.

This was 2011, early days for Silk Road, and the notorious dark-web drug marketplace was mostly known only to those in the internet underground, not the masses who would later discover it. Hutchins himself thought it had to be a hoax. "Bullshit," he remembers writing to Vinny. "Prove it."

So Vinny asked for Hutchins' address—and his date of birth. He wanted to send him a birthday present, he said. Hutchins, in a moment he would come to regret, supplied both.

On Hutchins' 17th birthday, a package arrived for him in the mail at his parents' house. Inside was a collection of weed, hallucinogenic mushrooms, and ecstasy, courtesy of his mysterious new associate.

**Hutchins finished** writing UPAS Kit after nearly nine months of work, and in the summer of 2012 the rootkit went up for sale. Hutchins didn't ask Vinny any questions about who was buying. He was mostly just pleased to have leveled up from a HackForums show-off to a professional coder whose work was desired and appreciated.

The money was nice too: As Vinny began to pay Hutchins thousands of dollars in commissions from UPAS Kit sales—always in bitcoin—Hutchins found himself with his first real disposable income. He upgraded his computer, bought an Xbox and a new sound system for his room, and began to dabble in bitcoin day trading. By this point, he had dropped out of school entirely, and he'd quit surf lifesaving after his coach retired. He told his parents that he was working on freelance programming projects, which seemed to satisfy them.

With the success of UPAS Kit, Vinny told Hutchins that it was time to build UPAS Kit 2.0. He wanted new features for this sequel, including a keylogger that could record victims' every keystroke and the ability to see their entire screen. And most of all, he wanted a feature that could insert fake text-entry fields and other content into the pages that victims were seeing—something called a web inject.

That last demand in particular gave Hutchins a deeply uneasy feeling, he says. Web injects, in Hutchins' mind, had a very clear purpose: They were designed for bank fraud. Most banks require a second factor of authentication when making a transfer; they often send a code via text message to a user's phone and ask them to enter it on a web page as a double check of their identity. Web injects allow hackers to defeat that security measure by sleight of hand. A hacker initiates a bank transfer from the victim's account, and then, when the bank asks the hacker for a confirmation code, the hacker injects a fake message onto the victim's screen asking them to perform a routine reconfirmation of their identity with a text message code. When the victim enters that code from their phone, the hacker passes it on to the bank, confirming the transfer out of their account.

VINNY ADDED THAT HE KNEW HUTCHINS' IDENTITY AND ADDRESS. IF THEIR BUSINESS RELATIONSHIP ENDED, PERHAPS HE WOULD SHARE THAT INFORMATION WITH THE FBI.

Over just a few years, Hutchins had taken so many small steps down the unlit tunnel of online criminality that he'd often lost sight of the lines he was crossing. But in this IM conversation with Vinny, Hutchins says, he could see that he was being asked to do something very wrong—that he would now, without a doubt, be helping thieves steal from innocent victims. And by engaging in actual financial cybercrime, he'd also be inviting law enforcement's attention in a way he never had before.

Until that point, Hutchins had allowed himself to imagine that his creations might be used simply to steal access to people's Facebook accounts or to build botnets that mined cryptocurrency on people's PCs. "I never knew definitively what was happening with my code," he says. "But now it was obvious. This would be used to steal money from people. This would be used to wipe out people's savings."

He says he refused Vinny's demand. "I'm not fucking working on a banking trojan," he remembers writing.

Vinny insisted. And he added a reminder, in what Hutchins understood as equal parts joke and threat, that he knew Hutchins' identity and address. If their business relationship ended, perhaps he would share that information with the FBI.

As Hutchins tells it, he was both scared and angry at himself: He had naively shared identifying details with a partner who was turning out to be a ruthless criminal. But he held his ground and threatened to walk away. Vinny, knowing that he needed Hutchins' coding skills, seemed to back down. They reached an agreement: Hutchins would work on the revamped version of UPAS Kit, but without the web injects.

As he developed that next-generation rootkit over the following months, Hutchins began attending a local community college. He developed a bond with one of his computer science professors and was surprised to discover that he actually wanted to graduate. But he strained under the load of studying while also building and maintaining Vinny's malware. His business partner now seemed deeply impatient to have their new rootkit finished, and he pinged Hutchins constantly, demanding updates. To cope, Hutchins began turning back to Silk Road, buying amphetamines on the dark web to replace his nighttime coffee binges.

After nine months of all-night coding sessions, the second version of UPAS Kit was ready. But as soon as Hutchins shared the finished code with Vinny, he says, Vinny responded with a surprise revelation: He had secretly hired another coder to create the web injects that Hutchins had refused to build. With the two programmers' work combined, Vinny had everything he needed to make a fully functional banking trojan.

Hutchins says he felt livid, speechless. He quickly realized he had very little leverage against Vinny. The malware was already written. And for the most part, it was Hutchins who had authored it.

In that moment, all of the moral concerns and threats of punishment that Hutchins had brushed off for years suddenly caught up with him in a sobering rush. "There is no getting out of this," he remembers thinking. "The FBI is going to turn up at my door one day with an arrest warrant. And it will be because I trusted this fucking guy."

**Still, as deep** as Hutchins had been reeled in by Vinny, he had a choice.

Vinny wanted him to do the work of integrating the other programmer's web injects into their malware, then test the rootkit and maintain it with updates once it launched. Hutchins says he knew instinctively that he should walk away and never communicate with Vinny again. But as Hutchins tells it, Vinny seemed to have been preparing for this conversation, and he laid out an argument: Hutchins had already put in nearly nine months of work. He had already essentially built a banking rootkit that would be sold to customers, whether Hutchins liked it or not.

Besides, Hutchins was still being paid on commission. If he quit now, he'd get nothing. He'd have taken all the risks, enough to be implicated in the crime, but would receive none of the rewards.

As angry as he was at having fallen into Vinny's trap, Hutchins admits that he was also persuaded. So he added one more link to the yearslong chain of bad decisions that had defined his teenage life: He agreed to keep ghostwriting Vinny's banking malware.

Hutchins got to work, stitching the web inject features into his rootkit and then testing the program ahead of its release. But he found now that his love of coding had evaporated. He would procrastinate for as long as possible and then submerge into daylong coding binges, overriding his fear and guilt with amphetamines.

In June 2014, the rootkit was ready. Vinny began to sell their work on the cybercriminal marketplaces Exploit.in and Dark0de. Later he'd also put it up for sale on AlphaBay, a site on the dark web that had replaced Silk Road after the FBI tore the original darknet market offline.

After arguments with jilted customers, Vinny had decided to rebrand and drop the UPAS label. Instead, he came up with a new moniker, a play on Zeus, one of the most notorious banking trojans in the history of cybercrime. Vinny christened his malware in the name of a cruel giant in Greek mythology, the one who had fathered Zeus and all the other vengeful gods in the pantheon of Mount Olympus: He called it Kronos.

## PART TWO
# RECOVERY

**When Hutchins** was 19, his family moved again, this time into an 18th-century, four-story building in Ilfracombe, a Victorian seaside resort town in another part of Devon. Hutchins settled into the basement of the house, with access to his own bathroom and a kitchen that had once been used by the house's servants. That setup allowed him to cut himself off even further from his family and the world. He was, more than ever, alone.

When Kronos launched on Exploit.in, the malware was only a modest success. The largely Russian community of hackers on the site were skeptical of Vinny, who didn't speak their language and had priced the trojan at an ambitious $7,000. And like any new software, Kronos had bugs that needed fixing. Customers demanded constant updates and new features. So Hutchins was tasked with nonstop coding for the next year, now with tight deadlines and angry buyers demanding he meet them.

To keep up while also trying to finish his last year of college, Hutchins ramped up his amphetamine intake sharply. He would take enough speed to reach what he describes as a state of euphoria. Only in that condition, he says, could he still enjoy his programming work and stave off his growing dread. "Every time I heard a siren, I thought it was coming for me," he says. Vanquishing those thoughts with still more stimulants, he would stay up for days, studying and coding, and then crash into a state of anxiety and depression before sleeping for 24-hour stretches.

All that slingshotting between manic highs and miserable lows took a toll on Hutchins' judgment—most notably in his interactions with another online friend he calls Randy.

When Hutchins met Randy on a hacker forum called TrojanForge after the Kronos release, Randy asked Hutchins if he'd write banking malware for him. When Hutchins refused, Randy instead asked for help with some enterprise and educational apps he was trying to launch as legitimate businesses. Hutchins, seeing a way to launder his illegal earnings with legal income, agreed.

Randy proved to be a generous patron. When Hutchins told him that he didn't have a MacOS machine to work on Apple apps, Randy asked for his address—which again, Hutchins provided—and shipped him a new iMac desktop as a gift. Later, he asked if Hutchins had a PlayStation console so that they could play games together online. When Hutchins said he didn't, Randy shipped him a new PS4 too.

Unlike Vinny, Randy was refreshingly open about his personal life. As he and Hutchins became closer, they would call each other or even video chat, rather than interact via the faceless instant messaging Hutchins had become accustomed to. Randy impressed Hutchins by describing his philanthropic goals, how he was using his profits to fund charities like free cod-

ing education projects for kids. Hutchins sensed that much of those profits came from cybercrime. But he began to see Randy as a Robin Hood–like figure, a model he hoped to emulate someday. Randy revealed that he was based in Los Angeles, a sunny paradise where Hutchins had always dreamed of living. At some points, they even talked about moving in together, running a startup out of a house near the beach in Southern California.

Randy trusted Hutchins enough that when Hutchins described his bitcoin day-trading tricks, Randy sent him more than $10,000 worth of the cryptocurrency to trade on his behalf. Hutchins had set up his own custom-coded programs that hedged his bitcoin buys with short selling, protecting his holdings against bitcoin's dramatic fluctuations. Randy asked him to manage his own funds with the same techniques.

One morning in the summer of 2015, Hutchins woke up after an amphetamine bender to find that there had been an electrical outage during the night. All of his computers had powered off just as bitcoin's price crashed, erasing close to $5,000 of Randy's savings. Still near the bottom of his spasmodic cycle of drug use, Hutchins panicked.

He says he found Randy online and immediately admitted to losing his money. But to make up for the loss, he made Randy an offer. Hutchins revealed that he was the secret author of a banking rootkit called Kronos. Knowing that Randy had been looking for bank fraud malware in the past, he offered Randy a free copy. Randy, always understanding, called it even.

This was the first time Hutchins had divulged his work on Kronos to anyone. When he woke up the next day with a clearer head, he knew that he had made a terrible mistake. Sitting in his bedroom, he thought of all the personal information that Randy had so casually shared with him over the previous months, and he realized that he had just confided his most dangerous secret to someone whose operational security was deeply flawed. Sooner or later, Randy would be caught by law enforcement, and he would likely be just as forthcoming with the cops.

Hutchins had already come to view his eventual arrest for his cybercrimes as inevitable. But now he could see the Feds' path to his door. "Shit," Hutchins thought to himself. "This is how it ends."

**When Hutchins** graduated from college in the spring of 2015, he felt it was time to give up his amphetamine habit. So he decided to quit cold turkey.

At first the withdrawal symptoms simply mired him in the usual depressive low that he had experienced many times before. But one evening a few days in, while he was alone in his room watching the British teen drama *Waterloo Road*, he began to feel a dark sensation creep over him—what he describes as an all-encompassing sensation of "impending doom." Intellectually, he knew he was in no physical danger. And yet, "My brain was telling me, I'm about to die," he remembers.

He told no one. Instead he just rode out the withdrawal alone, experiencing what he describes as a multiday panic attack. When Vinny demanded to know why he was behind on his Kronos work, Hutchins says he found it was easier to say he was still busy with school, rather than admit that he was caught in a well of debilitating anxiety.

But as his symptoms drew on and he became even less productive over the weeks that followed, he found that his menacing business associate seemed to bother him less. After a few scoldings, Vinny left him alone. The bitcoin payments for Kronos commissions ended, and with them went the partnership that had pulled Hutchins into the darkest years of his life as a cybercriminal.

For the next months, Hutchins did little more than hide in his room and recover. He played videogames and binge-watched *Breaking Bad*. He left his house only rarely, to swim in the ocean or join groups of storm chasers who would gather on the cliffs near Ilfracombe to watch 50- and 60-foot waves slam into the rocks. Hutchins remembers enjoying how small the waves made him feel, imagining how their raw power could kill him instantly.

It took months for Hutchins' feeling of impending doom to abate, and even then it was replaced by an intermittent, deep-

seated angst. As he leveled out, Hutchins began to delve back into the world of hacking. But he had lost his taste for the cybercriminal underworld. Instead, he turned back to a blog that he'd started in 2013, in the period between dropping out of secondary school and starting college.

The site was called MalwareTech, which doubled as Hutchins' pen name as he began to publish a slew of posts on the technical minutiae of malware. The blog's clinical, objective analysis soon seemed to attract both blackhat and whitehat visitors. "It was kind of this neutral ground," he says. "Both sides of the game enjoyed it."

At one point he even wrote a deep-dive analysis of web injects, the very feature of Kronos that had caused him so much anxiety. In other, more impish posts, he'd point out vulnerabilities in competitors' malware that allowed their victims' computers to be commandeered by other hackers. Soon he had an audience of more than 10,000 regular readers, and none of them seemed to know that MalwareTech's insights stemmed from an active history of writing malware himself.

During his post-Kronos year of rehabilitation, Hutchins started reverse-engineering some of the largest botnets out in the wild, known as Kelihos and Necurs. But he soon went a step further, realizing he could actually *join* those herds of hijacked machines and analyze them for his readers from the inside. The Kelihos botnet, for instance, was designed to send commands from one victim computer to another, rather than from a central server—a peer-to-peer architecture designed to make the botnet harder to take down. But that meant Hutchins could actually code his own program that mimicked the Kelihos malware and "spoke" its language, and use it to spy on all the rest of the botnet's operations—once he had broken past all the obfuscation the botnets' designers had devised to prevent that sort of snooping.

Using this steady stream of intelligence, Hutchins built a Kelihos botnet "tracker," mapping out on a public website the hundreds of thousands of computers around the world it had ensnared. Not long after that, an entrepreneur named Salim Neino, the CEO of a small Los Angeles–based cybersecurity firm called Kryptos Logic, emailed MalwareTech to ask if the anonymous blogger might do some work for them. The firm was hoping to create a botnet tracking service, one that would alert victims if their IP addresses showed up in a collection of hacked machines like Kelihos.

In fact, the company had already asked one of its employees to get inside Kelihos, but the staffer had told Neino that reverse-engineering the code would take too much time. Without realizing what he was doing, Hutchins had unraveled one of the most inscrutable botnets on the internet.

Neino offered Hutchins $10,000 to build Kryptos Logic its own Kelihos tracker. Within weeks of landing that first job, Hutchins had built a tracker for a second botnet too, an even bigger, older amalgamation of hacked PCs known as Sality. After that, Kryptos Logic made Hutchins a job offer, with a six-figure annual salary. When Hutchins saw how the numbers broke down, he thought Neino must be joking. "What?" he remembers thinking. "You're going to send me this much money *every month*?"

It was more than he had ever earned as a cybercriminal malware developer. Hutchins had come to understand, too late, the reality of the modern cybersecurity industry: For a talented hacker in a Western country, crime truly doesn't pay.

**In his first** months at Kryptos Logic, Hutchins got inside one massive botnet after another: Necurs, Dridex, Emotet—malware networks encompassing millions of computers in total. Even when his new colleagues at Kryptos believed that a botnet was impregnable, Hutchins would surprise them by coming up with a fresh sample of the bot's code, often shared with him by a reader of his blog or supplied by an underground source. Again and again, he would deconstruct the program and—still working from his bedroom in Ilfracombe—allow the company to gain access to a new horde of zombie machines, tracking the malware's spread and alerting the hackers' victims.

"When it came to botnet research, he was probably one of the best in the world at that

point. By the third or fourth month, we had tracked every major botnet in the world with his help," Neino says. "He brought us to another level."

Hutchins continued to detail his work on his MalwareTech blog and Twitter, where he began to be regarded as an elite malware-whisperer. "He's a reversing savant, when it comes down to it," says Jake Williams, a former NSA hacker turned security consultant who chatted with MalwareTech and traded code samples with him around that time. "From a raw skill level, he's off the charts. He's comparable to some of the best I've worked with, anywhere." Yet aside from his Kryptos Logic colleagues and a few close friends, no one knew MalwareTech's real identity. Most of his tens of thousands of followers, like Williams, recognized him only as the Persian cat with sunglasses that Hutchins used as a Twitter avatar.

In the fall of 2016, a new kind of botnet appeared: A piece of malware known as Mirai had begun to infect so-called internet-of-things devices—wireless routers, digital video recorders, and security cameras—and was lashing them together into massive swarms capable of shockingly powerful DDoS attacks. Until then, the largest DDoS attacks ever seen had slammed their targets with a few hundred gigabits per second of traffic. Now victims were being hit with more like 1 *terabit* per second, gargantuan floods of junk traffic that could tear offline anything in their path. To make matters worse, the author of Mirai, a hacker who went by the name Anna-Senpai, posted the code for the malware on HackForums, inviting others to make their own Mirai offshoots.

In September of that year, one Mirai attack hit the website of the security blogger Brian Krebs with more than 600 gigabits per second, taking his site down instantly. Soon after, the French hosting company OVH buckled under a 1.1-terabit-per-second torrent. In October, another wave hit Dyn, a provider of the domain-name-system servers that act as a kind of phone book for the internet, translating domain names into IP addresses. When Dyn went down, so did Amazon, Spotify, Netflix, PayPal, and Reddit for users across parts of North America and Europe. Around the same time, a Mirai attack hit the main telecom provider for much of Liberia, knocking most of the country off the internet.

Hutchins, always a storm chaser, began to track Mirai's tsunamis. With a Kryptos Logic colleague, he dug up samples of Mirai's code and used them to create programs that infiltrated the splintered Mirai botnets, intercepting their commands and creating a Twitter feed that posted news of their attacks in real time. Then, in January 2017, the same Mirai botnet that hit Liberia began to rain down cyberattacks on Lloyds of London, the largest bank in the UK, in an apparent extortion campaign that took the bank's website down multiple times over a series of days.

Thanks to his Mirai tracker, Hutchins could see which server was sending out the commands to train the botnet's firepower on Lloyds; it appeared that the machine was being used to run a DDoS-for-hire service. And on that server, he discovered contact information for the hacker who was administering it. Hutchins quickly found him on the instant messaging service Jabber, using the name "popopret."

So he asked the hacker to stop. He told popopret he knew that he wasn't directly responsible for the attack on Lloyds himself, that he was only selling access to his Mirai botnet. Then he sent him a series of messages that included Twitter posts from Lloyds customers who had been locked out of their accounts, some of whom were stuck in foreign countries without money. He also pointed out that banks were designated as critical infrastructure in the UK, and that meant British intelligence services were likely to track down the botnet administrator if the attacks continued.

The DDoS attacks on the banks ended. More than a year later, Hutchins would recount the story on his Twitter feed, noting that he wasn't surprised the hacker had ultimately listened to reason. In his tweets, Hutchins offered a rare hint of his own secret past—he knew what it was like to sit behind a keyboard, detached from the pain inflicted on innocents far across the internet.

"In my career I've found few people are truly evil, most are just too far disconnected from the effects of their actions," he wrote. "Until someone reconnects them."

**Around noon** on May 12, 2017, just as Hutchins was starting a rare week of vacation, Henry Jones was sitting 200 miles to the east amid a cluster of a half-dozen PCs in an administrative room at the Royal London Hospital, a major surgical and trauma center in northeast London, when he saw the first signs that something was going very wrong.

Jones, a young anesthesiologist who asked that WIRED not use his real name, was finishing a lunch of chicken curry and chips from the hospital cafeteria, trying to check his email before he was called back into surgery, where he was trading shifts with a more senior colleague. But he couldn't log in; the email system seemed to be down. He shared a brief collective grumble with the other doctors in the room, who were all accustomed to computer problems across the National Health Service; after all, their PCs were still running Windows XP, a nearly 20-year-old operating system. "Another day at the Royal London," he remembers thinking.

But just then, an IT administrator came into the room and told the staff that something more unusual was going on: A virus seemed to be spreading across the hospital's network. One of the PCs in the room had rebooted, and now Jones could see that it showed a red screen with a lock in the upper left corner. "Ooops, your files have been encrypted!" it read. At the bottom of the screen, it demanded a $300 payment in bitcoin to unlock the machine.

Jones had no time to puzzle over the message before he was called back into the surgical theater. He scrubbed, put on his mask and gloves, and reentered the operating room, where surgeons were just finishing an orthopedic procedure. Now it was Jones' job to wake the patient up again. He began to slowly turn a dial that tapered off the sevoflurane vapor feeding into the patient's lungs, trying to time the process exactly so that the patient wouldn't wake up before he'd had a chance to remove the breathing tube, but wouldn't stay out long enough to delay their next surgery.

As he focused on that task, he could hear the surgeons and nurses expressing dismay as they tried to record notes on the surgery's outcome: The operating room's desktop PC seemed to be dead.

Jones finished rousing the patient and scrubbed out. But when he got into the hallway, the manager of the surgical theater intercepted him and told him that all of his cases for the rest of the day had been canceled. A cyberattack had hit not only the whole hospital's network but the entire trust, a collection of five hospitals across East London. All of their computers were down.

Jones felt shocked and vaguely outraged. Was this a coordinated cyberattack on mul-

WANNACRY SEEMED POISED TO SPREAD TO THE U.S. HEALTH CARE SYSTEM. "IF THIS HAPPENS EN MASSE, HOW MANY PEOPLE DIE?" CORMAN REMEMBERS THINKING. "OUR WORST NIGHTMARE SEEMED TO BE COMING TRUE."

tiple NHS hospitals? With no patients to see, he spent the next hours at loose ends, helping the IT staff unplug computers around the Royal London. But it wasn't until he began to follow the news on his iPhone that he learned the full scale of the damage: It wasn't a targeted attack but an automated worm spreading across the internet. Within hours, it hit more than 600 doctor's offices and clinics, leading to 20,000 canceled appointments, and wiped machines at dozens of hospitals. Across those facilities, surgeries were being canceled, and ambulances were being diverted from emergency rooms, sometimes forcing patients with life-threatening conditions to wait crucial minutes or hours longer for care. Jones came to a grim realization: "People may have died as a result of this."

Cybersecurity researchers named the worm WannaCry, after the .wncry extension it added to file names after encrypting them. As it paralyzed machines and demanded its bitcoin ransom, WannaCry was jumping from one machine to the next using a powerful piece of code called EternalBlue, which had been stolen from the National Security Agency by a group of hackers known as the Shadow Brokers and leaked onto the open internet a month earlier. It instantly allowed a hacker to penetrate and run hostile code on any unpatched Windows computer—a set of potential targets that likely numbered in the millions. And now that the NSA's highly sophisticated spy tool had been weaponized, it seemed bound to create a global ransomware pandemic within hours.

"It was the cyber equivalent of watching the moments before a car crash," says one cybersecurity analyst who worked for British Telecom at the time and was tasked with incident response for the NHS. "We knew that, in terms of the impact on people's lives, this was going to be like nothing we had ever seen before."

As the worm spread around the world, it infected the German railway firm Deutsche Bahn, Sberbank in Russia, automakers Renault, Nissan, and Honda, universities in China, police departments in India, the Spanish telecom firm Telefónica, FedEx, and Boeing. In the space of an afternoon, it destroyed, by some estimates, nearly a quarter-million computers' data, inflicting between $4 billion and $8 billion in damage.

For those watching WannaCry's proliferation, it seemed there was still more pain to come. Josh Corman, at the time a cybersecurity-focused fellow for the Atlantic Council, remembers joining a call on the afternoon of May 12 with representatives from the US Department of Homeland Security, the Department of Health and Human Services, the pharmaceutical firm Merck, and executives from American hospitals. The group, known as the Healthcare Cybersecurity Industry Taskforce, had just finished an analysis that detailed a serious lack of IT security personnel in American hospitals. Now WannaCry seemed poised to spread to the US health care system, and Corman feared the results would be far worse than they had been for the NHS. "If this happens en masse, how many people die?" he remembers thinking. "Our worst nightmare seemed to be coming true."

**At around** 2:30 on that Friday afternoon, Marcus Hutchins returned from picking up lunch at his local fish-and-chips shop in Ilfracombe, sat down in front of his computer, and discovered that the internet was on fire. "I picked a hell of a fucking week to take off work," Hutchins wrote on Twitter.

Within minutes, a hacker friend who went by the name Kafeine sent Hutchins a copy of WannaCry's code, and Hutchins began trying to dissect it, with his lunch still sitting in front of him. First, he spun up a simulated computer on a server that he ran in his bedroom, complete with fake files for the ransomware to encrypt, and ran the program in that quarantined test environment. He immediately noticed that before encrypting the decoy files, the malware sent out a query to a certain, very random-looking web address: *iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*.

That struck Hutchins as significant, if not unusual: When a piece of malware pinged back to this sort of domain, that usually meant it was communicating with a command-and-control server somewhere that might be giving the infected computer instructions. Hutchins copied that long website string into his web browser and found, to his surprise, that no such site existed.

So he visited the domain registrar Namecheap and, at four seconds past 3:08 pm, registered that unattractive web address at a cost of $10.69. Hutchins hoped that in doing so, he might be able to steal control of some part of WannaCry's horde of victim computers away from the malware's creators. Or at least he might gain a tool to monitor the number and location of infected machines, a move that malware analysts call "sinkholing."

Sure enough, as soon as Hutchins set up that domain on a cluster of servers hosted by his employer, Kryptos Logic, it was bombarded with thousands of connections from every new computer that was being infected by WannaCry around the world. Hutchins could now see the enormous, global scale of the attack firsthand. And as he tweeted about his work, he began to be flooded with hundreds of emails from other researchers, journalists, and system administrators trying to learn more about the plague devouring the world's networks. With his sinkhole domain, Hutchins was now suddenly pulling in information about those infections that no one else on the planet possessed.

For the next four hours, he responded to those emails and worked frantically to debug a map he was building to track the new infections popping up globally, just as he had done with Kelihos, Necurs, and so many other botnets. At 6:30 pm, around three and a half hours after Hutchins had registered the domain, his hacker friend Kafeine sent him a tweet posted by another security researcher, Darien Huss.

The tweet put forward a simple, terse statement that shocked Hutchins: "Execution fails now that domain has been sinkholed."

In other words, since Hutchins' domain had first appeared online, WannaCry's new infections had continued to spread, but they hadn't actually done any new damage. The worm seemed to be neutralized.

Huss' tweet included a snippet of WannaCry's code that he'd reverse-engineered. The code's logic showed that before encrypting any files, the malware first checked if it could reach Hutchins' web address. If not, it went ahead with corrupting the computer's contents. If it did reach that address, it simply stopped in its tracks. (Malware analysts still debate what the purpose of that feature was—whether it was intended as an antivirus evasion technique or a safeguard built into the worm by its author.)

Hutchins hadn't found the malware's command-and-control address. He'd found its kill switch. The domain he'd registered was a way to simply, instantly turn off WannaCry's mayhem around the world. It was as if he had fired two proton torpedoes through the Death Star's exhaust port and into its reactor core, blown it up, and saved the galaxy, all without understanding what he was doing or even noticing the explosion for three and a half hours.

When Hutchins grasped what he'd done, he leaped up from his chair and jumped around his bedroom, overtaken with joy. Then he did something equally unusual: He went upstairs to tell his family.

Janet Hutchins had the day off from her job as a nurse at a local hospital. She had been in town catching up with friends and had just gotten home and started making dinner. So she had only the slightest sense of the crisis that her colleagues had been dealing with across the NHS. That's when her son came upstairs and told her, a little uncertainly, that he seemed to have stopped the worst malware attack the world had ever seen.

"Well done, sweetheart," Janet Hutchins said. Then she went back to chopping onions.

**It took a few** hours longer for Hutchins and his colleagues at Kryptos Logic to understand that WannaCry was still a threat. In fact, the domain that Hutchins had registered was still being bombarded with connections from WannaCry-infected computers all over the globe as the remnants of the neutered worm continued to spread: It would receive nearly 1 million connections over the next two days. If their web domain went

offline, every computer that attempted to reach the domain and failed would have its contents encrypted, and WannaCry's wave of destruction would begin again. "If this goes down, WannaCry restarts," Hutchins' boss, Salim Neino, remembers realizing. "Within 24 hours, it would have hit every vulnerable computer in the world."

Almost immediately, the problem grew: The next morning, Hutchins noticed a new flood of pings mixed into the WannaCry traffic hitting their sinkhole. He quickly realized that one of the Mirai botnets that he and his Kryptos colleagues had monitored was now slamming the domain with a DDoS attack—perhaps as an act of revenge for their work tracking Mirai, or simply out of a nihilistic desire to watch WannaCry burn down the internet. "It was like we were Atlas, holding up the world on our shoulders," Neino says. "And now someone was kicking Atlas in the back at the same time."

For days afterward, the attacks swelled in size, threatening to bring down the sinkhole domain. Kryptos scrambled to filter and absorb the traffic, spreading the load over a collection of servers in Amazon data centers and the French hosting firm OVH. But they got another surprise a few days later, when local police in the French city of Roubaix, mistakenly believing that their sinkhole domain was being used by the cybercriminals behind WannaCry, physically seized two of their servers from the OVH data center. For a week, Hutchins slept no more than three consecutive hours as he struggled to counter the shifting attacks and keep the WannaCry kill switch intact.

Meanwhile, the press was chipping away at Hutchins' carefully maintained anonymity. On a Sunday morning two days after WannaCry broke out, a local reporter showed up at the Hutchins' front door in Ilfracombe. The reporter's daughter had gone to school with Hutchins, and she recognized him in a Facebook photo that named him in its caption as MalwareTech.

Soon more journalists were ringing the doorbell, setting up in the parking lot across the street from their house, and calling so often that his family stopped answering the phone. British tabloids began to run headlines about the "accidental hero" who had saved the world from his bedroom. Hutchins had to jump over his backyard's wall to avoid the reporters staking out his front door. To defuse the media's appetite, he agreed to give one interview to the Associated Press, during which he was so nervous that he misspelled his last name and the newswire had to run a correction.

In those chaotic first days, Hutchins was constantly on edge, expecting another version of WannaCry to strike; after all, the hackers behind the worm could easily tweak it to remove its kill switch and unleash a sequel. But no such mutation occurred. After a few days, Britain's National Cybersecurity Center reached out to Amazon on Kryptos' behalf and helped the firm negotiate unlimited server capacity in its data centers. Then, after a week, the DDoS mitigation firm Cloudflare stepped in to offer its services, absorbing as much traffic as any botnet could throw at the kill-switch domain and ending the standoff.

When the worst of the danger was over, Neino was concerned enough for Hutchins' well-being that he tied part of his employee's bonus to forcing him to get some rest. When Hutchins finally went to bed, a week after WannaCry struck, he was paid more than $1,000 for every hour of sleep.

**As uncomfortable** as the spotlight made Hutchins, his newfound fame came with some rewards. He gained 100,000 Twitter followers virtually overnight. Strangers recognized him and bought him drinks in the local pub to thank him for saving the internet. A local restaurant offered him free pizza for a year. His parents, it seemed, finally understood what he did for a living and were deeply proud of him.

But only at Defcon, the annual 30,000-person Las Vegas hacker conference that took place nearly three months after WannaCry hit, did Hutchins truly allow himself to enjoy his new rock star status in the cybersecurity world. In part to avoid the fans who constantly asked for selfies with him, he and a group of friends rented a real estate mogul's mansion off the strip via Airbnb,

with hundreds of palm trees surrounding the largest private pool in the city. They skipped the conference itself, with its hordes of hackers lining up for research talks. Instead they alternated between debauchery partying—making ample use of the city's marijuana dispensaries and cybersecurity firms' lavish open-bar events—and absurd daytime acts of recreation.

One day they went to a shooting range, where Hutchins fired a grenade launcher and hundreds of high-caliber rounds from an M134 rotary machine gun. On other days they rented Lamborghinis and Corvettes and zoomed down Las Vegas Boulevard and through the canyons around the city. At a performance by one of Hutchins' favorite bands, the Chainsmokers, he stripped down to his underwear and jumped into a pool in front of the stage. Someone stole his wallet out of the pants he'd left behind. He was too elated to care.

Three years had passed since Hutchins' work on Kronos, and life was good. He felt like a different person. And as his star rose, he finally allowed himself—almost—to let go of the low-lying dread, the constant fear that his crimes would catch up with him.

Then, on his last morning in Vegas, Hutchins stepped barefoot onto the driveway of his rented mansion and saw a black SUV parked across the street.

AS HIS STAR ROSE, HUTCHINS FINALLY ALLOWED HIMSELF—ALMOST—TO LET GO OF THE LOW-LYING DREAD, THE CONSTANT FEAR THAT HIS CRIMES WOULD CATCH UP WITH HIM.

## PART THREE
# RECKONING

**Almost immediately,** Hutchins gave his FBI interrogators a kind of half-confession. Minutes after the two agents brought up Kronos in the McCarran Airport interrogation room, he admitted to having created parts of the malware, though he falsely claimed to have stopped working on it before he turned 18. Some part of him, he says, still hoped that the agents might just be trying to assess his credibility as a witness in their WannaCry investigation or to strong-arm him into giving them control of the WannaCry sinkhole domain. He nervously answered their questions—without a lawyer present.

His wishful thinking evaporated, however, when the agents showed him a printout: It was the transcript of his conversation with "Randy" from three years earlier, when 20-year-old Hutchins had offered his friend a copy of the banking malware he was still maintaining at the time.

Finally, the red-headed agent who had first handcuffed him, Lee Chartier, made the agents' purpose clear. "If I'm being honest with you, Marcus, this has absolutely nothing to do with WannaCry," Chartier said. The agents pulled out a warrant for his arrest on conspiracy to commit computer fraud and abuse.

Hutchins was driven to a Las Vegas jail in a black FBI SUV that looked exactly like the one he'd spotted in front of his Airbnb that morning. He was allowed one phone call, which he used to contact his boss, Salim Neino. Then he was handcuffed to a chair in a room full of prisoners and left to wait for the rest of the day and the entire night that followed. Only when he asked to use the bathroom was he let into a cell where he could lie down on a concrete bed until someone else asked to use the cell's toilet. Then he'd be moved out of the cell and chained to the chair again.

Instead of sleep, he mostly spent those long hours tumbling down the bottomless mental hole of his imagined future: months of pretrial detention followed by years in prison. He was 5,000 miles from home. It was the loneliest night of his 23-year-old life.

**Unbeknownst** to Hutchins, however, a kind of immune response was already mounting within the hacker community. After receiving the call from jail, Neino had alerted Andrew Mabbitt, one of Hutchins' hacker friends in Las Vegas; Mabbitt leaked the news to a reporter at Vice and raised the alarm on Twitter.

Immediately, high-profile accounts began to take up Hutchins' cause, rallying around the martyred hacker hero.

"The DoJ has seriously fucked up," tweeted one prominent British cybersecurity researcher, Kevin Beaumont. "I can vouch for @MalwareTechBlog being a really nice guy and also for having strong ethics," wrote Martijn Grooten, the organizer of the Virus Bulletin cybersecurity conference, using Hutchins' Twitter handle. Some believed that the FBI had mistakenly arrested Hutchins for his WannaCry work, perhaps confusing him with the hackers behind the worm: "It's not often I see the entire hacker community really get this angry, but arresting @MalwareTechBlog for *stopping an attack* [is] unacceptable," wrote Australian cypherpunk activist Asher Wolf.

Not everyone was supportive of Hutchins: Ex-NSA hacker Dave Aitel went so far as to write in a blog post that he suspected Hutchins had created WannaCry himself and triggered his own kill switch only after the worm got out of control. (That theory would be deflated eight months later, when the Justice Department indicted a North Korean hacker as an alleged member of a state-sponsored hacking team responsible for WannaCry.) But the overwhelming response to Hutchins' arrest was sympathetic. By the next day, the representative for Hutchins' region in the UK parliament, Peter Heaton-Jones, issued a statement expressing his "concern and shock," lauding Hutchins' work on WannaCry and noting that "people who know him in Ilfracombe, and the wider cyber community, are astounded at the allegations against him."

Mabbitt found Hutchins a local attorney for his bail hearing, and after Hutchins spent a miserable day in a crowded cage, his bail was set at $30,000. Stripped of his computers and phones, Hutchins couldn't get access to his bank accounts to cover that cost. So Tor Ekeland, a renowned hacker defense attorney, agreed to manage a legal fund in Hutchins' name to help cover the bond. Money poured in. Almost immediately, stolen credit cards began to show up among the sources of donations, hardly a good look for a computer fraud defendant. Ekeland responded by pulling the plug, returning all the donations and closing the fund.

But the hacker community's goodwill toward Hutchins hadn't run out. On the day he was arrested, a pair of well-known cybersecurity professionals named Tarah Wheeler and Deviant Ollam had flown back to Seattle from Las Vegas. By that Sunday evening, the recently married couple were talking to Hutchins' friend Mabbitt and learning about the troubles with Hutchins' legal fund.

Wheeler and Ollam had never met Hutchins and had barely even interacted with him on Twitter. But they had watched the Justice Department railroad idealistic young hackers for years, from Aaron Swartz to Chelsea Manning, often with tragic consequences. They imagined Hutchins, alone in the federal justice system, facing a similar fate. "We basically had a young, foreign, nerdy person of color being held in federal detention," Wheeler says. "He was the closest thing to a global hero the hacker community had. And no one was there to help him."

Wheeler had just received a five-figure severance package from the security giant Symantec because her division had been shuttered. She and Ollam had been planning to use the money as a down payment on a home. Instead, on a whim, they decided to spend it bailing out Marcus Hutchins.

Within 24 hours of leaving Las Vegas, they got on a flight back to the city. They landed on Monday afternoon, less than 90 minutes before the courthouse's 4 pm deadline for bail payments. If they didn't make it in time, Hutchins would be sent back to jail for another night. From the airport, they jumped in a Lyft to a bank where they took out a $30,000 cashier's check. But when they arrived at the courthouse, a court official told them it had to be notarized. Now they had only 20 minutes left until the court's office closed.

Wheeler was wearing Gucci loafers. She took them off and, barefoot in a black sweater and pencil skirt, sprinted down the street in the middle of a scorching Las Vegas summer afternoon, arriving at the notary less than 10 minutes before 4 pm. Soaked in sweat, she got the check notarized, flagged down a stranger's car, and convinced the driver to ferry her back to the courthouse. Wheeler burst through the door at 4:02 pm, just before the clerk closed up for the day, and handed him the check that would spring Marcus Hutchins from jail.

**From there,** Hutchins was bailed to a crowded halfway house, while even more forces in the hacker community were gathering to come to his aid. Two veteran lawyers, Brian Klein and well-known hacker defense attorney Marcia Hofmann, took his case pro bono. At his arraignment he pleaded not guilty, and a judge agreed that he could be put under house arrest in Los Angeles, where Klein had an office. Over the next two months, his lawyers chipped away at his pretrial detainment conditions, allowing him to travel beyond his Marina del Rey apartment and to use computers and the internet—though the court forbade him access to the WannaCry sinkhole domain he had created. Eventually, even his curfew and GPS monitoring ankle bracelet were removed.

Hutchins got the news that those last pretrial restrictions were being lifted while attending a bonfire party on the beach with friendly hackers from the LA cybersecurity conference Shellcon. Somehow, getting indicted for years-old cybercrimes on a two-week trip to the US had delivered him to the city where he'd always dreamed of living, with relatively few limits on his freedom of movement. Kryptos Logic had put him on unpaid leave, so he spent his days surfing and cycling down the long seaside path that ran from his apartment to Malibu.

And yet he was deeply depressed. He had no income, his savings were dwindling, and he had charges hanging over him that promised years in prison.

Beyond all of that, he was tormented by the truth: Despite all the talk of his heroics, he knew that he had, in fact, done exactly what he was accused of. A feeling of overwhelming guilt had set in the moment he first regained access to the internet and checked his Twitter mentions a month after his arrest. "All of these people are writing to the FBI to say 'you've got the wrong guy.' And it was heartbreaking," Hutchins says. "The guilt from this was a thousand times the guilt I'd felt for Kronos." He says he was tempted to publish a full confession on his blog, but was dissuaded by his lawyers.

Many supporters had interpreted his not-guilty plea as a statement of innocence rather than a negotiating tactic, and they donated tens of thousands of dollars more to a new legal fund. Former NSA hacker Jake Williams had agreed to serve as an expert witness on Hutchins' behalf. Tarah Wheeler and Deviant Ollam had become almost foster parents, fly-

ing with him to Milwaukee for his arraignment and helping him get his life set up in LA. He felt he deserved none of this—that everyone had come to his aid only under the mistaken assumption of his innocence.

In fact, much of the support for Hutchins was more nuanced. Just a month after his arrest, cybersecurity blogger Brian Krebs delved into Hutchins' past and found the chain of clues that led to his old posts on HackForums, revealing that he had run an illegal hosting service, maintained a botnet, and authored malware—though not necessarily Kronos. Even as the truth started to come into focus, though, many of Hutchins' fans and friends seemed undeterred in their support for him. "We are all morally complex people," Wheeler says. "For most of us, anything good we ever do comes either because we did bad before or because other people did good to get us out of it, or both."

But Hutchins remained tortured by a kind of moral impostor syndrome. He turned to alcohol and drugs, effacing his emotions with large doses of Adderall during the day and vodka at night. At times, he felt suicidal. The guilt, he says, "was eating me alive."

**In the spring** of 2018, nearly nine months after his arrest, prosecutors offered Hutchins a deal. If he agreed to reveal everything he knew about the identities of other criminal hackers and malware authors from his time in the underworld, they would recommend a sentence of no prison time.

Hutchins hesitated. He says he didn't actually know anything about the identity of Vinny, the prosecutors' real target. But he also says that, on principle, he opposed snitching on the petty crimes of his fellow hackers to dodge the consequences of his own actions. Moreover, the deal would still result in a felony record that might prevent him from ever returning to the US. And he knew that the judge in his case, Joseph Stadtmueller, had a history of unpredictable sentencing, sometimes going well below or above the recommendations of prosecutors. So Hutchins refused the deal and set his sights on a trial.

Soon afterward, prosecutors hit back with a superseding indictment, a new set of charges that brought the total to 10, including making false statements to the FBI in his initial interrogation. Hutchins and his lawyers saw the response as a strong-arm tactic, punishing Hutchins for refusing to accept their offer of a deal.

After losing a series of motions—including one to dismiss his Las Vegas airport confession as evidence—Hutchins finally took his lawyers' advice and accepted a plea bargain in April 2019. This new deal was arguably worse than the one he'd been offered earlier: After nearly a year and a half of wrangling with prosecutors, they now agreed only to make no recommendation for sentencing. Hutchins would plead guilty to two of the 10 charges, and would face as much as 10 years in prison and a half-million-dollar fine, entirely up to the judge's discretion.

Along with his plea, Hutchins finally offered a public confession on his website—not the full, guts-spilling one he wanted, but a brief, lawyerly statement his attorneys had approved. "I've pleaded guilty to two charges related to writing malware in the years prior to my career in security," he wrote. "I regret these actions and accept full responsibility for my mistakes."

Then he followed up with a more earnest tweet, intended to dispel an easy story to tell about his past immorality: that the sort of whitehat work he'd done was only possible because of his blackhat education—that a hacker's bad actions should be seen as instrumental to his or her later good deeds.

"There's [a] misconception that to be a security expert you must dabble in the dark side," Hutchins wrote. "It's not true. You can learn everything you need to know legally. Stick to the good side."

**On a warm** day in July, Hutchins arrived at a Milwaukee courthouse for his sentencing. Wearing a gray suit, he slipped in two hours early to avoid any press. As he waited with his lawyers in a briefing room, his vision tunneled; he felt that familiar sensation of impending doom begin to creep over him, the one that had loomed periodically at the back of his mind since he first went through amphetamine withdrawal five years earlier. This time, his anxiety wasn't irrational: The rest of his life was, in fact, hanging in the balance. He took a small dose of Xanax and walked through the halls to calm his nerves before the hearing was called to order.

When Judge Stadtmueller entered the court and sat, the 77-year-old seemed shaky, Hutchins remembers, and he spoke in a gravelly, quavering voice. Hutchins still saw Stadtmueller as a wild card: He knew that the judge had presided over only one previous cybercrime sentencing in his career, 20 years earlier. How would he decipher a case as complicated as this one?

But Hutchins remembers feeling his unease evaporate as Stadtmueller began a long soliloquy. It was replaced by a sense of awe.

Stadtmueller began, almost as if reminiscing to himself, by reminding Hutchins that he had been a judge for more than three decades. In that time, he said, he had sentenced 2,200 people. But none were quite like Hutchins. "We see all sides of the human existence, both young, old, career criminals, those like yourself," Stadtmueller began. "And I appreciate the fact that one might view the ignoble conduct that underlies this case as against the backdrop of what some have described as the work of a hero, a true hero. And that is, at the end of the day, what gives this case in particular its incredible uniqueness."

The judge quickly made clear that he saw Hutchins as not just a convicted criminal but as a cybersecurity expert who had "turned the corner" long before he faced justice. Stadtmueller seemed to be weighing the deterrent value of imprisoning Hutchins against the young hacker's genius at fending off malevolent code like WannaCry. "If we don't take the appropriate steps to protect the security of these wonderful technologies that we rely upon each and every day, it has all the potential, as your parents know from your mom's work, to raise incredible havoc," Stadtmueller said, referring obliquely to Janet Hutchins' job with the NHS. "It's going to take individuals like yourself, who have the skill set, even at the tender age of 24 or 25, to come up with solutions." The judge even argued that Hutchins might deserve a full pardon, though the court had no power to grant one.

Then Stadtmueller delivered his conclusion: "There are just too many positives on the other side of the ledger," he said. "The final call in the case of Marcus Hutchins today is a sentence of time served, with a one-year period of supervised release."

Hutchins could hardly believe what he'd just heard: The judge had weighed his good deeds against his bad ones and decided that his moral debt was canceled. After a few more

formalities, the gavel dropped. Hutchins hugged his lawyers and his mother, who had flown in for the hearing. He left the courtroom and paid a $200 administrative fee. And then he walked out onto the street, almost two years since he had first been arrested, a free man.

**After five months** of long phone calls, I arranged to meet Marcus Hutchins in person for the first time at a Starbucks in Venice Beach. I spot his towering mushroom cloud of curls while he's still on the crowded sidewalk. He walks through the door with a broad smile. But I can see that he's still battling an undercurrent of anxiety. He declines a coffee, complaining that he hasn't been sleeping more than a few hours a night.

We walk for the next hours along the beach and the sunny backstreets of Venice, as Hutchins fills in some of the last remaining gaps in his life story. On the boardwalk, he stops periodically to admire the skaters and street performers. This is Hutchins' favorite part of Los Angeles, and he seems to be savoring a last look at it. Despite his sentence of time served, his legal case forced him to overstay his visa, and he's soon likely to be deported back to England. As we walk into Santa Monica, past rows of expensive beach homes, he says his goal is to eventually get back here to LA, which now feels more like home than Devon. "Someday I'd like to be able to live in a house by the ocean like this," he says, "Where I can look out the window and if the waves are good, go right out and surf."

Despite his case's relatively happy ending, Hutchins says he still hasn't been able to shake the lingering feelings of guilt and impending punishment that have hung over his life for years. It still pains him to think of his debt to all the unwitting people who helped him, who donated to his legal fund and defended him, when all he wanted to do was confess.

I point out that perhaps this, now, is that confession. That he's cataloged his deeds and misdeeds over more than 12 hours of interviews; when the results are published—and people reach the end of this article—that account will finally be out in the open. Hutchins' fans and critics alike will see his life laid bare and, like Stadtmueller in his courtroom, they will come to a verdict. Maybe they too will judge him worthy of redemption. And maybe it will give him some closure.

He seems to consider this. "I had hoped it would, but I don't really think so anymore," he says, looking down at the sidewalk. He's come to believe, he explains, that the only way to earn redemption would be to go back and stop all those people from helping him—making sacrifices for him—under false pretenses. "The time when I could have prevented people from doing all that for me has passed."

His motives for confessing are different now, he says. He's told his story less to seek forgiveness than simply to have it told. To put the weight of all those feats and secrets, on both sides of the moral scale, behind him. And to get back to work. "I don't want to be the WannaCry guy or the Kronos guy," he says, looking toward the Malibu hills. "I just want to be someone who can help make things better."

---

**ANDY GREENBERG** *(@a_greenberg) is a senior writer at* WIRED *and the author of the book* Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. A small section of this story is adapted from that book.*

# COLOPHON

## Lifelines that helped get this issue out:

Long chats with old friends; remote movie nights using the Netflix Party browser extension; the countless sidewalk-chalk drawings in my neighborhood; meetings with Erica, 6 feet apart, at the top of the hill; cooking with my friend Emily and the holy spirit (Alison Roman); Nougat the cat; *Fetch the Bolt Cutters*; the many stuffed animals in my neighbors' windows; David Rose on *Schitt's Creek*; stolen lemons; animated movies; ghost pepper chili flakes; a daily 6 pm urban hike; homemade yogurt, extra fat; Duolingo; a new nickname for the dog (Snoozy/Stinky/Sneezy/Sneaky Magoo); Rusty's Southern; rooftop access; drinking an entire French press of coffee per day; *Fortnite* is OK / I play it every day / She says not today; themed Zoom parties; drinking hot cocoa by candlelight; learning how to bake with cannabis (and wishing there were a *Great British Baking Show* episode to guide me); extreme composting; reunification with the cowboy pony Arnie; Camilo's new album; beloved wife and son; level-headed leadership from my state and local authorities.

 Volume 28, No. 6. WIRED (ISSN 1059–1028) is published monthly, except for the combined July/August issue, by Condé Nast, which is a division of Advance Magazine Publishers Inc. Editorial office: 520 Third Street, Ste. 305, San Francisco, CA 94107-1815. Principal office: Condé Nast, 1 World Trade Center, New York, NY 10007. Roger Lynch, Chief Executive Officer; Pamela Drucker Mann, Chief Revenue & Marketing Officer, US; Mike Goss, Chief Financial Officer. Periodicals postage paid at New York, NY, and at additional mailing offices. Canada Post Publications Mail Agreement No.40644503. Canadian Goods and Services Tax Registration No. 123242885 RT0001.

**POSTMASTER:** Send all UAA to CFS (see DMM 707.4.12.5); NONPOSTAL AND MILITARY FACILITIES: Send address corrections to WIRED, PO Box 37617, Boone, IA 50037-0662. For subscriptions, address changes, adjustments, or back issue inquiries: Please write to WIRED, PO Box 37617, Boone, IA 50037-0662, call (800) 769 4733, or email subscriptions@WIRED.com. Please give both new and old addresses as printed on most recent label. First copy of new subscription will be mailed within eight weeks after receipt of order. Address all editorial, business, and production correspondence to WIRED Magazine, 1 World Trade Center, New York, NY 10007. For permissions and reprint requests, please call (212) 630 5656 or fax requests to (212) 630 5883. Visit us online at www.WIRED.com. To subscribe to other Condé Nast magazines on the web, visit www.condenet.com. Occasionally, we make our subscriber list available to carefully screened companies that offer products and services that we believe would interest our readers. If you do not want to receive these offers and/or information, please advise us at PO Box 37617, Boone, IA 50037-0662, or call (800) 769 4733.

IN SIX WORDS, WRITE ABOUT LOVE IN THE TIME OF CORONAVIRUS:

# SO I MARRIED THE DELIVERY MAN.

Hamish Hamish
via Facebook

## Honorable Mentions

LOVE IS SACRIFICING THE LAST PLY.
KRISTOS SAMARAS VIA FACEBOOK

THERE IS AN "US" IN "VIRUS."
ZACHY ALLEC VIA FACEBOOK

FEVERISH DESIRE RAGED BENEATH THE N95.
@SEEKINGFELICITY VIA INSTAGRAM

YOU CAN SNEEZE IN MY ELBOW.
@RALFCHARDON VIA INSTAGRAM

OUR EYES LOCKED IN ZOOM YOGA.
@JABBERWOCKIES VIA INSTAGRAM

SLOWLY, WINDOW AND I BECAME FRIENDS.
@JO.ONTHE.GO VIA INSTAGRAM

"DON'T KISS ME," HE WHISPERED GENTLY.
@ANNA_RCHIST VIA INSTAGRAM

THE CLOTHES CAME OFF; MASKS REMAINED.
@_V.SH VIA INSTAGRAM

CASUAL GETS SERIOUS WAY TOO FAST.
@KRISTINAFMILLER VIA INSTAGRAM

### Your next assignment:

IN SIX WORDS, IMAGINE AN APOCALYPSE WITH A HAPPY ENDING.

Each month we publish a six-word story—and it could be written by you. Submit your story on Facebook, Twitter, or Instagram, along with **#WIREDBACKPAGE**. We'll pick one to illustrate here.





ILLUSTRATION / MAXIME MOUYSSET


# Why settle for average? Earn a savings rate 5X the national average.

Open a new savings account in about 5 minutes and earn 5X the national average.

**This is Banking Reimagined®**

Capital One®

What's in your wallet?®