MIT Technology Review

The technonationalism issue

Volume 123 Number 5
Sept/Oct 2020
USD $9.99 CAD $10.99

Power

Who has it, who wants it, and who's losing it

0 74808 01308 1 10


Can the weather predict you?

WE WERE CURIOUS ABOUT THAT TOO

Because you are our greatest curiosity. And we noticed the temperature of your body is constantly fluctuating from one moment to the next. So we engineered the available Climate Concierge with as many as sixteen infrared sensors to monitor your ever-changing temperature, then react with up to twenty air vents, heated and ventilated seats, and a heated steering wheel. Keeping you comfortable, automatically. And not just the driver, but also your passengers. What amazing ideas will you inspire next? Discover the answer at lexus.com/curiosity.

CLIMATE
CONCIERGE

LEXUS
EXPERIENCE AMAZING

Options shown. ©2020 Lexus

In the last few decades, the received wisdom among global elites has been that technology tends to make the world flatter, smaller, more open, and more equal. This now seems increasingly false, or at least simplistic. Countries are vying for dominance in technologies that could give them a strategic advantage: communications, energy, AI, surveillance, agricultural tech, cybersecurity, military tech … and now, amidst a global pandemic, medicine and manufacturing. The urge for nations to amass technological prowess and use it as an instrument of geopolitical power is what we mean by technonationalism. The thesis of this issue is that the post–Cold War order was already splintering, and covid-19 is finishing the job.

The biggest driving force in this trend is China's rise as a tech superpower and the US's consequent belligerence as its supremacy comes under threat. Mara Hvistendahl looks at how US law enforcement has gotten mixed up in the rivalry between Western and Chinese agriculture giants (page 58), and at how China's government sweeps up data all around the world (page 56). Paradoxically, Karen Hao explains, even as the Chinese government amps up surveillance of its citizens, it is strengthening laws protecting their privacy as consumers (page 50). And James Temple shows how central China has become to renewable-energy technology (page 22).

As Steven Feldstein argues in the opening essay (page 10), technonationalism plays a part in the strengthening of other autocracies too. Evan Gershkovich writes about Russian tech giant Yandex's uneasy relationship with the Kremlin (page 38). Sonia Faleiro looks at the Indian government's attempts to control information by simply shutting down the internet for periods of time (page 44). Richard Kemeny reports on how Brazil is becoming a surveillance state (page 34). Patrick Howell O'Neill profiles Israeli spyware company NSO, which has quietly built up its fortune by helping governments around the world snoop on people (page 62).

Covid-19 is intensifying technonationalist tendencies in part by laying bare the differences between countries that are handling the pandemic well and those that aren't. Rowan Moore Gerety (page 68) delves into why America's once-vibrant manufacturing sector, which switched nimbly to a war footing in the 1940s, now can't churn out enough masks and equipment to keep citizens safe. Antonio Regalado examines the international race to find a vaccine (page 28) and interviews Larry Corey, who is in charge of the Trump administration's vaccine trials (page 31). Krithika Varagur talks to people on the pandemic's front lines in several of the countries that have done best against the disease (page 14). Kati Krause and Patrick Leger take a closer look at Germany—a federal system like the US, but one where clear leadership from the top has produced a very different outcome (page 24).

IAN ALLEN

Gideon Lichfield is editor in chief of MIT Technology Review.

Finally, Christine Rosen reviews a book by historian Jill Lepore on the forgotten history of "people analytics," a discipline that was born of governments' ambitions to predict and control their populations (page 78). Konstantin Kakaes sums up five books on the complicated relationship between governments and technology (page 76). And we round off with a thought-provoking piece of fiction from Fatin Abbas (page 82).

My guess is that while we wait for a vaccine or treatment, the international contrasts will only grow more stark. In some countries, economies are already picking back up and life is returning to some semblance of normalcy. In others, there is decline, depression, uncertainty, and a feeling of being trapped in the horror of now. Technology will continue to be one more means by which countries seek advantage. As nation-states reassert their power in the world, the stories in this issue will help you understand the nature and limits of what they can do.

MIT Technology Review

ATTENTION MAGAZINE SUBSCRIBER!

We launched a new podcast just for you.

Deep Tech (hosted by Gideon Lichfield) brings you closer to the people, places, and ideas featured in the pages of MIT Technology Review magazine.

Listen at
technologyreview.com/DeepTech

THE TECHNONATIONALISM ISSUE

Introduction

Fiction

The back page

Cover illustration by Selman Design

MIT Technology Review

TECH NEWS YOU NEED. WHEN YOU WANT IT. WHERE YOU WANT IT.

Get our newsletters delivered to your inbox.

The Download
Navigate the world of tech news.

The Airlock
A deep dive into off-world storylines.

The Algorithm
(Subscriber-only)
Artificial intelligence, demystified.

Coronavirus Tech Report
How Covid-19 is changing our world.

Weekend Reads
Technology in perspective.

Stay in the know:
technologyreview.com/inbox

Editorial

Editor in chief
Gideon Lichfield

Executive editor
Michael Reilly

Editor at large
David Rotman

News editor
Niall Firth

Managing editor
Timothy Maher

Commissioning editors
Bobbie Johnson
Konstantin Kakaes
Amy Nordrum

Senior editor, MIT News
Alice Dragoon

Senior editor, biomedicine
Antonio Regalado

Senior editor, energy
James Temple

Senior editor, digital culture
Abby Ohlheiser

Senior editor, cybersecurity
Patrick Howell O'Neill

Senior editor, AI
Will Douglas Heaven

Senior editor, podcasts and live journalism
Jennifer Strong

Senior reporters
Tanya Basu (humans and technology)
Karen Hao (AI)

Reporters
Charlotte Jee (news)
Neel Patel (space)

Copy chief
Linda Lowenthal

Social media editor
Benji Rosen

Editorial research manager
Tate Ryan-Mosley

Administrative assistant
Andrea Siegel

Proofreader
Barbara Wallraff

Design

Chief creative officer
Eric Mongeon

Art director
Emily Luong

Marketing and events designer
Kyle Thomas Hemingway

Photo editor
Stephanie Arnett

Corporate

Chief executive officer and publisher
Elizabeth Bramson-Boudreau

Assistant to the CEO
Katie McLean

Human resources manager
James Wall

Manager of information technology
Colby Wheeler

Office manager
Linda Cardinal

Product development

Chief technology officer
Drake Martinet

Director of software engineering
Molly Frey

Head of product
Mariya Sitnova

Senior product designer
Jon Akland

Director of analytics
Michelle Bellettiere

Senior project manager
Allison Chase

Senior software engineer
Jason Lewicki

Software engineer
Jack Burns

Events

Senior vice president, events and strategic partnerships
Amy Lammers

Director of event content and experiences
Brian Bryson

Head of international and custom events
Marcy Rizzo

Event content producer
Erin Underwood

Associate director of events
Nicole Silva

Event partnership coordinator
Madeleine Frasca

Events associate
Bo Richardson

Finance

Finance director
Enejda Xheblati

General ledger manager
Olivia Male

Accountant
Letitia Trecartin

Consumer marketing

Senior vice president, marketing and consumer revenue
Doreen Adger

Director of analytics systems
Tom Russell

Director of audience development
Rosemary Kelly

Director of digital marketing
Emily Baillieul

Product marketing manager
Amanda Saeli

Assistant consumer marketing manager
Caroline da Cunha

Circulation and print production manager
Tim Borton

Email marketing specialist
Tuong-Chau Cai

Advertising sales

Vice president, sales and brand partnerships
Andrew Hendler
andrew.hendler@technologyreview.com
646-520-6981

Executive director, brand partnerships
Marii Sebahar
marii@technologyreview.com
415-416-9140

Executive director, brand partnerships
Kristin Ingram
kristin.ingram@technologyreview.com
415-509-1910

Senior director, brand partnerships
Whelan Mahoney
whelan@technologyreview.com
201-417-0928

Director, brand partnerships
Debbie Hanley
debbie.hanley@technologyreview.com
214-282-2727

Director, brand partnerships
Ian Keller
ian.keller@technologyreview.com
203-858-3396

Business development sales manager
Ken Collina
ken.collina@technologyreview.com
617-475-8004

Digital sales strategy manager
Casey Sullivan
casey.sullivan@technologyreview.com
617-475-8066

Media kit
www.technologyreview.com/media

MIT Technology Review Insights and international

Vice president, Insights and international
Nicola Crepaldi

Director of custom content, US
Laurel Ruma

Senior project manager
Martha Leibs

Content manager
Jason Sparapani

Client services manager, licensing and syndication
Ted Hu

Director of custom content, international
Claire Beatty

Director of business development, Asia
Marcus Ulvne

Board of directors

Martin A. Schmidt, Chair
Peter J. Caruso II, Esq.
Whitney Espich
Jerome I. Friedman
David Schmittlein
Glen Shor
Alan Spoon

Customer service and subscription inquiries

National
877-479-6505

International
847-559-7313

Email
customer-service@technologyreview.com

Web
www.technologyreview.com/customerservice

MIT Records (alums only)
617-253-8270

Reprints
techreview@wrightsmedia.com
877-652-5295

Licensing and permissions
licensing@technologyreview.com

MIT Technology Review

One Main Street
13th Floor
Cambridge, MA 02142
617-475-8000

The mission of MIT Technology Review is to make technology a greater force for good by bringing about better-informed, more conscious technology decisions through authoritative, influential, and trustworthy journalism.

Technology Review, Inc., is an independent nonprofit 501(c)(3) corporation wholly owned by MIT; the views expressed in our publications and at our events are not always shared by the Institute.

Our insights. Your success.

Amplify your brand. Retain customers. Turn thought leadership into results. Partner with MIT Technology Review Insights. Join us and other smart companies to craft custom research, savvy articles, compelling visualizations, and more.

MIT Technology Review Insights

Artificial intelligence

The global AI agenda
Report in association with Genesys and Philips

The AI effect: How artificial intelligence is making health care more human
Survey and dynamic website in association with GE Healthcare

AI in health care: Capacity, capability, and a future of active health in Asia
Report in association with Baidu

Digital transformation

Digital platforms drive business success
Report in association with SAP

How to crack the skills dilemma
Report in association with Citrix

Marissa Mayer on the rise of women technology leaders
Podcast in association with (ISC)²

Don't get left behind: The business risk and cost of technology obsolescence
Report in association with Oracle

Data and analytics

DataOps and the future of data management
Report in association with Hitachi Vantara

Excelling in the new data economy
Report in association with Intel

Breaking the marketing mold with machine learning
Survey and report in association with Google

For data-savvy marketers, there's a new keyword: Intent
Online article in association with Google

Cybersecurity

Leading with a security-first mentality
Podcast in association with Microsoft Security

Cybersecurity in 2020: The rise of the CISO
Podcast in association with Microsoft Security

An innovation war: Cybersecurity vs. cybercrime
Report in association with HPE

Infrastructure and cloud

Supercharging with converged infrastructure
Report in association with Hitachi Vantara

Anticipating cloud work's most common side effects
Report in association with Citrix

From cloud to the edge: On-device artificial intelligence boosts performance
Online article in association with Arm

IoT, 5G, and blockchain

The 5G operator: Platforms, partnerships, and IT strategies for monetizing 5G
Report in association with Ericsson

Smaller, smarter, healthier
Report in association with Medtronic

Technology innovations: The future of AI and blockchain
Infographic in association with EY

For more information, please contact Andrew Hendler, Vice President of Sales, andrew.hendler@technologyreview.com.

MIT Technology Review

EmTech

ONLINE CONFERENCE

Essential technology

Geoffrey Hinton, one of the "**Godfathers of AI**," shares his **vision for AI** as it weaves itself into the fabric of our lives and businesses.

LEADING WIT

Reset, rethink, rebuild.

Our world has changed, and we must chart a new path forward through innovation and leadership. We need to reassess the underpinnings of our digital world – AI, biotech, cloud, and cybersecurity – and apply pioneering ideas, from experts and each other.

The big picture

Marc Benioff, **CEO of Salesforce**, gives his take on technology, climate, philanthropy, contact tracing, and **leading with innovation**.

Innovators under 35

Meet pioneers like **Inioluwa Deborah Raji**, whose research on racial bias in data for facial recognition systems is forcing companies to change their ways.

The tech ecosystem

Megan Smith, CEO of shift7 and former US CTO, talks about what **sustainable**, **equitable innovation** will take in today's changed world.

H INNOVATION

What's next?

Astro Teller, Captain of Moonshots at Alphabet's X, talks about his passion to solve the **world's biggest problems**.

MIT Technology Review's flagship event on emerging technology and trends

October 19–22, 2020

Subscribers save 10% with discount code PRINTSO20 at

EmTechMIT.com/RegisterNow

THE VIRUS THAT SPLIT THE WORLD

Covid-19 has accelerated two global trends that will shape the world in decades to come.

By **STEVEN FELDSTEIN**

Illustration by Pablo Delcan

By late July, most rich countries had brought their covid-19 infection rates down far below their initial peaks. In the US, however, the number of daily new cases was at record highs and still climbing.

The crisis has badly damaged global opinion about American competence. A report in June from survey company Dalia Research revealed a broad consensus that China has handled covid-19 far better than the US. Of the 53 countries surveyed, ranging from Denmark to Iran, only two thought the US had responded better than China: Japan and the US itself. The Dalia survey also found that across the board, public perceptions of US global influence have markedly deteriorated. Nearly as many people believe that America's impact on democracy has been negative as positive. People in stalwart democracies such as Canada, Germany, and the UK are particularly critical.

America's abject failure to deal adequately with the biggest global health emergency in a century has prompted some experts to argue that the pandemic may serve as a geopolitical inflection point. Kurt Campbell and Rush Doshi wrote in March in Foreign Affairs that just as a bungled intervention in the Suez crisis precipitated the end of the British empire, "the coronavirus pandemic could mark a 'Suez moment'" for the US, as China "position[s] itself as the global leader in pandemic response."

But even if the effects are not quite that drastic, they will be profound. The US's declining stature in the wake of the pandemic is accelerating two global political trends that have emerged in the last five years.

First, rising tensions between the US and China threaten to initiate a new arms race and a return of great-power rivalry. Second, from Turkey to Brazil to Hungary to Poland, an increasing number of countries are undergoing "autocratization," centralizing power and restricting political freedoms—putting an end to the post–Cold War waves of democratization that ushered in new freedoms and rights for hundreds of millions of people. Taken together, these two trends will make for a more divided and uncertain world.

A global digital divide

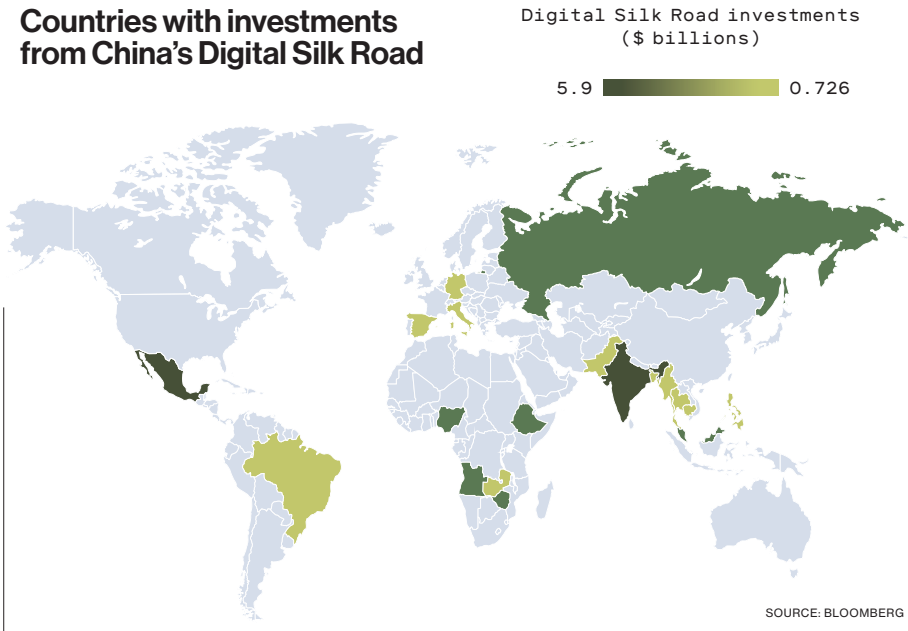
One visible manifestation of both the decline of US power and the resurgence of autocracy is the fragmenting of the global digital ecosystem. Since Google pulled out of China in 2010 over the government's censorship of search results, China has cultivated a walled garden of applications primarily for use by its citizens. While the decoupling isn't total—the Android and iOS mobile operating systems are prevalent, and programming languages like Java and Python are widely used—most Chinese never go on Twitter, Facebook, YouTube, Amazon, PayPal, or many other platforms, but instead use their local alternatives.

This fragmentation is part of a larger normative battle. China has been joined by Russia, Iran, and other autocratic regimes in promoting cyber sovereignty—the idea that countries should set their own rules on how their citizens use the internet. In Russia, the government is planning to implement a "sovereign internet," a self-contained, centrally controlled system that would allow the country to cut itself off from the global internet entirely (see "Yandex's balancing act," page 38). By contrast, while the US and Europe differ on the nature and importance of privacy, the limits of free speech, and the right way to regulate Big Tech, there is broad agreement that the internet should be open and interoperable.

These trends mean that increasingly, where large countries relied on size, military force, or economic influence, they now also view technology (and not just the military kind) as one of the keys to sustaining and extending their power. This paradigm, known as "technonationalism," rests on two crucial assumptions: first, that an early technological lead gives countries a first-mover advantage, and second, that dominance in certain technologies, such as artificial intelligence, gives them an edge in other fields. These assumptions do not need to be true to be influential. Under their logic, no country can afford to let competitors pull ahead.

An illustration of this was the US Commerce Department's decision in October 2019 to add 28 Chinese companies to its "entity list" of firms subject to

Countries with investments from China's Digital Silk Road



SOURCE: BLOOMBERG

trade restrictions. They include most of the leading Chinese AI firms, including iFlytek, SenseTime, and Megvii. Ostensibly, they were added as punishment for facilitating shocking human rights abuses against Muslim Uighurs in Xinjiang. But a secondary result was to hinder them from competing with US companies.

More recently, in May 2020, the White House released a strategy document accusing Chinese authorities of exploiting "the free and open rules-based order" and attempting to "reshape the international system in its favor." It calls for renewed prosecutions of Chinese trade-secret theft and a stronger process for preventing Chinese companies from acquiring advanced technologies, such as "hypersonics, quantum computing, artificial intelligence, and biotechnology." Subsequently, US officials tightened restrictions against Chinese electronics giant Huawei by blocking the company from using US technology or machinery to manufacture its chips. In late July, the Trump administration abruptly ordered China to close its consulate in Houston, alleging that it was a hub for industrial espionage (see "Hacker, G-man, seed thief, spy," page 58). China retaliated by closing the US consulate in Chengdu.

China, meanwhile, continues to lock out international companies that refuse to play by its rules—such as agreeing to censor search engine results, provide authorities with data on users, or hand over software source code and other proprietary data. It has also ramped up efforts to cultivate "mass innovation" and increase subsidies to strategic sectors such as AI, semiconductor chips, and aerospace through programs like "Made in China 2025."

China also promotes its companies and technologies to many countries in direct competition with US, European, and other firms. Beginning in 2015, Chinese officials began touting the "Digital Silk Road," focused on internet connectivity, artificial intelligence, the digital economy, telecommunications, smart cities, and cloud computing. This has led to investments in at least 20 countries, totaling nearly $40 billion, according to a 2019 estimate by the RWR Advisory Group, a consultancy.

The Trump administration's attempts to disentangle US technology supply chains from China and its moratorium on new visas for skilled foreign workers, announced in June and extended through December, only serve to help China. A report by Ishan Banerjee and Matt Sheehan published by the Paulson Institute, a think tank in Chicago, found that while Chinese-educated AI researchers produced nearly one-third of all papers accepted at the NeurIPS conference, the leading AI research meeting in the world, most Chinese researchers study, live, and work in the United States. If they are forced to leave, such talent cannot be easily replaced.

If Joe Biden is elected president, his administration will no doubt reconsider some of these policies. Jake Sullivan, a Biden campaign advisor, recently said at an event at the Carnegie Endowment for International Peace (where I am a fellow) that there should be "less focus on trying to slow China down and more on running faster ourselves." But whatever Biden does, the competition to determine international norms and standards for critical technologies will continue.

The geopolitics of repression

Other governments are also using technology to advance their political agendas. Even before the covid-19 crisis, the world was in the midst of an autocratic resurgence. Researchers from the Varieties of Democracy project estimate that 2.6 billion people, or 35% of the world's population, are having their political liberties curtailed.

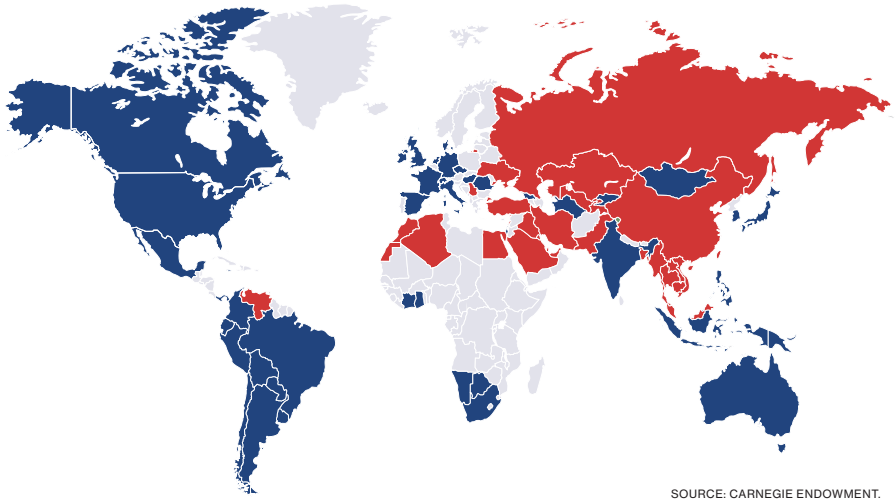
Authoritarians are using a raft of digital technologies to counter dissent, maintain political control, and stay in power. In my prior research and in an upcoming book, I document how cities in Kenya, Mexico, and Malaysia employ Chinese AI-powered technology to keep watch over citizens; how spyware from Israeli and US sources helps intelligence operatives in Saudi Arabia, the United Arab Emirates, and Egypt monitor dissent and track opposition figures; and how censorship and disinformation campaigns enable authorities in Thailand and Pakistan to tamp down criticism and flood digital channels with pro-government narratives.

Autocratic regimes are far more likely to use these instruments for repression, but democracies sometimes use them to curb civil rights too. In the United States, for example, the advocacy group Freedom House observes, police have used technologies such as drones, facial recognition, and social-media surveillance in response to escalating Black Lives Matter protests.

The pandemic has accelerated this attrition of individual liberties. Data collected by Samuel Woodhams of Top10VPN, a digital privacy group, shows that as of July 2020, 50 countries had introduced contact tracing apps, 35 had adopted alternative digital tracking measures, 11 had implemented advanced physical surveillance technologies, and 18 had imposed censorship related to covid-19. Many of the countries using these techniques are democracies.

A big problem is that governments are rushing out health surveillance technology without proper vetting or oversight. Bahrain, Kuwait, and Norway all launched intrusive covid-19 tracing apps that "actively carry out live or near-live tracking of users' locations by frequently uploading GPS coordinates to a central server," Amnesty International reported in June. The report caused Norway

Countries that possess public surveillance capabilities powered by big data and AI



SOURCE: CARNEGIE ENDOWMENT.

to suspend its app's rollout; Bahrain and Kuwait have not.

Of course, digital technology isn't responsible for authoritarianism's resurgence, but it gives crucial advantages to unsavory regimes. This illiberal assault is putting inordinate pressure on the liberal international order and the institutions that uphold it, including the UN, NATO, the World Health Organization, the World Trade Organization, and others.

China and Russia stand to gain the most from this. Indeed, some experts argue that they have directly pursued a "digital authoritarianism" strategy: providing powerful technology to help illiberal leaders entrench their regimes, thereby creating an autocratic alternative to the liberal international order.

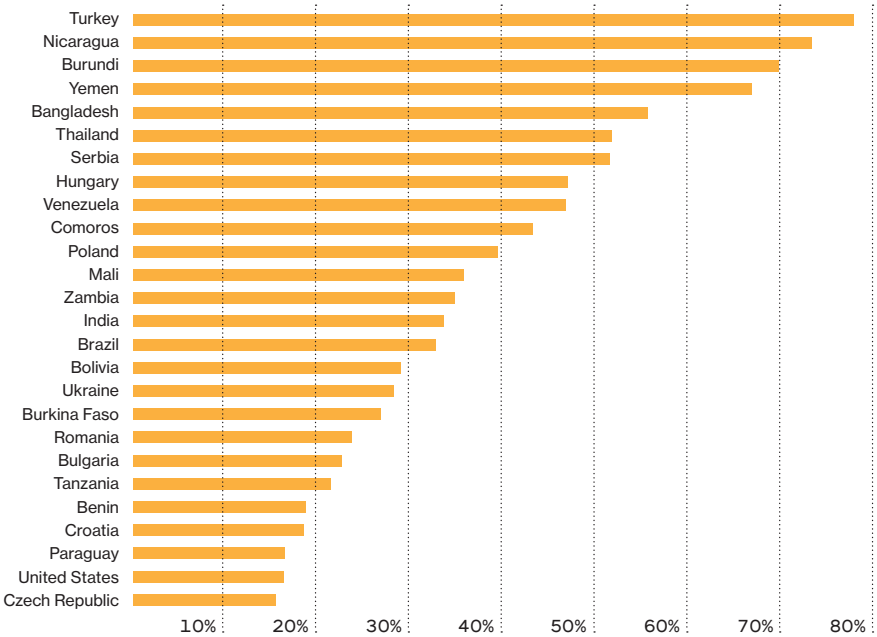
My own research suggests that most of these regimes would pursue antidemocratic digital strategies even without Russia's and China's help. All the same, there is reason to worry about the growing global spread of Chinese technology such as Huawei 5G networks, Transsion mobile phones, and WeChat for e-commerce and communication. Not only does this increase global reliance on Chinese technology, thereby enhancing China's influence, but many products, such as WeChat's social app or Alipay Health Code (which classifies users' health status and determines whether they are allowed to travel or enter certain public spaces), are designed to facilitate government surveillance and censorship. As Christopher Walker, Shanthi Kalathil, and Jessica Ludwig wrote this year in the Journal of Democracy, "The CCP [Chinese Communist Party] has been forging an increasingly seamless synthesis combining consumer convenience, surveillance, and censorship. This model is exemplified by such all-encompassing platforms as WeChat … which includes politically based content restrictions and lends itself to surveillance." (See also the interview with Samantha Hoffman on page 56.)

Of course, technologies are often two-edged swords. Digital tools help civic movements, journalists, and political challengers. The ability of social-media networks to rapidly mobilize citizens and swell mass protests is a potent threat that no regime has fully neutralized.

It's also worth remembering that while the US-China rivalry can dominate discussions about the future of technology, it's not the only thing determining where trends are headed. The European Union, for example, is increasingly staking out its own independent policy positions. It's emphasizing privacy, accountability for big tech firms, and transparency for big data and AI. India, Brazil, South Africa, Nigeria, and Indonesia are all deciding whether to try to carve out their own digital agendas or to act more as fence-sitters, playing China, the US, and the EU against one another.

Though commentators like Ian Bremmer of the Eurasia Group warn of a "great decoupling" between the US and China, with dire consequences for technology, talk of a new bipolar Cold War is overblown. There are too many new players and too many variables to assume that two superpowers will monopolize the rules of technology for the foreseeable future. Instead, we are likely to witness increased splintering as fresh ideas come to the fore, new platforms gain followings, and more people get online for the first time. A multipolar world with new, diverse sources of ideas, innovation, regulation, and geopolitical influence may not be such a bad thing at all.

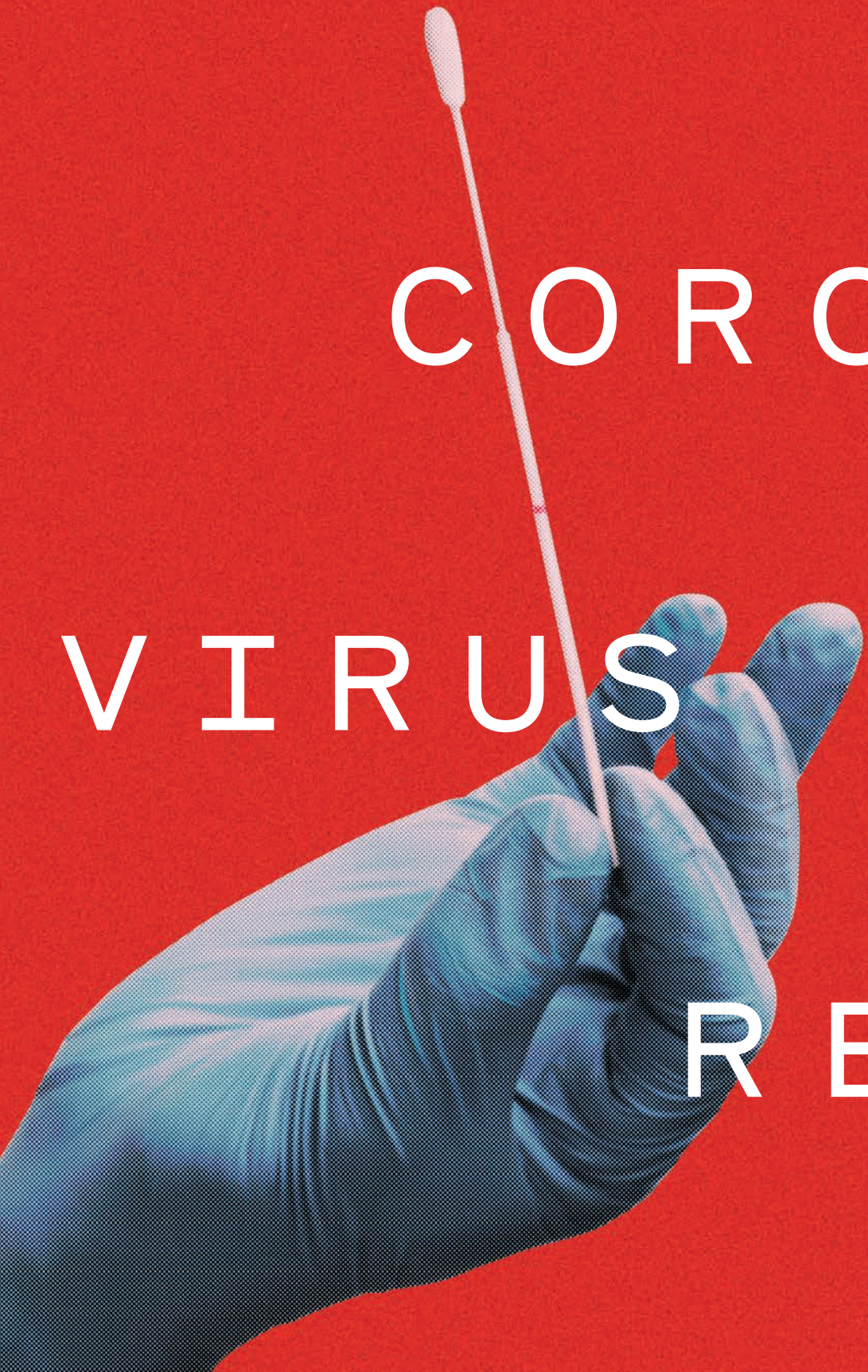
Countries with the biggest increases in degree of autocracy from 2009 to 2019, from the Varieties of Democracy project



MICHAEL COPPEDGE, ET AL. HTTPS://DOI.ORG/10.23696/VDEMDS20

Steven Feldstein is a senior fellow at the Carnegie Endowment for International Peace.

THE CORONA VIRUS RESP



ONDERS

Why have some countries fared so much better than others in the face of the pandemic? This summer, MIT Technology Review spoke with people on the front lines of the response in five countries that have tackled covid-19 exceptionally well: Mongolia, Germany, Liberia, Vietnam, and Uruguay.

These countries have nothing obvious in common. They run the gamut in terms of wealth, size, population, and style of government. What they shared was a swift, coordinated, apolitical government response. Where that has been lacking, no amount of scientific expertise, technical knowhow, or wealth can prevent disaster, as the United States all too grimly shows.

We also spoke with an official from Sweden, which has taken a different approach from its neighbors by deliberately avoiding complete lockdowns—a strategy with both virtues and defects. But even the most successful responders agreed, as they reflected on the last six months, that they face a long road ahead.

Interviews have been condensed and edited for clarity.

By Krithika Varagur

MONGOLIA

Mongolia shares the world's longest land border with China, but its early and highly centralized pandemic response has been so effective that not a single person in the landlocked country has died from covid-19. A former army colonel turned public health official explains how Mongolia enacted its extensive quarantine and testing regime under a state of emergency.

COVID DEATHS AS OF JULY 20, 2020:

0

DAVAADORJ RENDOO

EPIDEMIOLOGIST, NATIONAL CENTER FOR PUBLIC HEALTH

ULAANBAATAR, MONGOLIA

We first heard about a new virus spreading in China around New Year's Eve. On January 10, we issued our first public advisory, telling everyone in Mongolia to wear a mask.

Here's the thing: we don't actually have a great public health system. That's why our administrators were so afraid of covid-19. We don't have many respirators, for example. We were really afraid that if we got community transmission even once, it would become a disaster for us. What was in everyone's head was to be prepared before the spread. Another reason we were so keen to protect the community is because we have the world's longest land border with China—2,880 miles [4,600 kilometers]—as well as continuous human flow for education and business from China to Mongolia.

Mongolia is a big country with a sparse population, about 3.2 million people. Because our country has a very harsh, dry, and cold climate, every year from November to February we have an awful flu season, and the Ministry of Health always encourages people to practice good hygiene and wash hands, especially young children. So many of our suggestions were not new.

We have been doing tests since January. We even started randomly screening pneumonia patients for covid-19 but never found a patient. We got the majority of our test kits from the World Health Organization (WHO), including rapid tests, and were able to scale it up pretty quickly.

In February, we started flying Mongolians living abroad back home and testing them.

We did not detect a single domestic case until March 9. One French national working in the southern province of Dornogovi was discovered to have had coronavirus. Since that day, the Ministry of Health has been conducting daily situation briefings to talk about how many cases were imported, what the high-risk areas are. After that case was announced, people became even more obedient to our directives. But we were so ready for this case. We really had enough time to prepare.

For that French national, we undertook very extensive contact tracing and identified 120 people who had had some contact with him. This is not the first time we have done contact tracing; it has been part of the mandate of the National Center of Communicable Diseases since its inception. We do this for all kinds of disease, including sexually transmitted diseases.

We also opened a dedicated, 24-hour covid hotline. People were getting all kinds of wrong information from social media. One big hoax was that because Mongolians eat very healthily and live in traditional nomadic lifestyles, we would not get the virus and had a "natural immunity." Another big one was that because it is cold and dry, the virus does not survive here, and it only survives in warm and wet climates. Today, even the majority of herders and nomadic people have satellite TV with solar energy, so they can still access information.

One side effect of this lockdown has been a significant reduction in cases of seasonal flu, pneumonia (a very serious problem every year), and foodborne and digestive illness.

Every day, we are still concerned, but our people are getting less worried. It's summer now; the weather is getting nicer. People are going for picnics, riding horses. We have set up a lot of temperature checks at recreation spots in the countryside. Almost all the public spaces, starting with the malls and pharmacies, still require masks. But we realize that in the rural areas, wearing a mask every day is not possible.

We don't know how long the state of emergency will last. Some of our highest officials have said we will close our borders indefinitely. We cannot take anything for granted. In Japan, they lifted restrictions and the virus came back. Until the end of this summer, we are not easing quarantine at all. But schools will have to start in September. What we still recommend every day to the public is to stay ready, because community transmission might be just around the corner.

TS.NOMIN-ERDENE, RESEARCHER, DEPARTMENT OF EPIDEMIOLOGY AND EMERGENCY OPERATIONS, NCPH

GERMANY

The government-run Robert Koch Institute for public health research in Berlin has been at the forefront of the country's robust pandemic response, leading the search for a vaccine and racing to push out vast stocks of tests. A career epidemiologist at the institute explains the challenges of reopening, communicating risk, and contact tracing in the German context.

BERLIN, GERMANY

COVID DEATHS AS OF JULY 20, 2020:

9,086

ROBERT KOCH INSTITUTE

LARS SCHAADE

VICE PRESIDENT, ROBERT KOCH INSTITUTE

The first confirmed case in Germany was not really the first suspected case. We had several suspected cases earlier on, which were all negative, but then we were not so surprised that one day, on January 27 in Munich, one of these cases proved positive. By that time, we already had several important things in place: our case definition, our test criteria, our hygiene and infection prevention and control recommendations, and our recommendations concerning contact tracing.

Our value of "R," or the reproduction number of the virus, which Chancellor Angela Merkel has used frequently in public addresses, is still something we calculate and report on a daily basis. Of course now we have far fewer cases than in March, so any outbreak at this point has a direct impact on our reproduction numbers. It's up and down, but it's around one now (meaning every patient infects on average one other person). We currently [as of June 18] have a median case number of 300 to 350 cases each day, which is low.

Of course it's possible there will be a second wave. And our main objective then is to keep the incidence of new cases as low as possible. We are already trying to do sensitive testing of anyone with any respiratory disease and in any symptomatic patients that belong to a cluster, or who live in certain risky surroundings like nursing homes. And there is the political commitment that if necessary—if a county has cases above a certain threshold—they will have to reintroduce local lockdown measures.

We are also trying to prepare for a vaccine. In June, the Health Ministry formed an alliance with France, Italy, and the Netherlands and signed a contract for preorders of 300 million doses of a coronavirus vaccine currently in development.

One of the main pillars in our attempt to keep numbers low was intense contact tracing. As of June, we have a new mobile app. But before that, we did contact tracing the traditional way—ever since this started in January until the peak, when we had six or seven thousand cases each day. We tried to convince local health authorities that they have to do this contact tracing work, even if the numbers are high, because it's important to break any infection train in this outbreak. Very early on, we discussed the possibility of a contact tracing app, and of course it was on our mind to have a GPS tracking system. But also very early on, the data protection people called us and told us that this would never happen. Then we looked for an alternative, and it became clear that Bluetooth technology could offer one. [Editor's note: GPS-based contact tracing apps track a phone's location at all times, while Bluetooth-based ones just track proximity to other phones without necessarily revealing a person's movements.] We were very much in favor of the centralized system at first, because it would give us the opportunity to have an overview of what exactly happened. But balancing the concerns of data protection, we settled on this decentralized system, which has one main disadvantage: we don't know what happened in a specific case. (As in, it doesn't make it into our server.) So we have to still supplement it with additional surveillance and investigations, but the data protection people are happy with the solution.

> **They have to do this contact tracing work, even if the numbers are high.**

The coronavirus crisis has already lasted six months—a very long time for crisis management, even though we have dealt with pandemics in Germany in the past. Everyone at the institute is pretty tired right now.

LIBERIA

Covid-19 was the second pandemic of the decade for Liberia, which was devastated by Ebola just five years ago. A US-trained public health officer who served in both emergencies explains how some institutional knowledge was carried over, as well as how the virus entered the country despite considerable precautions.

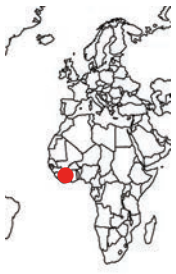
COVID DEATHS AS OF JULY 20, 2020:

70

FRANCIS KATEH

DEPUTY MINISTER OF HEALTH AND CHIEF MEDICAL OFFICER FOR LIBERIA

MONROVIA, LIBERIA



The moment we heard that there was this new disease in China, we knew there was no chance that we wouldn't get the disease in Liberia. The question was just: When is it coming? So we had to prepare.

In January, Liberia became one of the first countries in the world to start screening for covid-19 at airports, based on our experience from Ebola and our understanding that our health system would not be as strong as anticipated. Those coming from a highly infected country at that time (anywhere with over 200 recorded cases) would have to be quarantined in our Precautionary Observation Center for 14 days upon arrival in the country. These were in hotels, and we monitored the travelers two to three times a day.

Our initial strategy was to prevent covid from coming into Liberia. We knew that it would have to come through the airport. So we thought, if we can proactively get somebody who comes in from a high-risk area and quickly isolate them, and if they come down with the virus, we can quickly get their sample and get it tested. And if it were positive, you would not have to go through a major round of contact tracing, since this person was being isolated.

I have served in public health both during the Liberian Civil War and later during Hurricane Katrina in the US. I was the county health officer in Anson County, North Carolina. I learned a lot about disaster preparedness when I went to help out in Louisiana.

During the Ebola crisis [of 2014-2015] in Liberia, I was the deputy incident manager, in charge of medical response and planning. Once covid-19 arrived, we started immediately to put the lessons we'd learned from Ebola into practice, because people were still aware of them: basic preventive measures like handwashing and basic social distancing. But when people begin to realize that covid-19 is not as severe as Ebola was, doubts began to come in. Then the hoaxes began.

> **The biggest thing we are fighting is the idea that the coronavirus is not real, that the government and international organizations are doing this to make money for themselves.**

The biggest thing we are fighting is the idea that the coronavirus is not real, that the government and international organizations are doing this to make money for themselves. Another is the fact that even those who have been tested positive, [if they] don't show any major signs, sometimes don't believe that they have it. So if you are at the treatment unit and you communicate with your relatives and family members that "Oh, there is nothing happening to me," people don't think it's serious. The difference between covid and Ebola is that with Ebola I could see with my own eyes, even before the test result came, that a person had Ebola, because an infected person is usually not able to carry their own body weight. And when we did active case searches, it was very, very easy to quickly identify those who may have Ebola. For covid, there are people who are basically completely asymptomatic. We have begun to educate them that "Look, it's not just you being treated. What we are doing is basically to isolate you from your relatives so that you can't get them infected."

When covid started, we had only one ventilator in the country, but now we have three, thanks to donations. But we have been lucky thus far that we have not made use of our ventilators. What this means, of course, is that the cases in our country so far have not been too severe. But that can change.

ZOOM DOSSO/AFP VIA GETTY IMAGES

URUGUAY

Uruguay has been a rare bright spot in coronavirus-ravaged South America, thanks to a highly developed research infrastructure, a tradition of at-home medical care, and a strong public health system. Two key advisors to the government's pandemic response team explain how they scaled up their tests so fast and why they are now encouraging people to go outside more.

The first cases in Uruguay were confirmed on March 13, and the national working group that we convened of about 60 people met with the president on April 16. There were two main arms, one in health and one in data science and modeling.

The number of cases never really built up to the point where we had no control. You could almost track our epidemic through five or six distinct outbreaks that we've had, all with around 50 to 60 cases, and they're all basically isolated. The most recent outbreak was in a province called Treinta y Tres that is close to the Brazilian border, and this was the second outbreak we had of Brazilian origin. That border is technically closed, but there are some border towns which are binational, so it's hard to enforce. Actually, the main street in one of these towns is the border. So people will just cross freely. You cannot really be as locked down as we would like in those border towns.

Right now there's a reasonably good capability of PCR testing. [Editor's note: polymerase chain reaction, or PCR, is the standard method of identifying a virus from its genetic material.] We have built up enough capacity that if there's any outbreak, we can do contact tracing not just of the immediate contacts, but even second-order contacts. We've been doing that, plus some random testing of people around outbreak hot spots. As for the people who actually do the field testing, we have been relying on the existing capacity of the health ministry in terms of infectious diseases. We are used to dealing with other kinds of epidemics, like dengue, and so far we haven't had a high enough number of cases to involve people outside their expertise. But it's not really high tech. These guys are doing the job as it has long been done: lots of phone calls.

There was an early scientific response even before the disease arrived in the country in terms of interacting with research networks around the world and sharing reagents with different universities and centers abroad, such as the University of Hong Kong and the Pasteur Institute in France, to generate molecular biology tests here. Our first tests emerged from an agreement between the University of the Republic, a local affiliate of the Pasteur Institute, and our central government.

One specific thing we have here that is perhaps not so common around the world is that we have a lot of home-based medicine. We can tell people to stay at home and the doctor will come to you— not a paramedic, an actual doctor. So nobody really went to the hospital at the start of the pandemic, and there was no dissemination [of the virus] there. The testing teams went directly to people's homes with all the equipment on them, and they did the sampling there. That was a key factor, I think, in keeping the initial outbreak under control.

I think the initial scare played a role in getting people to follow social distancing guidelines because we were getting news mainly from Italy and Spain, and most of our population has Italian or Spanish origins. We were getting these pictures from Italy and Spain that were really scary, and when the government came out in a press conference and said "You need to stay at home and need to social-distance," people were very willing to comply, even if our lockdown wasn't mandatory.

Today, although Uruguay has one of the older populations in South America, we think it's necessary for the elderly to have affection and to have talks in patios or gardens, in the open air. There is very little infection that happens in open spaces. So we are now promoting social networks that interact in open spaces, maintaining social distance, and with a relatively short period of time, but trying to avoid isolation because that was creating a large physical and mental stress in the elderly.

One more thing: we have this popular traditional drink here called maté [a caffeine-rich herbal tea], which you typically pass from one person to another. This social tradition, which has been with us for hundreds of years, has been cut dramatically. We are not sharing maté anymore. We do single-serve maté now.

RAFAEL RADI

BIOCHEMIST

FERNANDO PAGANINI

DATA SCIENTIST

COVID DEATHS AS OF JULY 20, 2020:

33

MONTEVIDEO, URUGUAY

LEO BARIZZONI (RADI); COURTESY (PAGANINI)

SWEDEN

Sweden's controversial, less-stringent lockdown has made an unlikely star of its state epidemiologist. He told us why he still believes in the national strategy and why he thinks a classic second wave is unlikely. Proportionately, Sweden has suffered many more deaths than its neighbors. Norway has had 48 coronavirus deaths per million people, Finland 60, Denmark 105, and Sweden 547.

STOCKHOLM, SWEDEN

COVID DEATHS AS OF JULY 20, 2020:

5,619

ANDERS TEGNELL

STATE EPIDEMIOLOGIST OF SWEDEN

It's strange to have the world watching Sweden's coronavirus strategy. It's not what normally happens to public servants anywhere in the world, and definitely not in Sweden. And it's also kind of a problem, because it leaves a lot open to interpretation, especially when it's translated through different media sources.

We considered everything earlier in the year, including a harsher lockdown. I think a number of things led us to stick to our original plan. There was really no evidence showing that total lockdown was better. We managed to keep the increase in cases fairly low all the time. So we didn't have the dramatic changes in caseload that especially the UK, but also the Netherlands and some other countries, had. We could show that we managed to keep the number of cases down to a level where the system could keep on coping with it.

In the beginning we had what we call "IKEA syndrome," meaning that our health system was very reliant on just-in-time supply chains. Many hospitals even got supplies several times a day, and sufficient stocks didn't exist anywhere. Everything was always "on its way" from manufacturer to user. That caused a lot of unnecessary problems for health-care workers. Supplies arrived, but usually very, very late, so that they were never quite sure, when they went home in the evening, if there would be any more the next day. There was always protective equipment in place, but this constant fight to get hold of other things, I think, really nagged on people. It's not completely under control yet, but it's a lot better now: very few hospitals report lack of supplies anymore.

During our modified lockdown, Sweden increased its ICU [intensive care unit] capacity to the level where there are always at least 20% of the beds free at any given time. And then every medical procedure that could be delayed, has been delayed.

It's true that herd immunity has been slower than expected, for several reasons. The populations we've been testing are probably not very representative of patients as a whole. We've been only testing people who come into primary care and so on. When we test in companies or people working in hospitals, we see much higher levels of immunity. So we are now trying to put together this jigsaw puzzle from different sources of data. The problem with this disease is that the spread seems to be very patchy. Some workplaces in Sweden have 0.5% immunity; other workplaces have 20% immunity. So you really need to test a lot of people.

This patchiness in the virus is really a problem, because it makes it so difficult both to control it and to measure and understand it. It jumps from one group to the other in clusters. There was a recent outbreak in the mines up in the north [in Gällivare, in June 2020] because a lot of people collected in one place. So I think if anything, we need to have some preparedness for more of these local outbreaks—to be very much on our toes and to be able to handle them quickly.

To some extent, migrants and refugees have been hit harder by the pandemic. Crowdedness is one reason. And they tend to work in high-contact professions. So it's not an ethnicity problem per se. We definitely see to it that the information is available in all the many languages of people who come and live in Sweden these days. We have close connections with those communities through a number of people belonging to those communities.

We still don't, at this stage, see the obvious need for everyone to wear a mask in Sweden based on the knowledge that's been supplied so far. I mean, we're looking at everything and more data that is coming in. There might be a place for face masks at different times in different populations. But it's very difficult to measure the effect of face masks in a population.

It's difficult to know what the long run holds, because when you let people loose, there's a lot of temptation to go too far. That's why we believe in the Swedish model: to not have drastic changes in how much you can meet people and so on. For many of the countries opening up now, figuring out how to stop at the right level is going to be the big challenge. I'm not sure we're going to see your classical second wave, like in 1918. I think we're going to see more local outbreaks like the one in Gällivare.

COURTESY PHOTO

VIETNAM

COVID DEATHS AS OF JULY 20, 2020:

0

TRAN THI HAI NINH

HEAD OF INTERNAL MEDICINE, NATIONAL HOSPITAL FOR TROPICAL DISEASES

SAIGON, VIETNAM

NGUYEN KHANH

Vietnam, population 97 million, is the world's largest country with zero coronavirus deaths. The one-party state implemented aggressive quarantines. It also funneled most of its coronavirus patients into one central hospital in Saigon.

It was in December 2019 when I first heard about the new virus in Wuhan. We predicted that this disease would come to Vietnam soon, because China is very near Vietnam and we share a long border. We had different scenarios: What should we do when we have the first case? What should we do when we have 10 cases? 100 cases? Countless cases? We carefully prepared for each scenario. And we kept reminding all staff that they must protect themselves and strictly obey all of the hospital's guidance to keep them safe.

Our hospital is the national hospital for tropical disease, so the government decided to send the majority of our country's patients here. In Vietnam, the first case was in January 2020, and about two months after that we experienced the peak, when we had around 100 cases in our hospital. And we had hundreds more cases in isolation, who also stayed in our hospital. So our whole hospital was only for covid-19.

All the staff also stayed in the hospital. We didn't go home. So we were also quarantined for more than three months. We have around 350 staff. The decision for us to stay here was made in January. It was tough, because we had to stay away from our families, and every day we had to treat these sick patients and hear about their situations.

We always had enough PPE [personal protective equipment]. Our factories also started producing extra in February. At the beginning of the pandemic, we worried that maybe we would lack that, so we tried to reuse N95 masks and we tried to reduce using PPE by, for example, only wearing one during the four hours when we worked directly in the patients' area. But at this moment, we have so much PPE that we are exporting it to other countries.

> **All the staff also stayed in the hospital. We didn't go home. So we were also quarantined for more than three months.**

I think in the country's fight against covid-19, the media has been very important. They provide continuous information, so that the population can have real-time updates, and then believe in the government and strictly obey all their guidelines. We also have many funny videos about handwashing and wearing masks, some of them with famous singers. And this also made it easier for the children and for elderly people to understand and apply those guidelines. We highly appreciate that Vietnamese people basically followed all the rules, because it helped us a lot. The reason we can assist them up until today was because we successfully limited the numbers [of new infections]. Vietnam is a developing country and our resources are very, very limited.

When I finally got to go home to my family again, it was on May 29. We were allowed to go because we had no more positive cases in our hospital. On an average day during the peak in March and April, it really felt like we were working 24-hour days. Those three months were shorter than what I had expected, because at the beginning of the pandemic, it was growing so fast around the world. But we are lucky in Vietnam. Only two medical staff across the whole country ever got covid-19. They were both working in the ICU with severe patients, intubating them. It was a bad experience for us, but thanks to that, we improved our safety procedures. For me, life is still not back to normal now because our department still serves covid-19 patients, so we are still quarantined from the greater community. But our days are not as long now.

CHINA: CLEAN-TECH SUPERPOWER

China has transformed itself into a clean-energy powerhouse that now produces most of the world's solar panels, wind turbines, electric vehicles, and lithium-ion batteries.

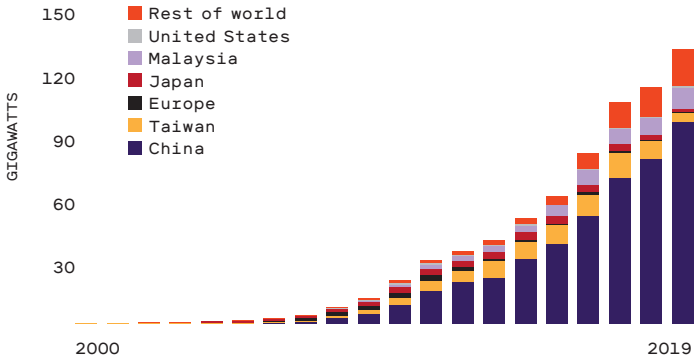
Market dominance, manufacturing expertise, and established supply chains give China huge leverage over the global clean-energy sector. It could enable the country to dictate technical standards and terms of trade, while seizing most of the jobs and revenue that arise from the shift away from fossil fuels.

Other nations hope to build up their own clean-tech manufacturing capacity to reduce their reliance on other countries and boost domestic jobs. But China's market share, and the nearly two decades it took to build it, means any country that hopes to rapidly shift away from fossil fuels will still need to find ways to successfully collaborate and trade with that nation.

By **James Temple**

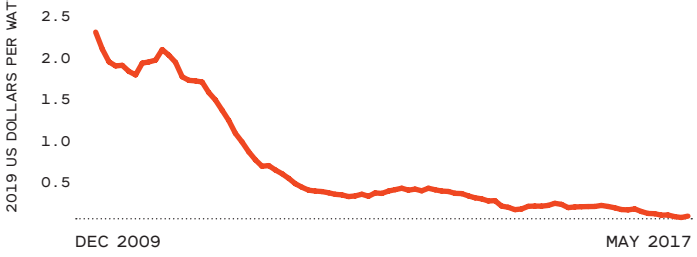
CHINA DOMINATES GLOBAL SOLAR PRODUCTION

Chinese manufacturers produce the vast majority of the world's growing supply of photovoltaic solar cells.

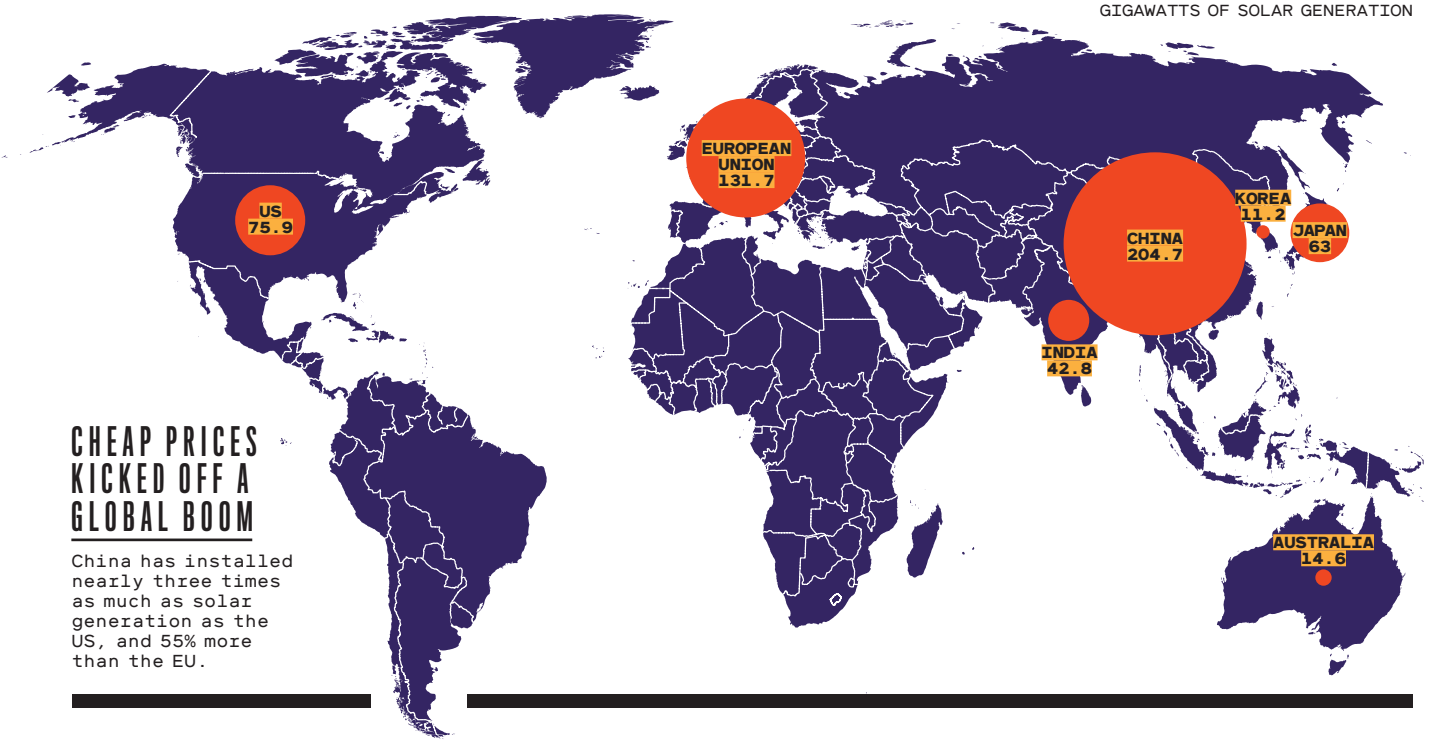


RAMPED-UP PRODUCTION PUSHED DOWN PRICES

China's manufacturers have used automation and other innovations to make photovoltaic modules cheaper.



GIGAWATTS OF SOLAR GENERATION



CHEAP PRICES KICKED OFF A GLOBAL BOOM

China has installed nearly three times as much as solar generation as the US, and 55% more than the EU.

SOURCE 1: ARNULF JÄGER-WALDAU OF THE EUROPEAN COMMISSION'S JOINT RESEARCH CENTRE / SOURCE 2: INTERNATIONAL RENEWABLE ENERGY AGENCY / SOURCE 3: INTERNATIONAL ENERGY AGENCY

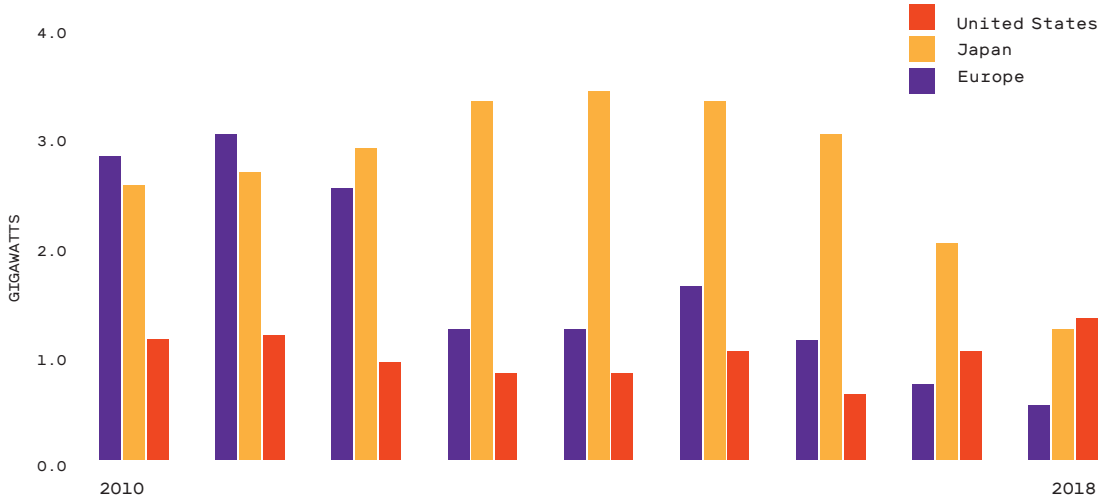
75% CHINA'S SHARE OF GLOBAL LITHIUM-ION CELL MANUFACTURING

54% CHINA'S SHARE OF WIND TURBINE ASSEMBLY CAPACITY

51% CHINA'S SHARE OF EV SALES

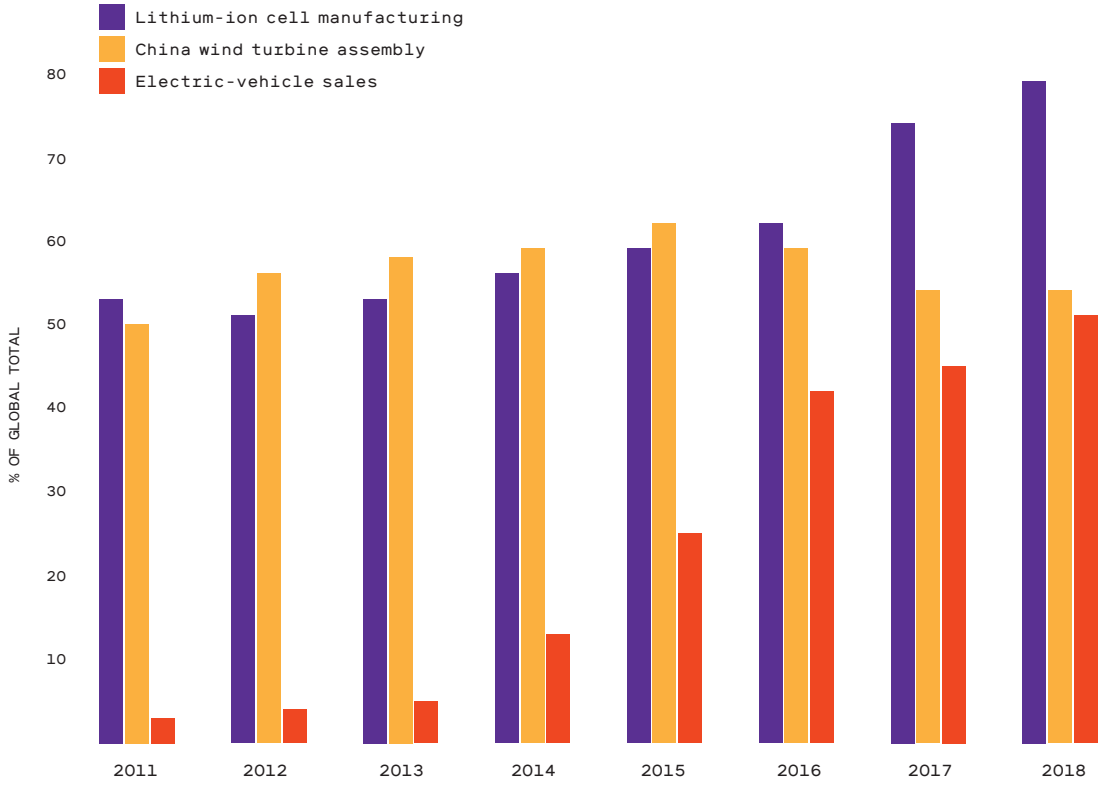
SOLAR PRODUCTION HAS LAGGED IN THE US, EUROPE, AND JAPAN

Japan and Europe produce fewer solar cells, and the US just about the same amount, compared with 2010.



CHINA ALSO DOMINATES IN WIND, BATTERIES, AND ELECTRIC VEHICLES

The nation produces most of the world's lithium-ion batteries and wind turbines, and sells the biggest share of the world's electric vehicles.



SOURCE 1: ARNULF JÄGER-WALDAU, EUROPEAN COMMISSION JOINT RESEARCH CENTRE / SOURCE 2,3: BLOOMBERGNEF

HOW GERMANY TAMED COVID

BY KATI KRAUSE / ILLUSTRATED BY PATRICK LEGER

FEBRUARY 2020. ANGELA MERKEL IS NEARING THE END OF HER FOURTH TERM AS GERMANY'S CHANCELLOR. THINGS AREN'T GOING WELL.

HER OPEN-DOOR POLICY TOWARD REFUGEES HAS FUELED THE RISE OF THE FAR RIGHT.

IN ONE STATE, HER OWN CDU PARTY HAS JUST VOTED TO JOIN FORCES WITH THE FAR-RIGHT AFD.

AND CDU CHAIR ANNEGRET KRAMP-KARRENBAUER, MERKEL'S CHOSEN SUCCESSOR, HAS QUIT.

SOME IN THE CDU ARE SPECULATING ABOUT AN EARLY END TO HER CHANCELLORSHIP.

AND NOW COVID-19 IS STARTING TO APPEAR.

GERMANY REGISTERED ITS FIRST CASES IN LATE JANUARY, AND THOUGHT IT COULD CONTAIN THEM.

BUT ON FEBRUARY 23, AS PARTS OF NORTHERN ITALY GO INTO LOCKDOWN, VIROLOGIST CHRISTIAN DROSTEN, A CLOSE ADVISOR TO MERKEL, GIVES THE BAD NEWS.

I NO LONGER BELIEVE WE CAN AVOID A PANDEMIC.

A FEW DAYS LATER, AUTHORITIES IDENTIFY GERMANY'S FIRST SUPERSPREADING EVENT, A CARNIVAL MEETING IN A TOWN NEAR THE DUTCH BORDER. THE PAINSTAKING TASK OF CONTACT TRACING BEGINS.

PLEASE TELL US EVERYONE YOU'VE BEEN IN CONTACT WITH OVER THE PAST TWO WEEKS.

ON MARCH 9, GERMANY REPORTS ITS FIRST TWO COVID DEATHS.

THE DAX STOCK INDEX DROPS BY 8%, ITS BIGGEST LOSS SINCE 9/11.

A DAY LATER, BERLIN CLOSES ITS BIG PUBLIC THEATERS AND OPERA HOUSES.

UP TO NOW, MERKEL HAS HARDLY BEEN SEEN.

BUT NOW SHE FINALLY SWINGS INTO ACTION, ACKNOWLEDGING THE GRIM TRUTH IN A SPEECH TO PARLIAMENT ON MARCH 10.

ON MARCH 12, SHE HOLDS A PHONE CONFERENCE WITH THE 16 STATE GOVERNORS. THEY ALL AGREE TO FOLLOW THE GUIDANCE OF THE FEDERAL DISEASE CONTROL AGENCY, THE ROBERT KOCH INSTITUTE.

THERE IS NO VACCINE, NO TREATMENT: 60% TO 70% OF THE POPULATION MAY BECOME INFECTED.

IT IS IMPERATIVE THAT WE ACT IN UNISON.

"OK." "AGREED." "JA."

MY DEAR FELLOW CITIZENS, THE CORONAVIRUS IS CHANGING DAILY LIFE IN OUR COUNTRY DRAMATICALLY.

AND ON MARCH 18, FOR THE FIRST TIME IN HER 15 YEARS AS CHANCELLOR, SHE ADDRESSES THE GERMAN PEOPLE DIRECTLY ON TV.

"I'M ADDRESSING YOU IN THIS UNUSUAL WAY TODAY BECAUSE THIS IS PART OF WHAT OPEN DEMOCRACY IS ABOUT: THAT WE MAKE POLITICAL DECISIONS TRANSPARENT AND EXPLAIN THEM."

"PLEASE TAKE THIS SERIOUSLY. SINCE GERMAN REUNIFICATION--NO, SINCE THE SECOND WORLD WAR--THERE HAS NOT BEEN A CHALLENGE FOR OUR COUNTRY THAT DEPENDS SO MUCH ON OUR ACTING IN SOLIDARITY."

"I FIRMLY BELIEVE THAT WE WILL PASS THIS TEST IF ALL CITIZENS GENUINELY SEE THIS AS ***THEIR*** TASK."

OVER THE NEXT WEEK, THE GOVERNMENT TAKES DRASTIC STEPS.

SCHOOLS AND NURSERIES CLOSE.

THE BUNDESLIGA SUSPENDS ALL SOCCER MATCHES.

CHURCH SERVICES ARE BANNED.

ALL SHOPS EXCEPT SUPERMARKETS AND PHARMACIES CLOSE.

MOST LAND BORDERS ARE LOCKED DOWN.

PLAYGROUNDS ARE SHUTTERED.

GERMANS ARE ASKED TO CANCEL ALL VACATIONS.

BUT THE PEOPLE TRUST MERKEL'S SCIENTIFIC ADVISORS.

DROSTEN'S 40-MINUTE "CORONAVIRUS UPDATE" QUICKLY BECOMES THE MOST POPULAR APPLE PODCAST IN GERMANY.

AND THE ROBERT KOCH INSTITUTE PUBLISHES THE VIRUS'S REPRODUCTION RATE, OR R-VALUE, EVERY DAY, URGING PEOPLE TO PUSH IT BELOW 1.

RKI: R-Value At 1.2

AS TOTAL CASES PASS 25,000, GERMANY GOES INTO LOCKDOWN.

SOURCE: OUR WORLD IN DATA

AT THE END OF APRIL, MASKS BECOME COMPULSORY IN SHOPS, ON PUBLIC TRANSPORT, AND IN OTHER PUBLIC INDOOR SPACES--

--A HUGE STEP FOR GERMANS, WHO CONSIDER SHOWING ONE'S FACE PART OF THE NATIONAL CULTURE.

PRIVACY-CONSCIOUS GERMANS NOW ALSO HAVE TO GIVE THEIR CONTACT DETAILS IN MANY PLACES, SO THEY CAN BE NOTIFIED IF IT TURNS OUT SOMEONE NEARBY HAD THE VIRUS.

I'D LIKE THE SCHNITZEL WITH...

I NEED YOUR NAME, ADDRESS, AND PHONE NUMBER FIRST!

BUT TRUST IN THE FEDERAL GOVERNMENT IS NOW SO HIGH THAT WHEN IT LAUNCHES A CORONAVIRUS TRACKING APP IN MID-JUNE, 15 MILLION PEOPLE DOWNLOAD IT IN THE FIRST THREE WEEKS.

HAVE YOU DOWN-LOADED THE APP YET?

YES, GRANDMA...

AND WHEN THE EU REOPENS MOST INTERNAL BORDERS ON JUNE 15, GERMANS ENTHUSIASTICALLY GO ON VACATION.

AS GERMANY ASSUMES THE EU COUNCIL PRESIDENCY ON JULY 1, 82% OF GERMANS THINK THE GOVERNMENT IS DOING A GOOD JOB. ONLY ONE IN FOUR IS STILL WORRIED ABOUT THE PANDEMIC.

MEANWHILE, TOGETHER WITH FRANCE'S EMMANUEL MACRON, MERKEL PUSHES EU LEADERS TO APPROVE A 500-BILLION-EURO RECOVERY FUND FOR STRUGGLING COUNTRIES.

IT WILL NOT FAIL BECAUSE OF US.

THE CHANCELLOR AND I PUT IT ON PAPER: IT'S OUR ABSOLUTE PRIORITY.

MOST GERMANS THINK MERKEL'S NEXT JOB SHOULD BE TO TACKLE CLIMATE CHANGE.

TAKE YO BEST SHOT

Illustrations by Nicolás Ortega

UR

The whole world wants a vaccine, but countries will naturally try to secure a supply for themselves first.

By Antonio Regalado

The Chinese company Sinovac Biotech developed an experimental vaccine for SARS back in 2004. That disease went away after killing just 800 people, and the project was shelved. But it meant that when the new coronavirus, SARS-CoV-2, exploded in China last January, the company had a road map for what to do next. Four months later, it published evidence that it could protect monkeys against the disease using a simple vaccine made from killed virus.

By then, though, China had a different problem: not enough covid-19. Its draconian lockdown measures had quashed the virus at home so effectively that doctors couldn't find patients to fully test their vaccine on. The US had plenty of infections, but tensions between the countries meant no Chinese vaccine for covid-19 will ever be tested on US soil.

So in June Sinovac struck a deal with a Brazilian vaccine center, the Butantan Institute in São Paulo, to run a large trial there on about 9,000 healthcare workers. For Brazil, battered by covid-19, the study comes with a clear quid pro quo. Butantan will pay for the trial and recruit volunteers; in exchange, Sinovac has promised to supply Brazil with 60 million vaccine doses and to let it manufacture further supplies as well.

Brazil can do that because, since the 1980s, it has carefully protected its ability to study, manufacture, and bottle vaccines at Butantan and at a second center near Rio de Janeiro. "The national immunization program of Brazil has self-sufficiency as a goal," says Ricardo Palacios, the Butantan infectious-disease doctor who is running the study.

People in every country in the world will soon be clamoring for covid-19 vaccines. The US, through a government initiative called Operation Warp Speed, has already spent more than $5 billion to get drug makers to manufacture vaccines on its soil. China has a portfolio of its own candidates and has ramped up investment in biomanufacturing. But other countries, particularly in Europe, over the years have sold off or shuttered government manufacturing centers, let national expertise disappear, lost interest, or come to rely on neighbors to make and bottle vaccines.

An ample supply of a covid vaccine could become a coin of geopolitical power, as oil and nuclear weapons are now. Governments will be counting on it to allow them to reopen economies and assure political stability. Alliances are already shifting, with leverage going to countries that can create vaccines, test them, manufacture bulk ingredients, and perform the "fill and finish" bottling. The rest of the world apprehensively watches, fearful of being left defenseless against the deadly pandemic.

AMERICA FIRST

The race toward covid vaccines has moved with unprecedented speed. As of July, several candidates, including Sinovac's, had been shown to protect monkeys and proved safe in initial tests on people; the next phase of clinical trials tests whether they work at conferring immunity.

Experts say we'll need several vaccines, not just one, and it's likely that supplies will be sharply limited at first. That's why there is already unprecedented competition among nations to secure the shots.

Behind the scenes, bartering for access to vaccines has already started, and everything is on the table, says Pierre Morgon, a biotech consultant who has been working with CanSino, another Chinese maker of covid vaccines. "You get into the dark world of horse trading," he says. During the H1N1 flu pandemic in 2009, when he was with the French drug company Sanofi, Morgon says, diplomats in Paris selected which countries should get priority supplies. The list included nations that supply commodities France depends on: gas, oil, and uranium. "It was not even thinly veiled," says Morgon.

And it won't only be states vying for access, but also companies, individuals, even criminal gangs ready to hijack a refrigerator truck. During the H1N1 outbreak, France posted its gendarmerie at the gates of the Sanofi factory. "When you have something in short supply and high demand, it has a street value," says Morgon. "Just look at the masks, with people reselling them at massive multiples." Western intelligence services allege that Russia has already deployed a team of hackers known as Cozy Bear to extract vaccine secrets from UK and US servers.

In the US, the Trump administration has the aim of securing 300 million doses of a safe, effective vaccine by January, something it has sought to guarantee through "pre-purchase" agreements. When it announced a $1.6 billion payment to Novavax, a biotech company with no vaccines on the market (the money is for manufacturing one), the Department of Health and Human Services specified that "the federal government will own the 100 million doses of investigational vaccine" expected to result from the contracts.

The implication: it's for Americans first.

A similarly risky US advance purchase deal with Paris-based Sanofi—risky because no vaccine is guaranteed to work—created a diplomatic breach with France. Sanofi's CEO, Paul Hudson, said the US "has the right to the largest preorder because it's invested in taking the risk." French officials called the explanation "unacceptable," saying a vaccine should be "a global public good" and that "equal access for everyone to the vaccine is not negotiable." Similarly, in June Doctors Without Borders, the international nongovernment medical group, put out a fiery statement against "nationalist stockpiling measures," saying that "global solidarity should be paramount."

The nonprofit Gavi vaccine alliance, which is based in Geneva and buys vaccines for poor countries, is raising $2 billion to make its own pre-purchase agreements for covid-19 immunizations so that everyone will get supplies at the same time. "We saw a danger that vaccines would get snapped up by wealthy countries, and there would be no vaccines for the rest of the world," says Gavi CEO Seth Berkley.

"I understand national governments trying to protect their citizens … but the issue is that you are not safe unless everyone is safe," he says. "If epidemics are raging in the rest of the world, you can't go back to normal, you can't travel, you can't do tourism—you are not going to get the reprieve from the economic crisis."

Better than trying to immunize everyone in a few countries first, says Berkley, would be to distribute the initial doses to vaccinate a portion of each country's population. If there are 2 billion doses available in 2021, as he anticipates, every country could vaccinate 20% of its people, including health workers, those at higher risk, and potential "superspreaders" like prisoners, people in refugee camps, and workers at meatpacking plants.

The reality could be a little different, says Clint Hermes, a lawyer at Bass, Berry & Sims, who specializes in vaccine trials. "It may not be fair that some countries buy ahead of others, but that is what is likely to happen," says Hermes. "I don't think anyone expects the US to send vaccine to Angola before it gets to Arkansas … The real challenge with equitable access is how to make it work. Ethicists can sit in a room and decide who gets what in what order, but none of that matters unless there is a financing mechanism."

COMMON TYPES OF VACCINES

LIVE VACCINE	A living virus that has been weakened or attenuated. Alternatively, a similar virus that's not dangerous.	**AVAILABLE FOR:** measles, influenza (children), smallpox
KILLED VACCINE	A virus that has been killed, most often with formalin, so it can't replicate.	**AVAILABLE FOR:** influenza (adults), polio
SUBUNIT VACCINE	A protein vaccine consisting of a part of a virus, such as its shell.	**AVAILABLE FOR:** human papillomavirus, hepatitis B
GENE VACCINE	Injections of DNA or RNA information from a virus. Genes can be introduced in a nanoparticle or another virus.	**NOT WIDELY AVAILABLE** Includes some of the covid-19 vaccines in development

THE GAMBLE

For now, there's no proof that any vaccine works, so all the bets involve risk. Early in the pandemic, the US and nonprofit funders heavily backed advanced technologies that

MEET THE MAN IN CHARGE OF US COVID VACCINE TRIALS

T R : Q + A

Larry Corey on how long it will take to find a vaccine and why it's much easier than for HIV/AIDS.

By Antonio Regalado

The Trump administration has battled governors and doctors on everything from closing restaurants to wearing masks to reopening schools, and even which drugs might help with covid-19.

But one area of agreement—for now—is the all-out push for a vaccine. Labs have generated dozens of candidate vaccines, employing everything from speedy RNA shots to old-fashioned injections of killed germs.

The White House effort to bring one or more of those to market by January is called Operation Warp Speed. It has handed out more than $5 billion to vaccine makers and is now racing toward the next hurdle: human trials involving as many as 150,000 volunteers to determine which, if any, of the vaccines work.

In July, the administration named Lawrence Corey, a virologist at the Fred Hutchinson Cancer Research Center, as point person for the big human tests. Corey, an HIV/AIDS expert, had been running a federally funded network of clinics testing possible HIV vaccines. Now those personnel, laboratories, and infrastructure are being thrown at covid-19.

MIT Technology Review's biomedicine editor, Antonio Regalado, asked Corey about the prospects for a covid vaccine.

Q: The goal of Operation Warp Speed is to have "substantial supplies" of a safe, effective vaccine by January in the US. Do you think that will happen?

A: I think that there is a possibility we might have an answer for one vaccine by January 2021, but February, March, April is the more logical timeline. Our goal is to test multiple vaccines and have answers about six months later. If we start in July, that is the end of January. But if we start one in September, that is the end of March. That's the timeline for vaccines that are 50% effective. If it is 90% effective, you will find out sooner, maybe by two months.

Q: It might be only partly effective?

A: Yes. Influenza vaccines are 60% or 80% effective, depending on the strain. But it's not unheard of for a vaccine to have a greater effect on the more severe end of the curve. It may fall out that it's 50% effective overall, but if among the elderly or among African-Americans or Hispanics [three groups disproportionately affected by covid-19] it reduced hospitalizations by 80%, that would be quite an effective vaccine.

Q: What vaccines will you be testing in volunteers?

A: The ones that are public knowledge are the Moderna RNA vaccine and vaccines from AstraZeneca, Johnson & Johnson, and Novovax. [Editor's note: after this interview, a grant to Pfizer was announced.]

Lawrence Corey, a virologist at the Fred Hutchinson Cancer Research Center

Q: When did you know your HIV trial network would play a big role in tackling covid?
A: It was after I returned from an HIV meeting in South Africa in February. Anthony Fauci, who is my close friend and colleague, called me and said, "Larry, we need to develop an infrastructure to test covid vaccines, and you are the logical guys to do it. Your network has the biggest infrastructure; you have the labs and the experience." The announcement only came out in July, but we've actually been working on it seven days a week for four and a half months.

Q: There still isn't an HIV vaccine after all these years. What does that say about a covid vaccine?
A: The human body doesn't cure HIV on its own. So it's been an amazingly difficult problem to create a vaccine. The science around covid-19 is way more optimistic. Depending on the mortality, 97% or 98% of people with covid-19 self-cure the infection. It means the immune system recognizes covid-19 in a way that it doesn't recognize HIV. So we should be a lot more successful.

Q: Why is finding a vaccine so important?
A: When it comes to population-based control of infectious disease, vaccination has really been the most effective tool. With HIV we closed the bars, closed the gay baths, and that had a certain effect, but it really takes biomedical interventions to make an impact. We can do behavior change, social distancing, but if we want to get on a plane to travel, and we want to feel comfortable going to restaurants, we need a vaccine for 7 billion people.

Q: But HIV is now controlled by antiviral drugs, which can also stop someone from spreading it. Why do we still need a vaccine for it?
A: It's because you can't diagnose and treat everyone quick enough to prevent transmission. We have had great drugs for a decade, almost two decades, yet we are still at 1.4 million new cases of HIV each year. The reality is you acquire HIV asymptomatically and you transmit it asymptomatically.

That gets to why testing and contact tracing is not working with covid. You acquire it asymptomatically, you don't know you have it, and you do the behavior that results in transmission. With HIV that is sex, but with covid, that is just walking around and touching people. The reality is you acquire these infections from the people you suspect the least.

Q: In some Warp Speed agreements, the US is guaranteed exclusive access to early lots of vaccine. Is it fair that the initial allocations are captured by the US?
A: When you look at the total program, you will see five vaccines, each with 100 million doses, or 500 million doses [total]. And Johnson & Johnson said a billion doses. If you add those up, that is way over what is needed for our country. There will be vaccine available to the rest of the world, and certainly the data will be.

were quick to generate candidates but have never yet led to an approved vaccine or been produced at scale. These include the RNA vaccine being developed by Moderna Pharmaceuticals, and a DNA injection from Inovio Pharmaceuticals; both try to directly deliver genetic information about the virus into a person's cells. Since then, the US has also funded Johnson & Johnson, which uses a more conventional approach.

Morgon compares it to a race in which there are "an ostrich, a horse, and a dog" at the starting gate. "You want to lay a bet on each kind of animal," he says.

In Brazil, far-right president Jair Bolsonaro, sometimes called the "Tropical Trump," has scoffed that the virus is a mere cold, fired his health minister, and claimed that a malaria drug, chloroquine, cured him when he contracted covid-19 in July. Instead of going through the federal government, the trial in Brazil of the Chinese vaccine is being financed by João Doria, governor of the country's richest state, São Paulo, and a rival of Bolsonaro's who has his eyes on the presidential palace.

Sinovac's vaccine uses a tried-and-true approach—virus that is chemically inactivated, or killed—and Palacios says Brazil will be equipped to manufacture it locally once a production line is retrofitted. Berkley therefore sees a "tortoise and hare" situation in which conventional approaches may reach the market first or become more widespread.

Despite the intense focus on a vaccine, some worry it's the wrong priority. William

ROBERT HOOD / FRED HUTCHINSON CANCER RESEARCH INSTITUTE

Haseltine, a onetime HIV researcher and biotech entrepreneur, thinks more effort should be spent on antiviral drugs—the strategy that eventually brought AIDS under control. That, he says, would buy time to create a vaccine whose safety is fully understood before trying to inoculate billions of people.

"This is not an ordinary situation for vaccine development, because there is such political and economic pressure to find a solution to the problem," says Haseltine. "If we launch a vaccine that is not fully vetted for safety, and has nasty side effects, there will be hell to pay for vaccines for years, which would cost hundreds of millions of lives."

SCIENCE ON TRIAL

This summer and fall, companies and researchers should start getting data on whether the vaccines under development really protect people against infection by the coronavirus, or at least from its worst effects.

The US has redirected a federally funded network based at the Fred Hutchinson Cancer Research Center in Seattle, which had been testing HIV vaccines, to instead gather evidence on five covid-19 vaccines in big trials of 30,000 people each. Chinese companies, without enough cases at home, are running studies in Canada, Brazil, and elsewhere.

Lawrence Corey, a virologist from Fred Hutchinson who was tapped by Warp Speed in July to head the US trials (see Q+A, page 31), says the vaccine hunt is moving quickly because scientists have been "planning for success." Rather than wait for final proof that a shot is effective, for example, companies are using US government funds to scale up manufacturing now. "The ramp-up for the studies is extremely fast—much faster than for any trial that I have ever been involved in," says Boris Juelg, a doctor at Harvard who is among those who have switched their efforts to covid-19 trials.

One danger now is that governments will push to release a vaccine prematurely. In the US, for instance, the Food and Drug Administration approved chloroquine for treating covid-19, only to reverse itself weeks later after it became plain the drug didn't work. By then, India had blocked exports of raw ingredients, the US had spent millions on useless stockpiles, and Brazil's president had ordered the army to manufacture vast supplies of the drug. "I expect the vaccines to be less of a circus, and a lot more cutthroat," says Hermes, the vaccine lawyer.

Another worry is that evidence for or against a vaccine could get twisted. Already, a sizable part of the population suspects vaccines are part of a plot. US polls carried out this summer show about a quarter of respondents say they would refuse a coronavirus vaccine.

The efforts risk getting caught up in politics, too. In July, President Trump said the US would exit the World Health Organization, a body that has a major role in setting common standards, such as which type of mouse to test vaccines on. The White House has also attacked its own top virologist, Anthony Fauci, whose institute funds the testing of vaccines.

Since the start of the pandemic, fast sharing of information has been a key weapon against the virus. It was the publication of the germ's genetic sequence in January, by Chinese scientists, that kicked off the vaccine race. After that, European doctors flooded academic journals with descriptions of cases and tricks they had learned for managing severe illness. With vaccines, whether they originate in China, the US, or the UK, sharing data will be crucial so that researchers can compare notes.

They may, for example, learn how to tell whether someone has developed immunity to the virus by measuring the level of antibodies or certain immune cells in the blood. If they do, the third or fourth vaccine to reach the market might get approval based on biomarkers alone. There will be no need to wait a year—as in a typical vaccine trial—to find out what proportion of people who were given the vaccine subsequently got sick.

To Corey, at the Fred Hutchinson, the involvement of large multinationals like AstraZeneca and Merck is likely to act as a bulwark against the politicization of vaccine research and supplies. During the Ebola crisis, the winning vaccine was created in Canada, sold to Merck, funded by the US, and tested in Guinea, under the coordination of the World Health Organization. It is now manufactured in Germany. Says Berkley, "Try to make that nationalistic—how would you even define that?"

ONE DANGER NOW IS THAT GOVERNMENTS WILL PUSH TO RELEASE A VACCINE PREMATURELY.

Antonio Regalado is MIT Technology Review's biomedicine editor.

REGISTER TO RULE THEM ALL

Brazil was already on its way to becoming a surveillance state. Then covid-19 happened.

For many years, Latin America's largest democracy was a leader on data governance. In 1995, it created the Brazilian Internet Steering Committee, a multi-stakeholder body to help the country set principles for internet governance. In 2014, impelled by Edward Snowden's revelations about surveillance by the US National Security Agency of countries including Brazil, Dilma Rousseff's government pioneered the *Marco Civil* (Civil Framework), an internet "bill of rights" lauded by Tim Berners-Lee, the inventor of the World Wide Web. Four years later, Brazil's congress passed a data protection law, the LGPD, closely modeled on Europe's GDPR.

Recently, though, the country has veered down a more authoritarian path. Even before the pandemic, Brazil had begun creating an extensive data-collection and surveillance infrastructure. In October 2019, President Jair Bolsonaro signed a decree compelling all federal bodies to share most of the data they hold on Brazilian citizens, from health records to biometric information, and consolidate it in a vast master database, the *Cadastro Base do Cidadão* (Citizen's Basic Register). With no debate or public consultation, the measure took many people by surprise.

In lowering barriers to the exchange of information, the government says, it hopes to increase the quality and consistency of data it holds. This could—according to the official line—improve public services, cut down on voter fraud, and reduce bureaucracy. In a country with some 210 million people, such a system could speed up the delivery of social welfare and tax benefits, and make public policies more efficient.

But critics have warned that under Bolsonaro's far-right leadership, this concentration of data will be used to abuse personal privacy and civil liberties. And the covid-19 pandemic appears to be accelerating the country's slide toward a surveillance state. Despite briefly falling ill himself, and although Brazil's death toll

By
RICHARD KEMENY

Illustrations by
Stuart Bradford

90
RS
N
/ SP - CEP: 139509-004

had passed 90,000 by the end of July, Bolsonaro has consistently downplayed the seriousness of the disease. Yet that hasn't stopped him from using the crisis to justify even more aggressive data grabs.

The instinct to centralize

According to Rafael Zanatta, a director of Data Privacy Brasil, an NGO, the government's discourse on using data to improve public services is strikingly similar to the way the military dictatorship in the 1970s justified its own efforts to create a unified system. That project, known as Renape, faced criticism from within the military and a backlash from the government technicians building it because of its lack of transparency and the threats it posed to freedom and privacy. It was eventually shelved.

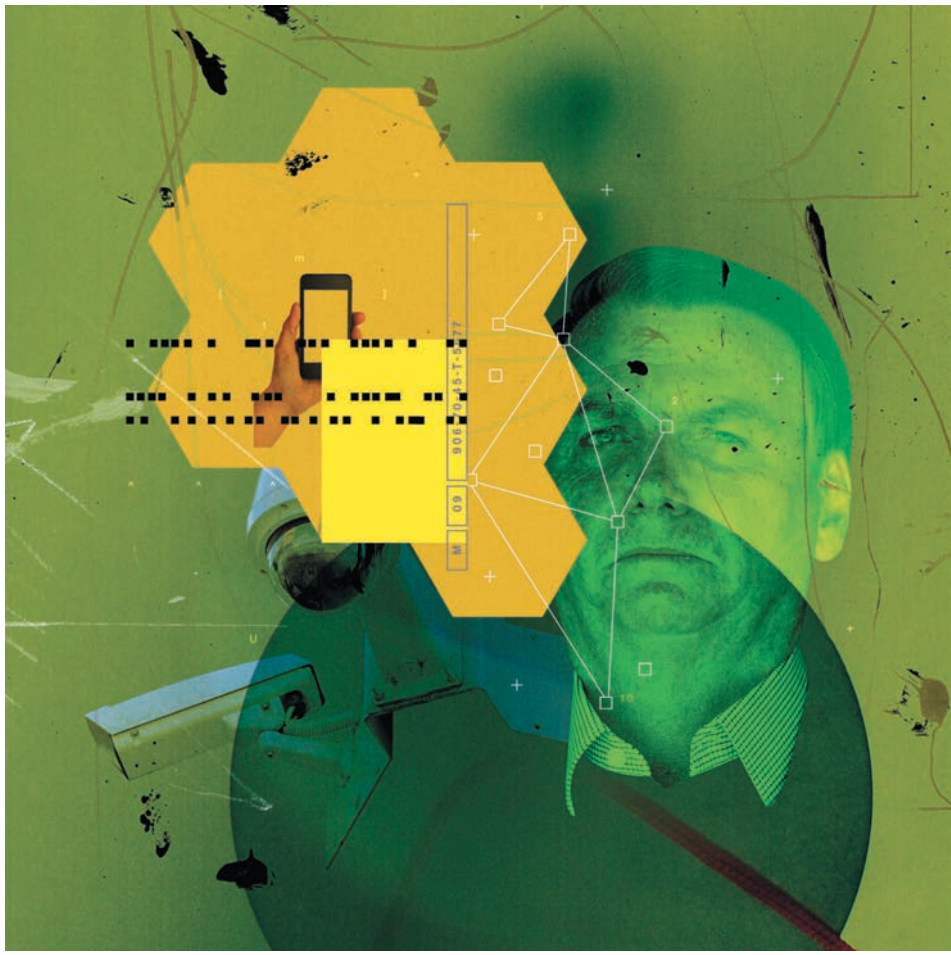
The *Cadastro* may have been born of good intentions, says Ronaldo Lemos, a lawyer and director of the Institute for Technology and Society Rio. Indeed, the pandemic quickly revealed the need for some sort of nationwide digital identity system: by the end of April, 46 million informal workers, previously invisible to the federal government, had registered online to receive emergency financial aid.

But Lemos, one of the authors of the *Marco Civil*, says its centralized nature is worrisome. He has long advocated for a model akin to that used in Estonia, a country widely seen as a paragon of digital governance. The Estonian government stores a broad range of citizens' data, yet no single government agency holds all the eggs in its institutional basket. Estonians have to give permission for one agency to access the data another agency holds on them, and they can track who looks at their data. "With this decree," says Lemos, "Brazil is doing precisely the opposite."

Dismantling safeguards

Under the October decree, any federal body could start requesting and gathering data from others. Documents leaked to The Intercept in June revealed that ABIN, Brazil's national intelligence agency, had already used the decree to ask Serpro, a state-owned data company, for the records of the 76 million Brazilian citizens who hold driver's licenses. Such examples mean citizens' data could start appearing in many new data sets without their knowing about it.

The scope for data acquisition under the decree is broad. Along with basic information such as name, marital status, and



employment, the *Cadastro* will include biometric data such as facial profiles; voice, iris, and retina scans; prints of digits and palms; even gait. There are no limits placed on how health data can be shared, and the list even includes genetic sequences. The plan, says Lemos, is "using genomics, faces, and fingerprints as a form of identifying people easily, without them knowing exactly how, which is pretty scary."

Centralizing so much data presents a "huge security risk," says Verónica Arroyo, a policy associate at the advocacy group Access Now. A hack or leak could open citizens up to identity theft, fraud, or worse. In 2016, São Paulo city hall accidentally exposed the personal data—including some medical records—of 365,000 patients in the public health system. In 2018, tax ID numbers and other information on 120 million people—more than half the population—were unveiled to the internet for weeks, after the server housing them was incorrectly renamed.

The *Cadastro* will be regulated by a Central Data Governance Committee. This body, made up of representatives from the federal government, will decide on the sensitivity of data and rule on any controversies. That's in sharp contrast to the Internet Steering Committee set up in 1995, whose members include people from government, business, civil society, and academia. "You don't have citizens, you don't have the technical community, you don't have civil society—it's not even intended to be an independent commission," says Danilo

"All these efforts can lead up to a high asymmetry of powers between citizens and the state."

Doneda, a civil lawyer and advisor to the Internet Steering Committee.

It's also not clear how the master database will be compatible with the LGPD, the new data protection law. There are stark inconsistencies—for example, biometric data is considered sensitive under the LGPD, yet in the new decree it falls under a less protected category. The new decree "basically ignores data protection legislation," says Doneda. "The government is still acting like it wasn't a concern."

In fact, the fate of the LGPD is still up in the air. It was originally meant to come into force in August, but its protections had already been watered down both by Bolsonaro and by Congress under his predecessor, Michel Temer. In April, however, the government sneaked through an extension to delay implementation until May 2021.

There were arguably good reasons to postpone the LGPD, as disruption caused by covid-19 made it harder for businesses to adapt. But some suspect the government's real motive is to postpone the increased scrutiny the LGPD would bring to political campaigning. Municipal elections are slated to take place later this year, and electoral courts could use the new law to investigate political parties for improper accumulation and use of data, according to Zanatta of Data Privacy Brasil.

There's ample reason to fear such misuse. During the 2018 presidential election that brought Bolsonaro into office, WhatsApp became a platform for widespread misinformation, most of it favoring Bolsonaro, according to an analysis by the Guardian. Some think the *Cadastro* could open the door to more targeted propaganda campaigns. Advanced profiling, including data gathered during the pandemic, could identify the voters most likely to believe and spread misinformation, who could then be unwittingly used to broadcast it, says Zanatta. One of Bolsonaro's sons is currently under investigation for allegedly organizing a criminal scheme to spread fake news.

Justifying surveillance

The covid-19 pandemic has produced further evidence of the president's intent to use data as an instrument of power. In April, when the governor of São Paulo launched a project using phone data to track how well people were adhering to isolation measures, Bolsonaro's son Eduardo called it an "invasion of rights," and the president quickly put a stop to a similar plan from the science ministry. Yet he apparently had no such qualms a week later when he signed a decree mandating that telecoms hand over data on 226 million Brazilians to IBGE, the government's statistical agency, ostensibly for surveying households during the pandemic. Critics said the data grab was unconstitutional and disproportionate, and it was eventually struck down by the supreme court.

Like many countries, Brazil has been increasing its use of technology for tracking its citizens. Surveillance camera networks installed for the 2014 World Cup and 2016 Olympics stayed in place after those events ended. Several police forces used facial recognition software during this year's carnival to scour the crowds for criminals. And a series of bills both enabling and mandating widespread adoption of the technology—on public transport, for example—have been making their slow way through Brazil's congress. Last year Brazilian police arrested 151 people who'd been identified with the help of facial recognition, including one man wanted for murder who was dressed as a woman for carnival. In December, facial recognition cameras were put in place near the border with Paraguay, a hot spot for drug trafficking and other organized crime.

Crime is a big issue in Brazil, where the murder rate is about five times the global average. A tough stance was key to Bolsonaro's rise to power. But the *Cadastro Base do Cidadão* and mass surveillance technology make a terrible combination, warns Arroyo: "All these efforts can lead up to a high asymmetry of powers between citizens and the state." And the fear of crime inclines Brazilians to relinquish their data privacy in return for security, says Doneda: "People are really afraid."

The shortcomings of facial recognition tech are well documented—particularly the fact that existing systems, most of them developed in majority-white countries, disproportionately misidentify people of color. César Muñoz, a researcher at Human Rights Watch, says this poses a particular problem in Brazil, where more than half the population is Black or brown. Almost half of those people work in the informal economy, and around a third live under the poverty line. "If you are a Black person with no means to secure a lawyer and are detained on the basis of facial recognition, it's going to be tough," Muñoz says.

In theory, the regulations being created today are reversible. But once surveillance technology and masses of data are in the hands of the authorities, it's hard to take them back. "If police buy the kit, they are going to use it until it stops working," says Doneda.

Compared with other parts of the world, Brazil is rich with NGOs dedicated to data privacy and rights. It's also relatively easy to launch collective-action lawsuits, making public pressure easier to apply. And as the pandemic has shown, the supreme court can still stand up to the federal government. In early June, it forced the health ministry to start publishing comprehensive data on covid-19 deaths again, after the ministry stopped doing so in what was widely seen as an attempt to cover up the rapidly rising death toll.

Lemos believes a culture of data protection could still flourish in Brazil, in a development similar to the paradigm shift that happened after a consumer protection code was introduced in 1990 and people started to exercise their newfound rights. Much will rest on when the LGPD comes into force, and whether it's backed up by a credible and independent data authority.

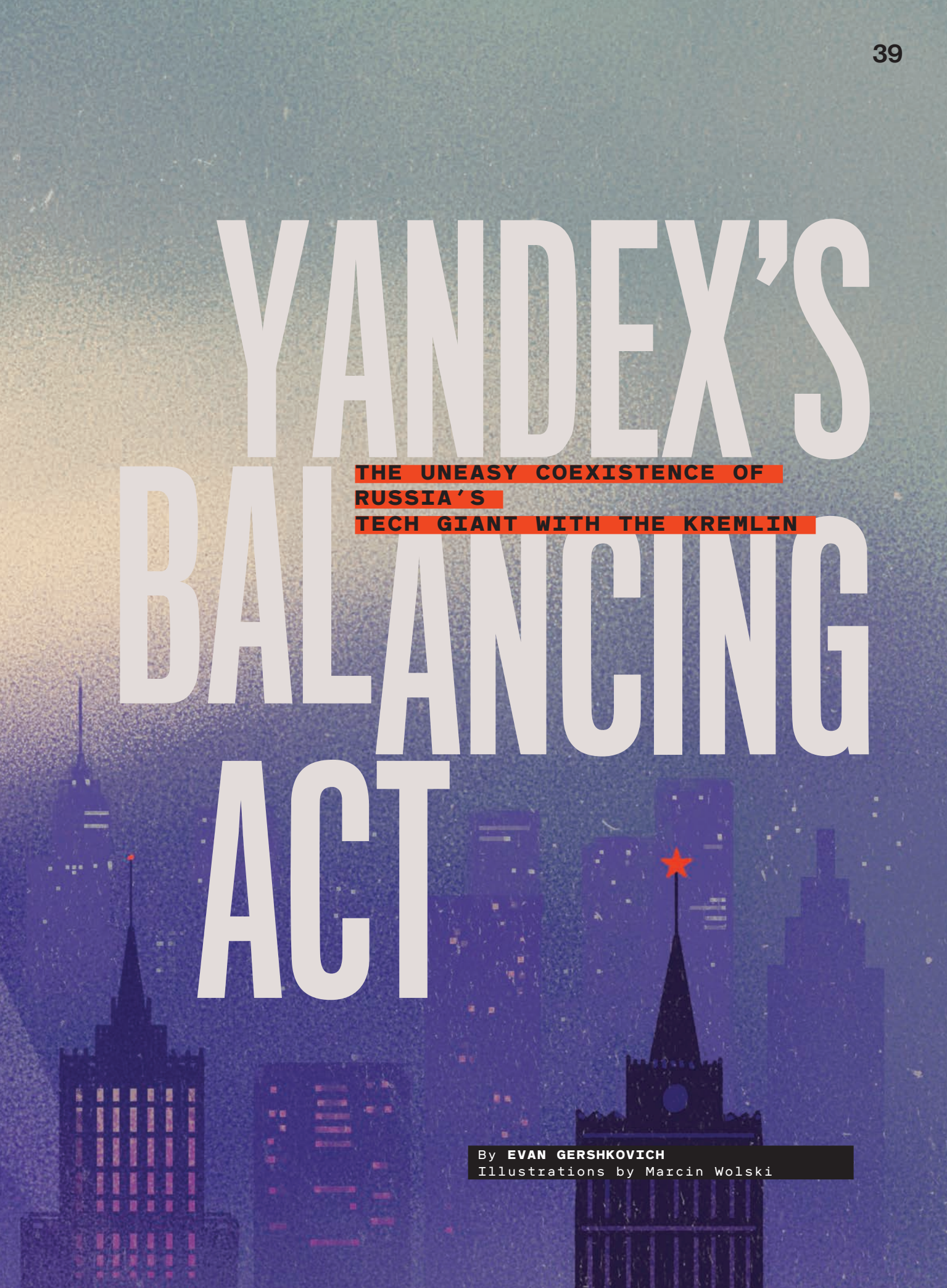
But some observers think the authority could be dominated by the military, members of which occupy about half of Bolsonaro's 22 cabinet seats. Military dictatorships are a not-too-distant memory in Latin America. Says Katitza Rodríguez, a Peruvian who is international rights director for the Electronic Frontier Foundation: "History has taught us that our democracies are not that strong."

Richard Kemeny is a freelance journalist based in São Paulo, Brazil.


У

YANDEX'S BALANCING ACT

THE UNEASY COEXISTENCE OF RUSSIA'S TECH GIANT WITH THE KREMLIN



By **EVAN GERSHKOVICH**
Illustrations by Marcin Wolski

From the end of March until mid-June, while Moscow was under coronavirus lockdown, the Russian capital emptied out—mostly. On walks to the supermarket or pharmacy I was passed by streams of cyclists in the trademark yellow uniform of Yandex's food delivery service. On the road, the few vehicles aside from police cars or buses were the taxis—disinfected at newly opened stations—of Yandex's ride-hailing company.

Often referred to in the West as Russia's Google, Yandex is really more like Google, Amazon, Uber, and maybe a few other companies combined. Russians query Alice, the company's virtual assistant, to help them order goods online in Yandex Market. They use its email system, listen to its music player, and visit its movie-recommending website. Over coffee, they read the morning news on the Yandex News aggregator. They send each other money through Yandex Wallet. And they find their way via Yandex Navigator, a tool analogous to Google Maps. Arkady Volozh, CEO and cofounder of the Nasdaq-traded company, has described it not simply as part of Russia's Silicon Valley, but as a Russian Silicon Valley unto itself.

New services appear at breakneck speed. Around Moscow, Yandex is testing a fleet of over 100 driverless cars, work that even the coronavirus was unable to pause. Yandex Lavka ("Yandex Shop"), a grocery delivery app that launched in June last year, guarantees deliveries within 15 minutes, faster than anything Amazon offers. One of the brains behind the project, Ilya Krasilshchik, 33, remembers how, during Russia's turbulent transition to a market economy in the early 1990s, his mother returned from a trip with a bucket of cocoa powder just in case the family wouldn't be able to get it at home. Now, decades later, Muscovites have excess at their fingertips: Lavka's most popular item in the summer of 2019 was quartered watermelon—delivered cold, of course.

On a snowy afternoon in late February, just before the pandemic gripped Russia, I turned off of a busy Moscow street into a quiet courtyard. I was meeting Rostislav Meshchersky, the 28-year-old manager of one of Lavka's so-called "dark stores," the places where the products ordered online are discreetly warehoused for distribution. Meshchersky led me to an open garage door at the back of the courtyard, which led down into a basement lined with shelves filled with everything from pasta to fruit juice to toilet paper. "I joke with my friends that I know immediately where to go in Moscow in the event of the apocalypse," he said.

Just weeks later, it wasn't such a joke. In April, Lavka received some 900,000 orders from Russians stuck at home under quarantine, while customers of Yandex's overall food services—restaurant delivery included—more than doubled. Although the company took a hit in businesses like ride-sharing when its entire fleet was taken off the streets during Russia's lockdown, the people stuck at home boosted traffic on the company's search and streaming video platforms.

But Yandex's success has come at a price. The Kremlin has long viewed the internet as a battlefield in its escalating tensions with the West and has become increasingly concerned that a company like Yandex, with the heaps of data it has on Russian citizens, could one day fall into foreign hands.

This means running a tech giant in Russia is a delicate dance. On the one hand is the Kremlin; on the other is New York, with investors' demands that the company maintain its independence. But in a pandemic-stricken world increasingly concerned with protecting borders and regulating the tech industry, Yandex's dilemma may not be just a Russian story.

Yandex's food-delivery cyclists remained ubiquitous on Moscow's streets even during the covid-19 lockdown.

ANATOLY ZHDANOV/KOMMERSANT/SIPA USA

A GOLDEN ARRANGEMENT

Yandex—short for "yet another indexer"—didn't always have its fingers in everything. After getting its start in 1997, the company for years vied for local search-engine supremacy with Rambler, another Russian company.

In the end, Rambler became the Yahoo to Yandex's Google. But Google itself soon entered the market, and while Yandex had an edge by rooting its search algorithm in the particulars of the Russian language, its California rival began to catch up. "About half a year before Google went public, it made an offer to buy Yandex, and I have to say that we were looking at that offer very seriously," Leonid Boguslavsky, one of the company's first investors, told me.

The offer was made in 2003. But one of Yandex's cofounders, Ilya Segalovich, said, "Let's fight," Boguslavsky recalled. Though Segalovich died in 2013 after a bout with stomach cancer, the fight continues to this day: while Google has periodically overtaken Yandex, the Russian firm currently has about 59% of Russian search traffic to Google's 39%.

The same year Segalovich died, Yandex hired Greg Abovsky, a Ukraine-born, Harvard Business School–educated hedge fund analyst who got his start with Morgan Stanley in New York. "We had a realization right around the time I got here that search is going to slow down at some point," says Abovsky, who now serves as both CFO and COO. When he joined, advertising from search accounted for around 99% of the company's revenue. Today it's about 64%, and total revenue grew from $1.2 billion in 2013 to $2.8 billion in 2019.

But as Yandex developed into the dominant player in the Russian tech market, it also inevitably came under the watchful eye of the authorities.

One of the first moments was in August 2008, when Russia fought a five-day war with neighboring Georgia. As the conflict played out, Yandex News featured Russian-language articles covering both sides of the divide. The next month, according to journalists Andrei Soldatov and Irina Borogan in their book *The Red Web*, two Kremlin officials visited Yandex's headquarters. One was Vladislav Surkov, the deputy chief of Russia's presidential administration—the man who coined the Orwellian term "sovereign democracy" to describe a Russian system of governance that brooks no foreign meddling in its affairs.

Lev Gershenzon, the director of Yandex News at the time, was given the task of explaining to the official visitors how the service worked. According to the book, he recalled showing screenshots of articles that the aggregator's algorithm had selected as top stories. Surkov interrupted. "This is our enemy," he said, pointing to a liberal outlet. "That's what we do not need!"

IN 2008, WHEN RUSSIA FOUGHT A FIVE-DAY WAR WITH GEORGIA, YANDEX NEWS FEATURED RUSSIAN-LANGUAGE ARTICLES COVERING BOTH SIDES OF THE DIVIDE. THE NEXT MONTH, TWO KREMLIN OFFICIALS VISITED YANDEX'S HEADQUARTERS.

The company promised from then on to maintain an open line to the Kremlin, though Gershenzon said he would always reiterate that an algorithm, not a person, chose the top news. Still, he didn't always agree with how the line of communication was maintained.

"Volozh and I went to the presidential administration building several times and I said to him, 'Listen, you have such a powerful business—why do you go to them? If it's really needed, let them come to you,'" Gershenzon recalled in *Holy War*, a documentary miniseries about the Russian-language internet. "Even a geek like me knew that if you bend over for them they'll never let you bend back upright again."

That same year, Yandex fought off a potential takeover by Kremlin-linked oligarch Alisher Usmanov, who lobbied for President Dmitry Medvedev's support on national security grounds. In 2009, to satisfy government interests, Yandex handed Russia's largest lender, the state-owned Sberbank, a so-called golden share, which allowed the bank to veto transactions involving more than a quarter of Yandex's stock. For a decade that arrangement appeased the Russian authorities—until it no longer did.

THE TIGHTROPE WALK

Last May, Russia passed a law to create a so-called "sovereign internet," a state-owned communications infrastructure that would allow the country to cut itself off from the global internet while remaining online in a bubble of Russian-owned services. The law requires internet service providers to install equipment provided by the government for counteracting broadly defined "threats" to the internet's stability and integrity, and gives the authorities sweeping powers to take control of the network if such threats appear. Over tea at his offices one afternoon last winter, Igor Ashmanov, who was the director of Yandex's rival Rambler for a time in the early aughts and now is a proponent of the sovereign internet on state television and in government hearings, laid out its purpose.

"Imagine you live in a small village near a city that provides your electricity, and the mayor of the city has said that you are his enemies and that if he can harm you, he will," Ashmanov told me. "You might decide to buy a generator to make sure your electricity keeps running in case this crazy mayor turns off the switch. This is what the sovereign internet is about."

Perhaps more important to the Kremlin, the sovereign internet would also give Russia more control over what its own citizens can see online. In 2011 the Arab Spring,

buoyed by social media, swept across the Middle East. That December, after Vladimir Putin announced he would run for president once again following an interim stint as prime minister, mass protests—planned on Facebook—rocked Russia. In the wake of the demonstrations, the Kremlin began to see foreign tech companies as tools used by other governments to meddle in its affairs. Putin himself vocalized those concerns at a press conference in 2014, when he described the internet as a "CIA project" and implied that Yandex itself had been "pressured" to include foreigners in its management and was registered overseas "not only for tax purposes but for other reasons." (The parent company is incorporated in the Netherlands, and six of the 12 current board members are non-Russians, including John Boynton, the chairman, who is based in Massachusetts.)

That fear of foreign interference has only intensified over the years. During a government hearing on national security in 2018, Ashmanov described Facebook, Instagram, and Twitter as American weapons trained against Russia. "What the Americans could do with a company like Yandex in their hands is something I don't even want to think about," Ashmanov told me.

As the ground shifted under its feet, Yandex struggled to keep its balance, according to Boynton, the board chairman. "We've done everything we can to steer clear of politics," he said in a phone interview. And yet, he added, the company found that it was increasingly getting "dragged into areas where we don't necessarily want to be."

Things came to a head on a Thursday morning in October 2018, when rumors leaked that Sberbank was in talks to buy up to a 30% stake in Yandex to protect the company from "potential trouble." When trading opened up in New York, its shares plummeted 9.4%, losing over $1 billion in market value, over fears that the state lender could take control of the company. "That was the moment when we realized that there was something bigger afoot," Boynton recalled.

IN FEBRUARY, A POLICEMAN ACCUSED OF PLANTING DRUGS ON AN INVESTIGATIVE REPORTER SAID HE HAD FOUND THE JOURNALIST'S ADDRESS BY ASKING YANDEX TAXI TO PROVIDE IT.

The next day the company lost another $1 billion. At an emergency meeting that went into the early hours of Saturday, the Financial Times reported, Volozh decided not to pursue the Sberbank deal.

Yandex began talks with Putin's administration over a new governance structure, but the pressure on it continued to intensify. In June 2019, a little-known lawmaker, Anton Gorelkin, introduced a bill to limit foreign ownership in companies that the Russian government deemed "significant information resources." Outside investors would be allowed to own only 20% of such companies—a severe blow to Yandex, which had 85% of its shares trading on US markets. When the Kremlin came out in support of Gorelkin's law a few months later, fears in New York wiped another $1.5 billion off Yandex's valuation in a single day.

In November last year, after 13 months of grueling negotiations, Yandex announced a solution. It would hand over Sberbank's golden share—that veto power over major transactions—to a newly formed "public interest foundation" with close government ties. The veto would also be beefed up to include deals and transactions relating to intellectual property or the transfer of Russian users' data. Although the new foundation would have 11 seats on its board, only three would belong to Yandex; the rest would be divided up among influential business groups and state-affiliated universities. Perhaps most important from the Kremlin's perspective, the new foundation would be able to block Yandex from entering into agreements with any foreign government.

That seemed to take the heat off. Gorelkin said he would take his law back to the drawing board. Days later, the Russian parliament passed a law requiring Russian tech to be automatically preloaded onto devices sold in Russia, a move that analysts calculated would boost Yandex's valuation by $1.4 billion. A few weeks after that, Putin, who had criticized Yandex's foreign ties a few years earlier, praised its projects with foreign partners and spoke positively of a closed-door meeting with its senior management.

Yet even if the Kremlin seems to have been appeased, not everyone is. Power in Russia's government is split between rival groups, with Putin mediating between them. For the constituency known as the *siloviki*—officials with ties to law enforcement—the Yandex foundation was seen as a half-victory, says Tatiana Stanovaya, the founder of a political analysis site, R.Politik. "On the one hand, they see that Yandex is indirectly beholden to the government," she says. "On the other hand, it's purely technical. Yandex won't

just fulfill any and all demands. And if the confrontation with the West keeps escalating, [the authorities] may rethink this arrangement."

When I spoke with Boynton last winter after the dust had settled, he was in a buoyant mood. But he also noted that things could quickly change again. "In Russia," he said, "nothing is guaranteed."

A TEMPLATE FOR BIG TECH?

If the *siloviki* see Yandex as an unreliable collaborator, liberal critics see increasing signs that it is in the pocket of the authorities. In late February, for example, a policeman accused of planting drugs on an investigative reporter said he had found the journalist's address by asking Yandex Taxi to provide it. Yandex responded that it always yields to requests by security services to "help save lives," though Roskomsvoboda, an anti-censorship group, pointed out that it is not always legally required to do so.

As the pandemic grew, questions about the company's independence became only more pointed. In early April, news surfaced that Moscow authorities were considering surveilling foreign tourists via their cellphone data once borders opened back up again—and that Yandex might develop the tool. The company denied the claim.

Then, when critical comments from opposition activists began popping up next to government buildings in Yandex Navigator, as a sort of digital alternative to street protests, Yandex deleted the messages, saying they were off-topic. Finally, one evening in late April, some internet users noticed that searches on Yandex for opposition leader Alexei Navalny were returning mostly negative content. Yandex apologized, saying that it was an "experiment" shown only to a small number of users. One Russian commentator, Alexander Plushev, noted that such testing is common on all tech platforms, but he added: "Any incident with Yandex is now interpreted through the prism of its control by the authorities."

If Yandex capitulates too much to state control, it risks losing its most prized asset: its talent. "I always say that my main competitors are [Moscow airports] Sheremetyevo and Domodedovo," says Misha Bilenko, who heads Yandex's Machine Intelligence and Research division.

Bilenko himself spent 23 years in the United States, including a decade at Microsoft, before returning to Russia several years ago. What drew him back, he says, was the access to so many different resources within Yandex and the opportunity to help improve the lives of Russians en masse. But as one employee who asked to speak anonymously told me, Yandex would lose that type of draw and power if the government tried too hard to tame it. "We have a lot of progressive people here," the person said. "If we don't like what we see, we'll leave."

Today Yandex, at least publicly, is claiming that all is well. Its concessions to the Kremlin could have been much bigger. They're also ones that others may soon consider. "What Yandex has done isn't only relevant within the context of Putin's Russia," Bloomberg columnist Leonid Bershidsky argued last year. "It could be seen as a template for Big Tech."

Like Yandex, Bershidsky continued, companies such as Google or Facebook could set up quasi-autonomous governance structures with the right to veto certain decisions. "If such a structure can win approval even from an authoritarian regime such as the Russian one … it could probably satisfy most Big Tech critics in democracies, too," he wrote.

Indeed, in May of this year Facebook named the first members of its "oversight board" as a response to anger over its opaque content moderation process. The body is stacked with legal and human rights luminaries who can review and overturn some of the platform's decisions. Though the board has nothing like the power of Yandex's public interest foundation, it was a big concession from a company that has always fiercely defended its control over what goes on its platform.

With politicians on both ends of the US political spectrum calling for increasing regulation of Big Tech, such moves are likely to keep happening. The kind of flexibility Yandex has had to learn may prove essential for companies that want to not only survive but flourish.

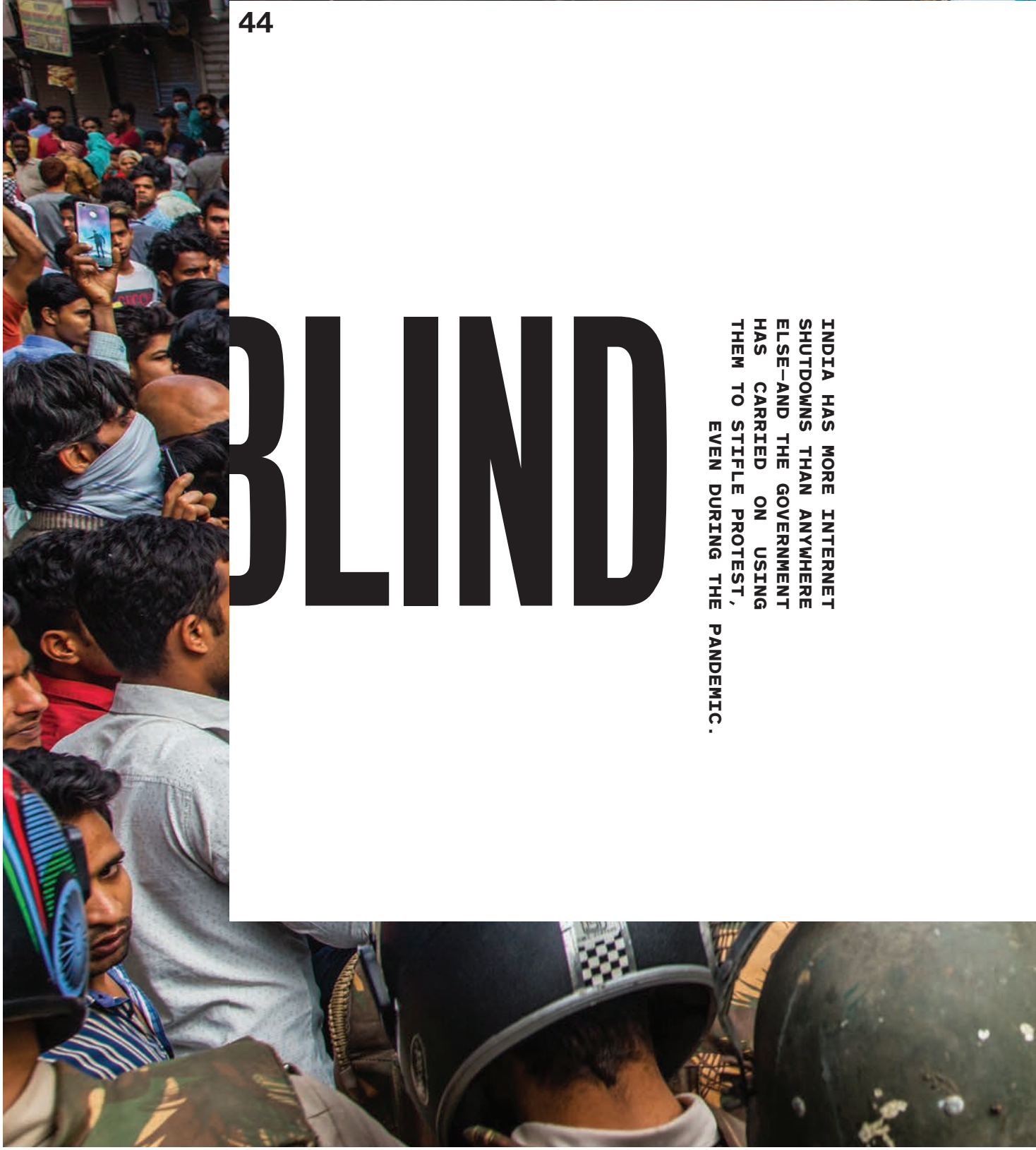
ITAR-TASS NEWS AGENCY/ALAMY STOCK PHOTO

Yandex CEO Arkady Volozh (left) with President Vladimir Putin, who was visiting Yandex's offices in 2017 to mark its 20th anniversary.

Evan Gershkovich is a reporter for the Moscow Times. His work can also be found in the New York Times, Foreign Policy, and Politico Europe, among other publications.

BLIND

INDIA HAS MORE INTERNET SHUTDOWNS THAN ANYWHERE ELSE—AND THE GOVERNMENT HAS CARRIED ON USING THEM TO STIFLE PROTEST, EVEN DURING THE PANDEMIC.



SPOT

BY SONIA FALEIRO

Spring arrived, as always in the Kashmir Valley, with melting snow and blossoming chinar trees. This year, though, brought something new. On March 18, in Srinagar, the largest city in the Himalayan region of Kashmir, a man tested positive for covid-19—the first in the valley. The mayor asked everyone to stay home, but the message didn't travel widely. Communication across Kashmir was limited, mobile-phone services were often disrupted, and internet speeds were stuck at a plodding 2G. So although some Kashmiris followed the order to shelter in place, many had no idea they were at risk. "We knew nothing about the virus," says Omar Salim Akhtar, a urologist at the Government Medical College in Srinagar. "Even health workers were helpless. We had to ask people traveling outside Kashmir to download the medical guidelines and bring back printouts."

The Indian government had imposed a communications shutdown in Kashmir last August in an attempt to suppress dissent in the volatile region. The shutdown was total—no mobile internet, broadband, landlines, or cable TV. Akhtar was detained during a demonstration (his placard read "This is not a protest, this is a request, patients are suffering") but released without charge. The shutdown lasted until January, making it the longest internet blackout ever seen in the democratic world.

After partly restoring internet connectivity, the government initially banned the use of social media, and several people who violated the ban by masking their location were arrested under anti-terror laws. At the time of writing, connection speeds continue to be heavily throttled.

But as the coronavirus spread, the information blockade itself became a threat to public safety. The day after the valley's first diagnosis, Amnesty International asked the government to restore access. "The right to health," it said in a statement, "provides for the right to access healthcare [and] access to health-related information." The government didn't oblige.

India's nationwide lockdown was still a week away, but outside Kashmir most people had no problems with internet access. They were already scrambling to move their work and classes online. In Kashmir, though, where even downloading Zoom was a struggle, switching schoolrooms or businesses to the internet was a nonstarter.

The information vacuum left people bewildered and prone to believing the swirling rumors. "On the one hand, people were saying that the virus was a plot to earn money from a vaccine and that everyone should continue visiting the mosque and attending weddings," says Akhtar. "Others got busy drawing up wills and wanting to dig mass graves."

The Indian government claims the slow speeds, service limitations, and blackouts are necessary to maintain peace. Kashmir, a disputed region on the border of India and Pakistan, is subject to regular outbreaks of violence, and some Kashmiris who support a movement for independence use social media to organize. The government in Delhi argues that without connectivity, the independence movement will come to a halt.

Even if that were true—the movement predates social media by decades—the shutdowns also bring normal life to a standstill. After the region suffered billions of dollars' worth of economic losses because of the August blackout, it was hard for locals to see the government's actions as anything but a collective punishment.

Samreen Hamdani, a 30-year-old mechanical engineer, is one of those who felt that retribution. When the shutdown was imposed, she was teaching applied mathematics at a women's polytechnic in Srinagar. Life was busy—she also ran a nonprofit to bring education to rural areas—and the days didn't seem long enough. Then the blackout happened.

"Losing the internet is like losing the ability to talk," Hamdani says. "It's like losing the ability to walk."

The school canceled classes, and she had to let her nonprofit employees go. She didn't have a plan B: her life was too closely entwined with the internet. Her once-packed days became a cycle of waking, eating, and sleeping, with little else to do or look forward to.

For years, many Indians bought the government line that internet shutdowns in Kashmir curb violence and save lives. But in 2018, instead of being limited to the volatile valley, they began taking place all over India. According to user-reported figures, there were 134 internet blackouts in more than half a dozen Indian states that year, and a further 106 of them across more than 10 states in

YAWAR NAZIR/GETTY IMAGES

Clashes between those who support the rights of Indian Muslims and the police, like this confrontation in Delhi in March, continued despite the nationwide lockdown.

BEFORE THE LOCKDOWN, MOST OF INDIA WAS SCRAMBLING TO MOVE ONLINE. IN KASHMIR, THE BLACKOUT MEANT THAT SWITCHING SCHOOLS AND BUSINESSES TO THE INTERNET WAS A NONSTARTER.

2019. Hundreds of millions of people were affected. That makes India, a democracy, the world leader in such shutdowns—ahead of China, Iran, and Venezuela. And it has become harder for ordinary Indians to dismiss the people affected as a threat to national security—because it's happening to them, in their own cities, in their own homes.

At 3:50 a.m. on December 19, 2019, Kishi Arora was woken up by a text message from her mobile-phone company. The government, it said, was shutting down internet access in her neighborhood. Arora had followed the many shutdowns in Kashmir but never imagined that she would experience one in Delhi, the national capital.

Although dawn was yet to break, she immediately set to thinking about what a blackout would mean for her and her work. A hugely popular pastry chef, Arora had built her business online: she had 160,000 followers on Twitter, 17,000 on Facebook, and 24,000 on Instagram. Her team spent their days taking orders (many through social media), making food, and delivering it to customers all over the city. The text didn't mention how long the blackout would last, and as Arora imagined the digital orders for her signature cheesecake steadily piling up, she felt her concerns pulsate like a headache.

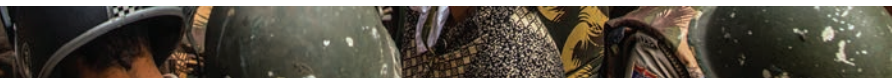
How would she keep in touch with her mother, an ailing widow, when she was at work? Her siblings lived abroad, and the close-knit family chatted throughout the day over WhatsApp; what would they do?

It was clear why the shutdown was happening: thousands of people were in the streets protesting the passage of a controversial new immigration law, the Citizenship (Amendment) Act of 2019, and things in the capital had become fractious. The CAA was a scheme to put persecuted minorities who had arrived from Bangladesh, Pakistan, and Afghanistan on a fast track to citizenship—unless they were Muslims, who had to go through the onerous normal channels.

On top of this, the government said it would start immigration checks across the entire country, even in states with little to no history of undocumented immigration, and planned to send those who could not prove they were either Indian citizens or eligible for fast-tracking into mass detention camps. In a country where many poor people don't have documents to prove that they even exist (according to one report, only 62% of Indian children under the age of five have birth certificates), millions were at risk of failing the check.

The potential consequence for many of India's 200 million Muslims was clear: they could become stateless people, treated like the Uighur Muslim minority in China. India is a secular republic, but Prime Minister Narendra Modi, an avowed Hindu nationalist who joined a known supremacist group when he was just eight years old, was turning it into a majoritarian Hindu state.

When protests against the CAA took off, the government turned to the tactic it had used elsewhere: shutting off the internet. There were shutdowns in India's largest state, Uttar Pradesh; in Modi's home state, Gujarat; and even in Karnataka, whose tech-friendly



capital, Bengaluru, is known as the Silicon Valley of India.

As Arora realized the extent of the Delhi shutdown, she worried for her own security as well as for her business. The city was already notoriously unsafe for women, and as the antigovernment protests continued, the khaki-uniformed police had responded to peaceful chants and demonstrations with live rounds, tear gas, and smoke grenades. Across the country the police had already killed 25 protesters.

That day, a prominent march was planned at the historic Red Fort, where India's prime minister traditionally hoists the flag on Independence Day. In the morning, Nikhil Pahwa, a friend of Arora's who worked as a digital rights activist, had tweeted, "Telecom operators have confirmed to us: The Internet is being shut down in parts of Delhi. Not sure of which areas. Awaiting update."

It turned out that not all service operators had made the effort to tell users in advance. Many of the estimated 1.7 million people affected started their day in an information black hole.

The shutdown didn't cover the entire city—only those areas with a large Muslim population. "The idea was to stop them communicating as they roamed around," says Danish Khan, a reporter with the Economic Times newspaper. His neighborhood had experienced a blackout that morning. "They didn't want people to mobilize quickly or share pictures and videos," he adds.

News of what the government had surreptitiously done only spurred people on. Hundreds of protesters gathered, but many of them were immediately taken into custody. While still standing on the street trying to catch a Wi-Fi signal, Arora thought of the two young Muslim women who worked for her. Would they be safe at home without the internet, or outside where the police roamed? Sometimes, she says, it became difficult to remember that she lived in a democracy.

135 years in the making

When the Indian government wants to plunge the public into a digital darkness, all it has to do is invoke one law.

The Indian Telegraph Act of 1885 gives the federal and state governments the right to "prevent the transmission of any telegraphic message or class of messages during a public emergency or in the interest of public safety." The British created the law and found it a useful tool for stopping uprisings during the colonial era. Later, Indian governments used it to wiretap citizens, including opposition politicians and journalists. In 2017, the law was amended to specify that it allowed "the temporary suspension of telecom services."

The Software Freedom Law Center (SFLC), a Delhi-based digital rights group, says that there are two official explanations for a shutdown: public safety and public emergency. The government either claims that misinformation circulating on social media and WhatsApp is likely to cause violence, or that an ongoing violent situation can only be brought under control by closing down communications.

Stopping violence was at least sometimes the goal when shutdowns started to increase in 2018. In June that year, two tourists were murdered in the northeastern state of Assam following rumors on WhatsApp of child kidnappers on the prowl. When two more people were beaten the next day, apparently on the same suspicion, the government shut off the state's internet to stop the rumors from spreading.

Over the next few months, similar messages and fake videos of so-called "child lifters" popped up as WhatsApp forwards in many other states. By the end of 2019, such rumors were linked to at least 70 violent incidents, according to analysis by the data journalism website IndiaSpend.

The episode highlighted a burgeoning epidemic of fake news in India, stoked by a price war in 2016 among phone operators that had slashed the cost of mobile data and brought hundreds of millions of new people online. The internet, which had been the domain of the educated and wealthy, was now everywhere: vegetable vendors streamed Bollywood films as they parceled tomatoes and onions, and auto rickshaw drivers scrolled YouTube videos while they waited for their next customer. Today Indian mobile data is the cheapest in the world, and the average social-media user spends 17 hours on the platforms each week, more than people in China.

This dramatic expansion exposed the widespread lack of information literacy. The concept of online disinformation is largely unknown to Indians outside major cities, and while WhatsApp has taken steps to limit the spread of fake news, the government continues to deal with it through shutdowns rather than attempting education, investing in computer literacy, or even just using social media to set the record straight.

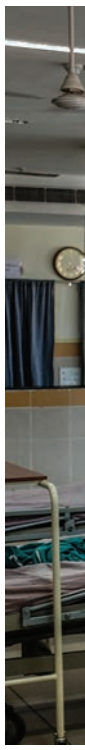
And increasingly, as the shutdowns in Delhi and elsewhere show, the authorities are now using the tactic not only to curb violence but also to suppress dissent. There is no true legal recourse: the Telegraph Act doesn't limit how long a shutdown can last, and although there is a committee that reviews such actions, it is staffed by bureaucrats and rarely diverges from the government line.

Telecom companies themselves are badly affected by shutdowns: one estimate says they lost $350,000 every hour that the internet was down during the 2019 protests. However, they offer virtually no resistance to the state. One company, Airtel, even went back and deleted tweets in which it had informed customers of the Delhi shutdown.

Even the courts respond halfheartedly. When the SFLC filed a writ arguing that the Delhi shutdown violated fundamental rights to freedom of speech and life, the case was dismissed on the grounds that the shutdown had already been lifted. In January of this year, the Supreme Court declared the Kashmir blackout illegal, but when the government switched communications back on it kept the internet throttled to unusable speeds, and faced no consequences.

Berhan Taye, a senior policy analyst at the digital rights nonprofit Access Now, says there is "a direct correlation between shutdowns and human rights violations."

In Kashmir, even now, it's difficult to say exactly how many people were detained during the months-long blackout. The government's own figures say there were 5,116 "preventive arrests," but campaigners



ATUL LOKE/THE NEW YORK TIMES/REDUX

do not believe this accounts for everybody. In Uttar Pradesh, the police arrested more than 100 people in just a single day of protests in January and beat some brutally in public view. Without the internet, however, it was difficult to get the news out.

Jan Rydzak, a research analyst at the human rights nonprofit Ranking Digital Rights, says it's important that people continue to protest government excesses. "We have to keep showing that shutdowns aren't effective for the government's purposes," he says. Otherwise, he warns, they could begin to cascade. First, other democracies in the region may formalize systems to close off the internet rather than rely on broad public safety laws. Then, as such tactics spread, the balance around the world could shift. Instead of one or two blackouts globally, there could be prolonged siege-like blockades, and "a continuous stream of ephemeral shutdowns that will never end."

This year, the pandemic has slowed the rate of shutdowns—but it has not stopped them. The Indian government has already shut off the internet on 35 separate occasions, 26 of them in Kashmir. Even as the number of confirmed covid-19 cases in Jammu and Kashmir crossed 13,000 and the death toll passed 200 in mid-July, the government refused to restore 4G internet speeds. In May, the Supreme Court referred a judgment on a petition calling for the restoration of full service to a committee of government-appointed officials—in essence asking the government to decide whether or not its own actions were lawful. To no one's surprise, the committee said the current 2G speed doesn't "pose any hindrance to Covid-19 control measures."

Akhtar, the doctor in Srinagar, disagrees. On May 19, around two months into the pandemic, he stepped out of the operating theater and reached for his mobile phone, only to realize that he couldn't load his emails. He immediately understood that the city was in the midst of another internet shutdown.

Usually he would call around to see if anyone knew what was going on. This time, however, even making a phone call was impossible. It turned out that security personnel had shot dead two suspected militants in downtown Srinagar, and the government had turned off all connectivity to prevent the news from circulating and protesters from gathering.

Standing in his scrubs, Akhtar had no idea when, or if, he would get back on the grid.

Since the start of the pandemic he had felt handicapped, almost entirely reliant on others to give him health-care updates. He didn't have the latest research. Now, even his phone was useless. The world was in the middle of one deadly crisis, but faced with everyday violence, surrounded by security forces, and cut off from sources of information, it seemed to Akhtar that Kashmir was in the middle of two.

IF OTHER COUNTRIES ARE INSPIRED BY INDIA'S EXTENDED AND EXTENSIVE BLOCKADES, THE WORLD COULD FACE A "CONTINUOUS STREAM OF EPHEMERAL SHUTDOWNS THAT WILL NEVER END."

Omar Akhtar, a urologist, has been vocal about the impact of shutdowns. In 2019, he was detained for protesting. In 2020, he worried about further blackouts during the crisis.

Sonia Faleiro is the author of Beautiful Thing: Inside the Secret World of Bombay's Dance Bars. Her new book The Good Girls: An Ordinary Killing will be released in January 2021.

Photo by Stefen Chow

CHINA'S DATA PRIVACY PARADOX

Even as the Chinese surveillance state grows more intrusive, the laws protecting consumers' personal data are getting stronger. Can both these things keep happening?

By Karen Hao

Late in the summer of 2016, Xu Yuyu received a call that promised to change her life. Her college entrance examination scores, she was told, had won her admission to the English department of the Nanjing University of Posts and Telecommunications. Xu lived in the city of Linyi in Shandong, a coastal province in China, southeast of Beijing. She came from a poor family, singularly reliant on her father's meager income. But her parents had painstakingly saved for her tuition; very few of her relatives had ever been to college.

A few days later, Xu received another call telling her she had also been awarded a scholarship. To collect the 2,600 yuan ($370), she needed to first deposit a 9,900 yuan "activation fee" into her university account. Having applied for financial aid only days before, she wired the money to the number the caller gave her. That night, the family rushed to the police to report that they had been defrauded. Xu's father later said his greatest regret was asking the officer whether they might still get their money back. The answer – "Likely not" – only exacerbated Xu's devastation. On the way home she suffered a heart attack. She died in a hospital two days later.

An investigation determined that while the first call had been genuine, the second had come from scammers who'd paid a hacker for Xu's number, admissions status, and request for financial aid.

For Chinese consumers all too familiar with having their data stolen, Xu became an emblem. Her death sparked a national outcry for greater data privacy protections. Only months before, the European Union had adopted the General Data Protection Regulation (GDPR), an attempt to give European citizens control over how their personal data is used. Meanwhile, Donald Trump was about to win the American presidential election, fueled in part by a campaign that relied extensively on voter data. That data included details on 87 million Facebook accounts, illicitly obtained by the consulting firm Cambridge Analytica. Chinese regulators and legal scholars followed these events closely.

Hong Yanqing (left) led a task force on data privacy.

In the West, it's widely believed that neither the Chinese government nor Chinese people care about privacy. US tech giants wield this supposed indifference to argue that onerous privacy laws would put them at a competitive disadvantage to Chinese firms. In his 2018 Senate testimony after the Cambridge Analytica scandal, Facebook's CEO, Mark Zuckerberg, urged regulators not to clamp down too hard on technologies like face recognition. "We still need to make it so that American companies can innovate in those areas," he said, "or else we're going to fall behind Chinese competitors and others around the world."

In reality, this picture of Chinese attitudes to privacy is out of date. Over the last few years the Chinese government, seeking to strengthen consumers' trust and participation in the digital economy, has begun to implement privacy protections that in many respects resemble those in America and Europe today.

Even as the government has strengthened consumer privacy, however, it has ramped up state surveillance. It uses DNA samples and other biometrics, like face and fingerprint recognition, to monitor citizens throughout the country. It has tightened internet censorship and developed a "social credit" system, which punishes behaviors the authorities say weaken social stability. During the pandemic, it deployed a system of "health code" apps to dictate who could travel, based on their risk of carrying the coronavirus. And it has used a slew of invasive surveillance technologies in its harsh repression of Muslim Uighurs in the northwestern region of Xinjiang.

This paradox has become a defining feature of China's emerging data privacy regime. It raises a question: Can a system endure with strong protections for consumer privacy, but almost none against government snooping? The answer doesn't affect only China. Its technology companies have an increasingly global footprint, and regulators around the world are watching its policy decisions.

November 2000 arguably marks the birth of the modern Chinese surveillance state. That month, the Ministry of Public Security, the government agency that oversees daily law enforcement, announced a new project at a trade show in Beijing. The agency envisioned a centralized national system that would integrate both physical and digital surveillance using the latest technology. It was named Golden Shield.

Eager to cash in, Western companies including American conglomerate Cisco, Finnish telecom giant Nokia, and Canada's Nortel Networks worked with the agency on different parts of the project. They helped construct a nationwide database for storing information on all Chinese adults, and developed a sophisticated system for controlling information flow on the internet—what would eventually become the Great Firewall. Much of the equipment involved had in fact already been standardized to make surveillance easier in the US—a consequence of the Communications Assistance for Law Enforcement Act of 1994.

Despite the standardized equipment, the Golden Shield project was hampered by data silos and turf wars within the Chinese government. Over time, the ministry's pursuit of a singular, unified system devolved into two separate operations: a surveillance and database system, devoted to gathering and storing information, and the social-credit system, which some 40 government departments participate in. When people repeatedly do things that aren't allowed—from jaywalking to engaging in business corruption—their social-credit score falls and they can be blocked from things like buying train and plane tickets or applying for a mortgage.

The Chinese government has begun to implement privacy protections that resemble those in America and Europe today.

In the same year the Ministry of Public Security announced Golden Shield, Hong Yanqing entered the ministry's police university in Beijing. But after seven years of training, having received his bachelor's and master's degrees, Hong began to have second thoughts about becoming a policeman. He applied instead to study abroad. By the fall of 2007, he had moved to the Netherlands to begin a PhD in international human rights law, approved and subsidized by the Chinese government.

Over the next four years, he familiarized himself with the Western practice of law through his PhD research and a series of internships at international organizations. He worked at the International Labor Organization on global workplace discrimination law and the World Health Organization on road safety in China. "It's a very legalistic culture in the West—that really strikes me. People seem to go to court a lot," he says. "For example, for human rights law, most of the textbooks are about the significant cases in court resolving human rights issues."

Hong found this to be strangely inefficient. He saw going to court as a final resort for patching up the law's inadequacies, not a principal

An epidemic control worker checks the temperatures of people waiting in line to be tested for covid-19 in the Xicheng district of central Beijing.

KEVIN FRAYER/GETTY IMAGES

tool for establishing it in the first place. Legislation crafted more comprehensively and with greater forethought, he believed, would achieve better outcomes than a system patched together through a haphazard accumulation of case law, as in the US.

After graduating, he carried these ideas back to Beijing in 2012, on the eve of Xi Jinping's ascent to the presidency. Hong worked at the UN Development Program and then as a journalist for the People's Daily, the largest newspaper in China, which is owned by the government.

Xi began to rapidly expand the scope of government censorship. Influential commentators, or "Big Vs"—named for their verified accounts on social media—had grown comfortable criticizing and ridiculing the Chinese Communist Party. In the fall of 2013, the party arrested hundreds of microbloggers for what it described as "malicious rumor-mongering" and paraded a particularly influential one on national television to make an example of him.

The moment marked the beginning of a new era of censorship. The following year, the Cyberspace Administration of China was founded. The new central agency was responsible for everything involved in internet regulation, including national security, media and speech censorship, and data protection. Hong left the People's Daily and joined the agency's department of international affairs. He represented it at the UN and other global bodies and worked on cybersecurity cooperation with other governments.

By July 2015, the Cyberspace Administration had released a draft of its first law. The Cybersecurity Law, which entered into force in June of 2017, required that companies obtain consent from people to collect their personal information. At the same time, it tightened internet censorship by banning anonymous users—a provision enforced by regular government inspections of data from internet service providers.

In the spring of 2016, Hong sought to return to academia, but the agency asked him to stay. The Cybersecurity Law had purposely left the regulation of personal data protection vague, but consumer data breaches and theft had reached unbearable levels. A 2016 study by the Internet Society of China found that 84% of those surveyed had suffered some leak of their data, including phone numbers, addresses, and bank account details. This was spurring a growing distrust of digital service providers that required access to personal information, such as ride-hailing, food-delivery, and financial apps. Xu Yuyu's death poured oil on the flames.

The government worried that such sentiments would weaken participation in the digital economy, which had become a central part of its strategy for shoring up the country's slowing economic growth. The advent of GDPR also made the government realize that Chinese tech giants would need to meet global privacy norms in order to expand abroad.

Hong was put in charge of a new task force that would write a Personal Information Protection Specification (PIPS) to help solve these challenges. The document, though nonbinding, would tell companies how regulators intended to implement the Cybersecurity Law. In the process, the government hoped, it would nudge them to adopt new norms for data protection by themselves.

Hong's task force set about translating every relevant document they could find into Chinese. They translated the privacy guidelines put out by the Organization for Economic Cooperation and Development and by its counterpart, the Asia-Pacific Economic Cooperation; they translated GDPR and the California Consumer Privacy Act. They even translated the 2012 White House Consumer Privacy Bill of Rights, introduced by the Obama administration but never made into law. All the while, Hong met regularly with European and American data protection regulators and scholars.

Bit by bit, from the documents and consultations, a general choice emerged. "People were saying, in very simplistic terms, 'We have a European model and the US model,'" Hong recalls. The two approaches diverged substantially in philosophy and implementation. Which one to follow became the task force's first debate.

At the core of the European model is the idea that people have a fundamental right to have their data protected. GDPR places the burden of proof on data collectors, such as companies, to demonstrate why they need the data. By contrast, the US model privileges industry over consumers. Businesses define for themselves what constitutes reasonable data collection; consumers only get to choose whether to use that business. The laws on data protection are also far more piecemeal than in Europe, divvied up among sectoral regulators and specific states.

At the time, without a central law or single agency in charge of data protection, China's model more closely resembled the American one. The task force, however, found the European approach compelling. "The European rule structure, the whole system, is more clear," Hong says.

But most of the task force members were representatives from Chinese tech giants, like Baidu, Alibaba, and Huawei, and they felt that GDPR was too restrictive. So they adopted its broad strokes—including its limits on data collection and its requirements on data storage and data deletion—and then loosened some of its language. GDPR's principle of data minimization, for example, maintains that only necessary data should be collected in exchange for a service. PIPS allows room for other data collection relevant to the service provided.

PIPS took effect in May 2018, the same month that GDPR finally took effect. But as Chinese officials watched the US upheaval over the Facebook and Cambridge Analytica scandal, they realized that a nonbinding agreement would not be enough. The Cybersecurity Law didn't have a strong mechanism for enforcing data protection. Regulators could only fine violators up to 1,000,000 yuan ($140,000), an inconsequential amount for large companies. Soon after, the National People's Congress, China's top legislative body, voted to begin drafting a Personal Information Protection Law within its current five-year legislative period, which ends in 2023. It would strengthen data protection provisions, provide for tougher penalties, and potentially create a new enforcement agency.

After Cambridge Analytica, says Hong, "the government agency understood, 'Okay, if you don't really implement or enforce those privacy rules, then you could have a major scandal, even affecting political things.'"

Xu Yuyu, who died after being defrauded by a scammer, and her university acceptance letter.

The local police investigation of Xu Yuyu's death eventually identified the scammers who had called her. It had been a gang of seven who'd cheated many other victims out of more than 560,000 yuan using illegally obtained personal information. The court ruled that Xu's death had been a direct result of the stress of losing her family's savings. Because of this, and his role in orchestrating tens of thousands of other calls, the ringleader, Chen Wenhui, 22, was sentenced to life in prison. The others received sentences between three and 15 years.

Emboldened, Chinese media and consumers began more openly criticizing privacy violations. In March 2018, internet search giant Baidu's CEO, Robin Li, sparked social-media outrage after suggesting that Chinese consumers were willing to "exchange privacy for safety, convenience, or efficiency." "Nonsense," wrote a social-media user, later quoted by the People's Daily. "It's more accurate to say [it is] impossible to defend [our privacy] effectively."

In late October 2019, social-media users once again expressed anger after photos began circulating of a school's students wearing

SOHU.COM

brainwave-monitoring headbands, supposedly to improve their focus and learning. The local educational authority eventually stepped in and told the school to stop using the headbands because they violated students' privacy. A week later, a Chinese law professor sued a Hangzhou wildlife zoo for replacing its fingerprint-based entry system with face recognition, saying the zoo had failed to obtain his consent for storing his image.

But the public's growing sensitivity to infringements of consumer privacy has not led to many limits on state surveillance, nor even much scrutiny of it. As Maya Wang, a researcher at Human Rights Watch, points out, this is in part because most Chinese citizens don't know the scale or scope of the government's operations. In China, as in the US and Europe, there are broad public and national security exemptions to data privacy laws. The Cybersecurity Law, for example, allows the government to demand data from private actors to assist in criminal legal investigations. The Ministry of Public Security also accumulates massive amounts of data on individuals directly. As a result, data privacy in industry can be strengthened without significantly limiting the state's access to information.

The onset of the pandemic, however, has disturbed this uneasy balance.

On February 11, Ant Financial, a financial technology giant headquartered in Hangzhou, a city southwest of Shanghai, released an app-building platform called AliPay Health Code. The same day, the Hangzhou government released an app it had built using the platform. The Hangzhou app asked people to self-report their travel and health information, and then gave them a color code of red, yellow, or green. Suddenly Hangzhou's 10 million residents were all required to show a green code to take the subway, shop for groceries, or enter a mall. Within a week, local governments in over 100 cities had used AliPay Health Code to develop their own apps. Rival tech giant Tencent quickly followed with its own platform for building them.

"Has history ever shown that once the government has surveillance tools, it will maintain modesty and caution when using them?

The apps made visible a worrying level of state surveillance and sparked a new wave of public debate. In March, Hu Yong, a journalism professor at Beijing University and an influential blogger on Weibo, argued that the government's pandemic data collection had crossed a line. Not only had it led to instances of information being stolen, he wrote, but it had also opened the door to such data being used beyond its original purpose. "Has history ever shown that once the government has surveillance tools, it will maintain modesty and caution when using them?" he asked.

Indeed, in late May, leaked documents revealed plans from the Hangzhou government to make a more permanent health-code app that would score citizens on behaviors like exercising, smoking, and sleeping. After a public outcry, city officials canceled the project. That state-run media had also published stories criticizing the app likely helped.

The debate quickly made its way to the central government. That month, the National People's Congress announced it intended to fast-track the Personal Information Protection Law. The scale of the data collected during the pandemic had made strong enforcement more urgent, delegates said, and highlighted the need to clarify the scope of the government's data collection and data deletion procedures during special emergencies. By July, the legislative body had proposed a new "strict approval" process for government authorities to undergo before collecting data from private-sector platforms. The language again remains vague, to be fleshed out later—perhaps through another nonbinding document—but this move "could mark a step toward limiting the broad scope" of existing government exemptions for national security, wrote China scholars at New America, a think tank in Washington, DC.

Hong similarly believes the discrepancy between rules governing industry and government data collection won't last, and the government will soon begin to limit its own scope. "We cannot simply address one actor while leaving the other out," he says. "That wouldn't be a very scientific approach."

Other observers disagree. The government could easily make superficial efforts to address public backlash against visible data collection without really touching the core of the Ministry of Public Security's national operations, says Wang, of Human Rights Watch. She adds that any laws would likely be enforced unevenly: "In Xinjiang, Turkic Muslims have no say whatsoever in how they're treated."

Still, Hong remains an optimist. In July, he started a job teaching law at Beijing University, and he now maintains a blog on cybersecurity and data issues. Monthly, he meets with a budding community of data protection officers in China, who carefully watch how data governance is evolving around the world.

Karen Hao is a senior reporter at MIT Technology Review.

HOW CHINA SURVEILS THE WORLD

T R : Q + A

The government taps into a vast global array of data sources through partnerships with both foreign and domestic firms.

By Mara Hvistendahl

China doesn't only collect enormous amounts of data on its own citizens: it also sucks up data from around the world that might one day be useful for its national security, using both domestic and foreign companies as conduits. Samantha Hoffman of the Australian Strategy Policy Institute, one of the leading experts on the Chinese surveillance state, shed light on this phenomenon last year with a report, "Engineering Global Consent," that focuses on GTCOM, one of the state-owned firms at the heart of China's global data-gathering strategy. *This interview has been condensed and edited for clarity.*

Q: How does the Chinese Communist Party (CCP) collect data?

A: The data used by the Party comes in many forms, including text, images, video, and audio. Inside China, accessing this data is straightforward. To get access to global data, the Party uses state-owned enterprises, both Chinese and foreign tech firms, and partners such as university researchers.

The CCP doesn't only collect data through invasive surveillance technologies like cameras that employ facial recognition. It also relies on technologies that provide everyday services, like devices associated with smart cities. Long before AI or "big data" became buzzwords, the Party's intent was to co-opt—not simply coerce—society to participate in its own control.

Q: What is the CCP doing with all of this data?

A: The CCP collects data in bulk and worries about what to do with it later. Even if it's not all immediately usable, the Party anticipates better technical ability to exploit the data later on.

Large data sets can reveal patterns and trends in human behavior, which help the CCP with intelligence and propaganda as well as surveillance. Some of that data is fed into tools such as the social credit system. Bulk data, like images and voice data, can also be used to train algorithms for facial and voice recognition.

The CCP's methods are not that different from what we see in the global advertising industry. But instead of trying to sell a product, the CCP is trying to exert authoritarian control. It's using capitalism as a vehicle to access data that can help it disrupt democratic processes and create a more favorable global environment for its power.

Q: Why is this a threat outside China?

A: Citizens of liberal democracies are rightly concerned with how tech companies abuse their data, but at least in liberal democracies there are growing restraints on how data is used. In China, where the party-state literally says that the purpose of the law is to "strengthen and improve the Party's leadership," technology is deployed to extend the political power of the party-state and developed according to that standard. The Party talks about its intent to shape global public opinion in order to protect and expand its own political power. At the same time, Chinese tech companies collect data in support of such efforts. Anyone living in a liberal democracy should be concerned about the ramifications this has for freedoms and privacy.

Q: So should we all delete TikTok from our phones?

A: I will not put it on mine. TikTok is a good example of a seemingly benign app that can give the CCP a lot of useful data. You wouldn't think of a social-media app that is used by a lot of children around the world as being inherently problematic for

ROHAN THOMSON

Samantha Hoffman is an analyst at the Australian Strategic Policy Institute in Canberra.

political reasons. But the sentiment data from an app like TikTok can be used to understand how people are influenced and how they think. A lawsuit recently filed against the company in California alleges that face data collected from the app was connected to PRC [People's Republic of China]–based servers, raising significant privacy concerns.

TikTok has said that it stores user data in servers located in the US and Singapore, but this is a way of evading questions about the Party's potential political control over the company. Additionally, the app has been found censoring or suppressing Black Lives Matter and LGBTQ content, among other subjects. To me this has happened frequently enough around the world to look like a pattern rather than a mistake, and this is a wrong that I cannot overlook.

Q: Can you explain why you are concerned about GTCOM, a little-known Chinese company you've studied?

A: GTCOM is a big-data and AI company that is controlled by China's Central Propaganda Department, which is deeply involved in Party attempts to shift the global narrative around China's power. One of their products claims to collect 10 terabytes of data a day, or two to three petabytes per year, from web pages, forums, Twitter, Facebook, WeChat, and other sources. In terms of size, that's the equivalent of 20 billion Facebook photos. The company describes its work as contributing directly to China's national security, including military intelligence and propaganda.

GTCOM's research and development arm has developed algorithms that look for military keywords in the information it collects, which could for instance come from CVs or patents. The company has specifically stated that its work assists with state security. In 2017, a senior executive said that GTCOM had established an information security system that relies on image, text, and voice recognition to "prevent security risks" and "provide technical support and assistance for state security."

Q: What about GTCOM's work overseas?

A: GTCOM has strong relationships with Chinese tech companies that have a large global presence. For instance, it has a strategic agreement with Alibaba Cloud to embed its translation services in the company's technology. GTCOM's service-providing business model allows it to collect any data that GTCOM translation services generate. At face value, it might look like its services are used to improve translation quality, but in reality they are also used to build other products, including products connected to national security work.

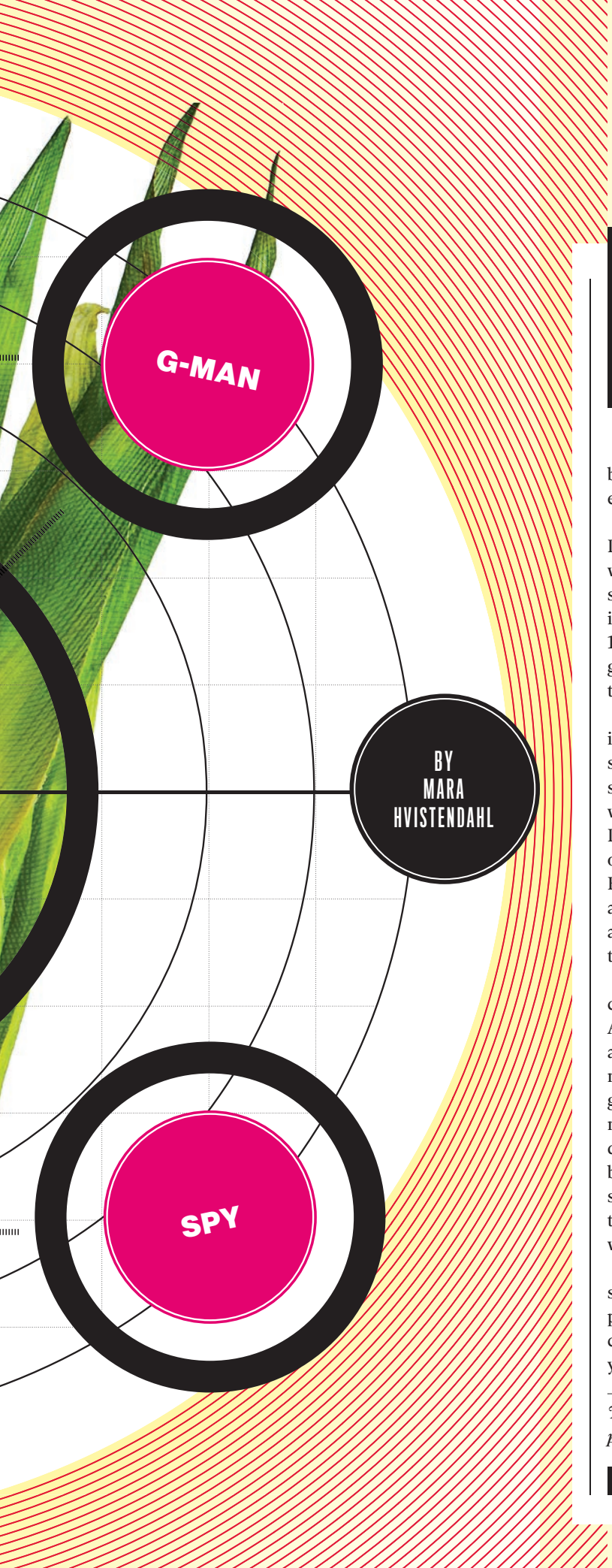
GTCOM has established partnerships with linguistics researchers worldwide. These partnerships give GTCOM access to a broad variety of data. What GTCOM is doing is not dissimilar to [American analytics company] Palantir in terms of big-data analytics. The difference is that the intent driving GTCOM's work is framed by the CCP, whose interests run counter to those of a liberal democracy.

Q: What should we do about all this?

A: Ideal solutions don't exist yet, partly because research on these issues hasn't been in-depth or forward-looking. But we can start with greater investment in data literacy and data transparency programs. Liberal democracies must improve due diligence around security in the digital supply chain, invest in research and development, and become more competitive in the smart technologies market. They cannot go at this alone; alliances must be strengthened. Finally, liberal democratic governments must bolster data privacy laws and rethink how to manage propaganda from both foreign and domestic sources in the digital age—but without compromising democratic values along the way. To do that, they must be clear about what their values are and why they differ from those of authoritarian regimes.

Mara Hvistendahl is an investigative reporter with The Intercept.


HACKER
Agricultural technology is a key US-China battleground, and the FBI is at the center of the action.
But who's really benefiting ?
SEED THIEF



In the summer of 2011, Mark Betten drove north from Des Moines through the heart of Iowa farm country. It was a blistering hot Thursday just before the Fourth of July, the sort of day when no one wants to be in a car on the interstate. His trip to Johnston, a Des Moines suburb, was not intended to be particularly momentous. But what Betten learned there would end up consuming his life for the next few years.

He soon arrived at the headquarters of the seed company DuPont Pioneer, which occupies a low-slung building plastered with gigantic images of corn. Inside, Betten met with corporate security officers. The Federal Bureau of Investigation was shifting its focus to economic espionage cases involving China. A 14-year veteran of the bureau with a close-cropped haircut and a gravelly voice, Betten was at Pioneer for what the FBI calls a routine liaison visit—a chance to exchange ideas and trawl for tips.

A dizzying array of technologies were now portrayed as critical to national security: wind turbines, paint whiteners, corn seed. The bureau worked closely with companies to identify the secrets targeted by Chinese competitors, and the relationship with DuPont, Pioneer's parent company, was particularly cozy. DuPont was already a giant corporation: it would make a profit of over $4 billion in 2011, on revenue of nearly 10 times as much. By then, the US Department of Justice (DOJ) had already brought at least four federal trade cases on behalf of DuPont subsidiaries and affiliates on trade-secret theft. In the years that followed, that focus would only intensify.

At the meeting, Betten explained the bureau's efforts to combat economic espionage and tackle cybersecurity threats. A Pioneer security officer mentioned that a few months earlier, a contract farmer in a remote part of Iowa had found a Chinese national crouched on his knees in a field where the company grew genetically modified inbred seed. Another man waited nearby in a parked car. When the farmer asked what they were doing, the kneeling man stammered out an excuse; then he bolted for the car and jumped in the passenger seat as the car sped away. Pioneer security later used the license plate to trace the rental car to a man with a Florida driver's license. His name was Hailong Mo.

Back at the FBI field office, Betten soon learned of two other suspicious incidents involving Hailong Mo and other seed companies operating in Iowa—including Monsanto, another agricultural giant, which would earn over $2 billion in profits that year. Agricultural technology is among the sectors designated for

---

This story was adapted in part from The Scientist and the Spy, *published by Riverhead Books.*

strategic development in China, and the US Office of the National Counterintelligence Executive, which advises the president on intelligence matters related to national security, had identified it as a frequent target of industrial spies. Betten ordered surveillance on Mo.

It turned out that Mo, who also goes by the first name Robert, worked for DBN, an agricultural company based in Beijing. DBN competed with Pioneer and Monsanto in the Chinese market. The Chinese government didn't yet allow companies to sell genetically modified corn of the sort that had been growing in the Iowa field, but most experts expected the policy to change, and DBN, it seemed, was trying to prepare. Over the coming years, Betten followed closely as Mo and his colleagues at DBN executed an elaborate, if occasionally comical, plot to steal seeds from Monsanto and Pioneer. They posed as farmers, shipped boxes of seed using FedEx, and even attempted to smuggle the seed back to China in Orville Redenbacher microwave popcorn bags.

To catch Mo stealing agricultural trade secrets, the FBI pulled out tools it might use against drug cartels.

But the FBI's reaction was equally outsized. Betten came to oversee a vast dragnet involving dozens of agents across the United States. To catch Mo stealing the trade secrets of the two agricultural giants, the FBI pulled out the tools that might be used against drug cartels or organized crime: car chases, airport busts, and aerial surveillance. The difference was that the target was a Chinese-born scientist with two PhDs—a new sort of criminal, and one that the US would increasingly take aim at over the years to come.

The Justice Department is waging war on Chinese industrial espionage. In 2018, the department launched the China Initiative, an effort to crack down on intellectual-property theft and other crimes. Overseen by FBI and DOJ officials, as well as a group of federal prosecutors, it takes a "whole of government" approach that involves coordinating ideas across multiple agencies. Though ostensibly about upholding the law, the China Initiative has also become one of the US's principal tools in its brewing technological standoff with China. And although it is partly the creation of Trump administration hawks, the groundwork was laid years ago, under the Obama-era Justice Department.

The FBI now has over 2,000 active investigations involving China, spanning all 56 field offices. "We're talking about everything from Fortune 100 companies to Silicon Valley startups, from government and academia to high tech and even agriculture," FBI director Christopher Wray said at a conference at a Washington, DC, think tank in February. Even the pandemic has not slowed the effort. At a virtual event hosted by another think tank in July, Wray said that the FBI opens a new counterintelligence investigation involving China every 10 *hours*. Unlike those of bureau targets like election interference or far-right domestic terrorism, China-related investigations have full support from the highest levels of the Justice Department.

In recent months, federal prosecutors have charged, in absentia, four members of China's People's Liberation Army (PLA) with hacking into the servers of the credit-rating agency Equifax and stealing data on millions of Americans. They have also unveiled charges of trade-secret theft against Huawei, the telecommunications giant whose ambitions to dominate the emerging 5G mobile telephony industry are seen by some as a threat to US national security interests. And they have charged US-based scientists at academic labs with lying about grants from Chinese institutions. (Former Harvard University chemistry chair Charles Lieber is the most prominent researcher to have been indicted.)

But critics question whether the DOJ's China push achieves its goals of deterring crime and protecting innovation in America. In some cases, the drive to go after technology threats has resulted in hasty prosecutions, with charges later dropped or downgraded. "Everything looks like a nail when you've got a hammer," says Margaret Lewis, an expert on China and Taiwan at Seton Hall Law School in Newark, New Jersey. "DOJ is sweeping together everything from PLA hackers to misreporting on grants into one big China threat."

The US focus on industrial espionage didn't begin with China. It goes back to the end of the Cold War, when the dissolution of the Soviet Union left a vacuum in the intelligence agencies. As agents left in droves, intelligence leaders sought out a new purpose. Industrial espionage was a natural fit. The increasing reach of the internet made technologies much easier to steal.

At the time, most US companies dealt with trade-secret theft through civil lawsuits, with one company suing another—and assuming the attendant legal costs. No international treaty or agreement addressed industrial espionage. In 1996, President Bill Clinton signed the Economic Espionage Act into law, making trade-secret theft a federal crime and marking attacks on American business as a national security threat. The act's

THIS PAGE AND PREVIOUS: GETTY IMAGES

stiffest penalties against individuals—fines of up to $5 million and up to 15 years in prison—are reserved for thefts that can be connected to a foreign government. At the time that meant France and Israel. Thefts by Chinese companies were not yet a significant concern.

Federal prosecutors brought only a handful of cases in those early years, and after the terrorist attacks of September 11, 2001, industrial espionage took a back seat to counterterrorism on the FBI's list of priorities. Only when investigations picked up again in the late 2000s did the focus shift to China. The country's ambitious plans to build up strategic technology industries were provoking alarm in Washington. As the two countries moved into a more adversarial relationship, the determination to focus on trade-secret theft only increased.

In 2009, the FBI created a dedicated Economic Espionage Unit. In the years that followed, the bureau spearheaded an information blitz—holding seminars for companies and universities and printing brochures with titles like "Agricultural Economic Espionage: A Growing Threat." At moments, the FBI has even staged international sting operations to defend US companies' technology. In 2012, for example, an informant lured two Chinese entrepreneurs to the United States. The entrepreneurs had targeted the trade secrets of Pittsburgh Corning, which makes glass-block insulation. In a fictionalized film that the FBI produced about the operation, *The Company Man*, a gong sounds when the Chinese villains enter the frame. Later, the hero's wife intones, "Just say no to the Chinese!"

Such clunky messaging continues today. Though FBI officials have repeatedly said their investigations are not predicated on ethnicity, they have distributed pamphlets warning that "foreign adversaries" might try to entice US-based scholars through "appeals to ethnicity or nationality." That could be counterproductive, argues Lewis. "You risk alienating people," she says, adding that ethnic Chinese scientists who have not done anything wrong might conclude, "I'm not actually welcome here, so I will go back."

China-related investigations are costly: they require translators and analysts and often stretch over years. By one estimate, over 70 agents worked on Mo's case. But it's not clear that they have a strong deterrent effect. Take the decision to charge Chinese army officers in absentia for hacking into Equifax's servers. "If China is doing a cost-benefit calculus, and the cost-benefit calculus is 'We can steal 145 million records and it means that four of our people can't travel outside China,' that's a pretty good trade-off for China," says Jack Goldsmith, who headed the Justice Department's Office of Legal Counsel in the George W. Bush administration.

Economic espionage cases are intended to protect American innovators from unfair foreign competition. But in prosecuting them, the US government has defended the interests of corporate giants whose practices are often themselves disturbingly anticompetitive. Farmers looking to buy seed could once choose from among dozens of small seed companies. That number has dwindled year by year, as DuPont Pioneer and Monsanto have bought up their competitors. Often the new owners have kept the small seed companies' names, so that many farmers do not even realize that their preferred brand has been acquired.

Indeed, at the time that Betten opened an investigation into Mo, the Justice Department's Antitrust Division was spearheading a separate inquiry into Monsanto for anticompetitive practices. Midway through the corn theft investigation, the DOJ abandoned the probe for reasons that are still unclear. It dropped several other agricultural investigations around the same time.

Since then, seed companies have grown even larger. In 2016, the German conglomerate Bayer made a bid to acquire Monsanto; it concluded the purchase in 2018. In 2017, DuPont Pioneer merged with Dow Chemical, forming a conglomerate with about $90 billion in annual revenue. It subsequently spun out the agrichemical division as Corteva. Together with Syngenta and BASF, two other agricultural giants, Bayer and Corteva now dominate seed corn sales in the US and indeed in much of the world.

All of this means "higher prices and less innovation for farmers and consumers," says Austin Frerick, an antitrust researcher at the Yale School of Management who ran for Congress in Iowa in 2018 on a platform that included opposing Bayer's acquisition of Monsanto. (He dropped out at the primary stage, citing challenges raising money.) "The price of corn seed has more than doubled in the past decade, and I promise you that seed didn't get twice as good," he says. "And as study after study in the economic literature demonstrates, innovation declines as industries get consolidated, because they lose the incentive to compete."

On December 11, 2013, agents streamed into Mo's house in Florida at the crack of dawn, arrested him, and led him out to a government car. It had taken years of work by dozens of agents in five states to build a case against him. In 2016, after two years of pretrial proceedings, Mo pleaded guilty to conspiring to steal trade secrets. Later that year, as Betten watched from a bench in a Des Moines courtroom, Mo was sentenced to three years in prison.

But the government did not manage to apprehend five other people indicted in the case—Mo's colleagues at DBN, who today remain on the FBI's Most Wanted list. DBN, meanwhile, suffered no real consequences. Its stock took a dip after Mo's arrest but later recovered. By the time the case had played out, Bayer had completed its acquisition of Monsanto. The FBI and Justice Department had worked hard to protect the company's intellectual property in the name of safeguarding American innovation. But now that company was no longer even American.

Mara Hvistendahl is an investigative reporter with The Intercept.

PEGASUS UNBOUND

THE WORLD'S MOST NOTORIOUS SPYWARE COMPANY SAYS IT WANTS TO CLEAN UP ITS ACT.

GO ON, WE'RE LISTENING.

BY Patrick Howell O'Neill / ILLUSTRATIONS BY Ariel Davis

Maâti Monjib speaks slowly, like a man who knows he's being listened to.

It's the day of his 58th birthday when we speak, but there's little celebration in his voice. "The surveillance is hellish," Monjib tells me. "It is really difficult. It controls everything I do in my life."

A history professor at the University of Mohammed V in Rabat, Morocco, Monjib vividly remembers the day in 2017 when his life changed. Charged with endangering state security by the government he has fiercely and publicly criticized, he was sitting outside a courtroom when his iPhone suddenly lit up with a series of text messages from numbers he didn't recognize. They contained links to salacious news, petitions, and even Black Friday shopping deals.

A month later, an article accusing him of treason appeared on a popular national news site with close ties to Morocco's royal rulers. Monjib was used to attacks, but now it seemed his harassers knew everything about him: another article included information about a pro-democracy event he was set to attend but had told almost no one about. One story even proclaimed that the professor "has no secrets from us."

He'd been hacked. The messages had all led to websites that researchers say were set up as lures to infect visitors' devices with Pegasus, the most notorious spyware in the world.

Pegasus is the blockbuster product of NSO Group, a secretive billion-dollar Israeli surveillance company. It is sold to law enforcement and intelligence agencies around the world, which use the company's tools to choose a human target, infect the person's phone with the spyware, and then take over the device. Once Pegasus is on your phone, it is no longer your phone.

NSO sells Pegasus with the same pitch arms dealers use to sell conventional weapons, positioning it as a crucial aid in the hunt for terrorists and criminals. In an age of ubiquitous technology and strong encryption, such "lawful hacking" has emerged as a powerful tool for public safety when law enforcement needs access to data. NSO insists that the vast majority of its customers are European democracies, although since it doesn't release client lists and the countries themselves remain silent, that has never been verified.

Monjib's case, however, is one of a long list of incidents in which Pegasus has been used as a tool of oppression. It has been linked to cases including the murder of Saudi journalist Jamal Khashoggi, the targeting of scientists and campaigners pushing for political reform in Mexico, and Spanish government surveillance of Catalan separatist politicians. Mexico and Spain have denied using Pegasus to spy on opponents, but accusations that they have done so are backed by substantial technical evidence.

Some of that evidence is contained in a lawsuit filed last October in California by WhatsApp and its parent company, Facebook, alleging that Pegasus manipulated WhatsApp's infrastructure to infect more than 1,400 cell phones. Investigators at Facebook found more than 100 human rights defenders, journalists, and public figures among the targets, according to court documents. Each call that was picked up, they discovered, sent malicious code through WhatsApp's infrastructure and caused the recipient's phone to download spyware from servers owned by NSO. This, WhatsApp argued, was a violation of American law.

NSO has long faced such accusations with silence. Claiming that much of its business is an Israeli state secret, it has offered precious little public detail about its operations, customers, or safeguards.

Now, though, the company suggests things are changing. In 2019, NSO, which was owned by a private equity firm, was sold back to its founders and another private equity firm, Novalpina, for $1 billion. The new owners decided on a fresh strategy: emerge from the shadows. The company hired elite public relations firms, crafted new human rights policies, and developed new self-governance documents. It even began showing off some of its other products, such as a covid-19 tracking system called Fleming, and Eclipse, which can hack drones deemed a security threat.

Over several months, I've spoken with NSO leadership to understand how the company works and what it says it is doing to prevent human rights abuses carried out using its tools. I have spoken to its critics, who see it as a danger to democratic values; to those who urge more regulation of the hacking business; and to the Israeli regulators responsible for governing it today. The company's leaders talked about NSO's future and its policies and procedures for dealing with problems, and it shared documents that detail its relationship with the agencies to which it sells Pegasus and other tools. What I found was a thriving arms dealer—inside the company, employees acknowledge that Pegasus is a genuine weapon—struggling with new levels of scrutiny that threaten the foundations of its entire industry.

NSO's basic argument is that it is the creator of a technology that governments use, but that since it doesn't attack anyone itself, it can't be held responsible.

"A DIFFICULT TASK"

From the first day Shmuel Sunray joined NSO as its general counsel, he faced one international incident after another. Hired just days after WhatsApp's lawsuit was filed, he found other legal problems waiting on his desk as soon as he arrived. They all centered on the same basic accusation: NSO Group's hacking tools are sold to, and can be abused by, rich and repressive regimes with little or no accountability.

Moroccan academic and free-speech campaigner Maâti Monjib has been watched by his government for years. "The surveillance is hellish," he says.

FADEL SENNA / GETTY

Sunray had plenty of experience with secrecy and controversy: his previous job was as vice president of a major weapons manufacturer. Over several conversations, he was friendly as he told me that he's been instructed by the owners to change NSO's culture and operations, making it more transparent and trying to prevent human rights abuses from happening. But he was also obviously frustrated by the secrecy that he felt prevented him from responding to critics.

"It's a difficult task," Sunray told me over the phone from the company's headquarters in Herzliya, north of Tel Aviv. "We understand the power of the tool; we understand the impact of misuse of the tool. We're trying to do the right thing. We have real challenges dealing with government, intelligence agencies, confidentiality, operational necessities, operational limitations. It's not a classic case of human rights abuse by a company, because we don't operate the systems—we're not involved in actual operations of the systems—but we understand there is a real risk of misuse from the customers. We're trying to find the right balance."

This underpins NSO's basic argument, one that is common among weapons manufacturers: the company is the creator of a technology that governments use, but it doesn't attack anyone itself, so it can't be held responsible.

Still, according to Sunray, there are several layers of protection in place to try to make sure the wrong people don't have access.

MAKING A SALE

Like most other countries, Israel has export controls that require weapons manufacturers to be licensed and subject to government oversight. In addition, NSO does its own due diligence, says Sunray: its staff examine a country, look at its human rights record, and scrutinize its relationship with Israel. They assess the specific agency's track record on corruption, safety, finance, and abuse—as well as factoring in how much it needs the tool.

Sometimes negatives are weighed against positives. Morocco, for example, has a worsening human rights record but a lengthy history of cooperating with Israel and the West on security, as well as a genuine terrorism problem, so a sale was reportedly approved. By contrast, NSO has said that China, Russia, Iran, Cuba, North Korea, Qatar, and Turkey are among 21 nations that will never be customers.

Finally, before a sale is made, NSO's governance, risk, and compliance committee has to sign off. The company says the committee, made up of managers and shareholders, can decline sales or add conditions, such as technological restrictions, that are decided case by case.

PREVENTING ABUSE

Once a sale is agreed to, the company says, technological guardrails prevent certain kinds of abuse. For example, Pegasus does not allow American phone numbers to be infected, NSO says, and infected phones cannot even be physically located in the United States: if one does find itself within American borders, the Pegasus software is supposed to self-destruct.

NSO says Israeli phone numbers are among others also protected, though who else gets protection and why remains unclear.

When a report of abuse comes in, an ad hoc team of up to 10 NSO employees is assembled to investigate. They interview the customer about the allegations, and they request Pegasus data logs. These logs don't contain the content the spyware extracted, like chats or emails—NSO insists it never sees specific intelligence—but do include metadata such as a list of all the phones the spyware tried to infect and their locations at the time.

According to one recent contract I obtained, customers must "use the system only for the detection, prevention, and investigation of crimes and terrorism and ensure the system will not be used for human rights violations." They must notify the company of potential misuse. NSO says it has terminated three contracts in the past for infractions including abuse of Pegasus, but it refuses to say which countries or agencies were involved or who the victims were.

"WE'RE NOT NAÏVE"

Lack of transparency is not the only problem: the safeguards have limits. While the Israeli government can revoke NSO's license for violations of export law, the regulators do not take it on themselves to look for abuse by potential customers and aren't involved in the company's abuse investigations.

Many of the other procedures are merely reactive as well. NSO has no permanent internal abuse team, unlike almost any other billion-dollar tech firm, and most of its investigations are spun up only when an outside source such as Amnesty International or

Citizen Lab claims there has been malfeasance. NSO staff interview the agencies and customers under scrutiny but do not talk to the alleged victims, and while the company often disputes the technical reports offered as evidence, it also claims that both state secrecy and business confidentiality prevent it from sharing more information.

The Pegasus logs that are crucial to any abuse inquiry also raise plenty of questions. NSO Group's customers are hackers who work for spy agencies; how hard would it be for them to tamper with the logs? In a statement, the company insisted this isn't possible but declined to offer details.

If the logs aren't disputed, NSO and its customers will decide together whether targets are legitimate, whether genuine crimes have been committed, and whether surveillance was done under due process of law or whether autocratic regimes spied on opponents.

Sunray, audibly exasperated, says he feels as if secrecy is forcing him to operate with his hands tied behind his back.

"It's frustrating," he told me. "We're not naïve. There have been misuses. There will be misuses. We sell to many governments. Even the US government—no government is perfect. Misuse can happen, and it should be addressed."

But Sunray also returns to the company's standard response, the argument that underpins its defense in the WhatsApp lawsuit: NSO is a manufacturer, but it's not the operator of the spyware. *We* built it but *they* did the hacking—and they are sovereign nations.

That's not enough for many critics. "No company that believes it can be the independent watchdog of their own products ever convinces me," says Marietje Schaake, a Dutch politician and former member of the European Parliament. "The whole idea that they have their own mechanisms while they have no problem selling commercial spyware to whoever wants to buy it, knowing that it's used against human rights defenders and journalists—I think it shows the lack of responsibility on the part of this company more than anything."

So why the internal push for more transparency now? Because the deluge of technical reports from human rights groups, the WhatsApp lawsuit, and increasing governmental scrutiny threaten NSO's status quo. And if there is going to be a new debate over how the industry gets regulated, it pays to have a powerful voice.

GROWING SCRUTINY

Lawful hacking and cyberespionage have grown enormously as a business over the past decade, with no signs of retreat. NSO Group's previous owners bought the company in 2014 for $130 million, less than one-seventh of the valuation it was sold for last year. The rest of the industry is expanding too, profiting from the spread of communications technology and deepening global instability. "There's no doubt that any state has the right to buy this technology to fight crime and terrorism," says Amnesty International's deputy director, Danna Ingleton. "States are rightfully and lawfully able to use these tools. But that needs to be accompanied more with a regulatory system that prevents abuses and provides an accountability mechanism when abuse has happened." Shining a much brighter light on the hacking industry, she argues, will allow for better regulation and more accountability.

Earlier this year Amnesty International was in court in Israel arguing that the Ministry of Defense should revoke NSO's license because of abuses of Pegasus. But just as the case was starting, officials from Amnesty and 29 other petitioners were told to leave the courtroom: a gag order was being placed on the proceedings at the ministry's urging. Then, in July, a judge rejected the case outright.

"I do not believe as a matter of principle and as a matter of law that NSO can claim a complete lack of responsibility for the way their tools are being used," says United Nations special rapporteur Agnès Callamard. "That's not how it works under international law."

If NSO loses the WhatsApp case, one lawyer says, it calls into question all those companies that make their living by finding flaws in software and exploiting them.

Callamard advises the UN on extrajudicial executions and has been vocal about NSO Group and the spyware industry ever since it emerged that Pegasus was being used to spy on friends and associates of Khashoggi shortly before he was murdered. For her, the issue has life-or-death consequences.

"We're not calling for something radically new," says Callamard. "We are saying that what's in place at the moment is proving insufficient, and therefore governments or regulatory agencies need to move into a different gear quickly. The industry is expanding, and it should expand on the basis of the proper framework to regulate misuse. It's important for global peace."

There have been calls for a temporary moratorium on sales until stronger regulation is enacted, but it's not clear what that legal framework would look like. Unlike conventional arms, which are subject to various international laws, cyber weapons are currently not regulated by any worldwide arms control agreement. And while nonproliferation treaties have been suggested, there is little clarity on how they would measure existing capabilities, how monitoring or enforcement would work, or how the rules would keep up with rapid technological developments. Instead, most scrutiny today is happening at the national legal level.

In the US, both the FBI and Congress are looking into possible hacks of American targets, while an investigation led by Senator Ron Wyden's office wants to find out whether any Americans

are involved in exporting surveillance technology to authoritarian governments. A recent draft US intelligence bill would require a government report on commercial spyware and surveillance technology.

The WhatsApp lawsuit, meanwhile, has taken aim close to the heart of NSO's business. The Silicon Valley giant argues that by targeting California residents—that is, WhatsApp and Facebook—NSO has given the court in San Francisco jurisdiction, and that the judge in the case can bar the Israeli company from future attempts to misuse WhatsApp's and Facebook's networks. That opens the door to an awful lot of possibilities: Apple, whose iPhone has been a paramount NSO target, could feasibly mount a similar legal attack. Google, too, has spotted NSO targeting Android devices.

And financial damages are not the only sword hanging over NSO's head. Such lawsuits also bring with them the threat of courtroom discovery, which has the potential to bring details of NSO's business deals and customers into the public eye.

"A lot depends on exactly how the court rules and how broadly it characterizes the violation NSO is alleged to have committed here," says Alan Rozenshtein, a former Justice Department lawyer now at the University of Minnesota Law School. "At a minimum, if NSO loses this case, it calls into question all of those companies that make their products or make their living by finding flaws in messaging software and providing services exploiting those flaws. This will create enough legal uncertainty that I would imagine these would-be clients would think twice before contracting with them. You don't know if the company will continue to operate, if they'll get dragged to court, if your secrets will be exposed." NSO declined to comment on the alleged WhatsApp hack, since it is still an active case.

"WE ARE ALWAYS SPIED ON"

In Morocco, Maâti Monjib was subjected to at least four more hacking attacks throughout 2019, each more advanced than the one before. At some point, his phone browser was invisibly redirected to a suspicious domain that researchers suspect was used to silently install malware. Instead of something like a text message that can raise the alarm and leaves a visible trace, this one was a much quieter network injection attack, a tactic valued because it's almost imperceptible except to expert investigators.

On September 13, 2019, Monjib had lunch at home with his friend Omar Radi, a Moroccan journalist who is one of the regime's sharpest critics. That very day, an investigation later found, Radi was hit with the same kind of network injection attacks that had snared Monjib. The hacking campaign against Radi lasted at least into January 2020, Amnesty International researchers said. He's been subject to regular police harassment ever since.

At least seven more Moroccans received warnings from WhatsApp about Pegasus being used to spy on their phones, including human rights activists, journalists, and politicians. Are these the kinds of legitimate spying targets—the terrorists and criminals—laid out in the contract that Morocco and all NSO customers sign?

In December, Monjib and the other victims sent a letter to Morocco's data protection authority asking for an investigation and action. Nothing formally came of it, but one of the men, the pro-democracy economist Fouad Abdelmoumni, says his friends high up at the agency told him the letter was hopeless and urged him to drop the matter. The Moroccan government, meanwhile, has responded by threatening to expel Amnesty International from the country.

What's happening in Morocco is emblematic of what's happening around the world. While it's clear that democracies are major beneficiaries of lawful hacking, a long and growing list of credible, detailed, technical, and public investigations shows Pegasus being misused by authoritarian regimes with long records of human rights abuse.

"Morocco is a country under an authoritarian regime who believe people like Monjib and myself have to be destroyed," says Abdelmoumni. "To destroy us, having access to all information is key. We always consider that we are spied on. All of our information is in the hands of the palace."

Patrick Howell O'Neill covers cybersecurity for MIT Technology Review.

The Rosenau Brothers clothing factory in Lansford, Pennsylvania, once employed 500 people. It closed for good in the 1990s.

IN AMERICA

DECADES OF DECLINE LEFT THE US'S INDUSTRIAL COMMONS INCAPACITATED IN THE FACE OF THE PANDEMIC.

BY
ROWAN MOORE GERETY

Photographs by
Matthew Christopher

In early March, as the coronavirus pandemic forced America to contemplate a nationwide shutdown, Dan St. Louis started to get nervous. St. Louis runs a facility in Conover, North Carolina, called the Manufacturing Solutions Center, which prototypes and tests new fabrics and other materials; most of its funding comes from contracts with what remains of the American textile industry. With stay-at-home orders on the horizon, "our business just dried up immediately," he says.

A week later, St. Louis's cell phone began to ring incessantly: hospitals, nursing homes, and funeral homes from as far away as New York. Everyone wanted to know if he could find them masks and gowns, or tell them who could, or at least help them figure out whether the personal protective equipment (PPE) they *could* get was any good. "And that was just half my calls," he says. The others were from makers of furniture, pants, and shirts, and dozens of other businesses with industrial facilities they wanted to put to use to help shore up the supply of whatever was needed. St. Louis breaks into rapid-fire gibberish trying to mimic the callers' urgency, and then, chuckling, can't seem to find the right words.

"I'm telling you… It was… You couldn't."

St. Louis has worked at the Manufacturing Solutions Center since it was founded, in 1990, as a division of Catawba Valley Community College. He keeps a list eight pages long of every kind of test the facility has ever run to evaluate specialty fabrics: filters used in motorcycle cooling systems and clothing that dispenses pain medication, hard casts for bone fractures and nontoxic treatment for raw silk, hybrid sock-tights featured on *Oprah*. But they'd never worked on PPE before March: "There wasn't anybody calling us saying, 'Hey, will you test this stuff?'" That's because most PPE was made overseas.

St. Louis's sudden education began just as governments across the world started treating the looming shortage of masks and face shields as a matter of national security. Germany banned PPE exports on March 4. Malaysia, India, and dozens of others soon took similar measures. Diplomacy eased some of this early jockeying over the existing supply—Taiwan pledged to donate 10 million masks overseas, President Donald Trump grudgingly allowed 3M to sell N95s to Canada, the EU convinced Germany to share its PPE with the rest of the bloc and then prohibited exports outside it—but by the end of April, the World Trade Organization was reporting that more than 80 countries around the world had taken steps to limit exports of PPE during the pandemic.

It was a scenario St. Louis had often thought about before: the US, abruptly forced to go it alone, discovering how little the country makes of the stuff it consumes. Usually, he imagined a war with China: "You can't call and say 'Our guys are cold—we need stuff.'" But the pandemic made clear that the pinch could come in a variety of forms.

In 1990, he recalled, the US textile industry produced 60% of the "cut & sew" apparel made worldwide—that is, clothing with stitches on the seams, as opposed to knitted wool sweaters or rain gear whose pieces are welded together with heat. Today that figure is 3%. When federal and state agencies began to publish numbers about how much PPE they'd need to outlast the accelerating outbreak, St. Louis was flabbergasted. "We need a billion gowns! Good God," he says. "We need a billion? A *billion*? I can't even fathom that."

The sudden need for a range of lifesaving fabrics threw the handful of facilities like St. Louis's into overdrive. In the middle of March, they began ferrying samples, performance specs, and recommended adjustments back and forth to fabric mills trying to convert their operations overnight to making essential goods. At the end of three months, St. Louis says, the Manufacturing Solutions Center had helped 28 companies begin churning out fabric suitable for hospital gowns.

Masks and respirators are a different question. Existing worldwide supplies of the melt-blown polypropylene used in the most coveted PPE item in hospitals—the N95 respirators capable of filtering out the virus—are spoken for through at least the first few months of 2021. In March, a senior official at the US Department of Health and Human Services estimated that American health-care workers alone would go through 3.5 billion N95 masks fighting the coronavirus.

Surgical masks are not as protective as N95s, but they do shield the wearer from droplets and fluids better than the now ubiquitous cloth masks—3% to 25% better, depending on the study. To sustain any meaningful reopening of the economy, surgical masks will likely have to be made by the tens or even hundreds of billions. Outfits like the Manufacturing Solutions Center are also uniquely qualified to develop a new generation of higher-performance cloth masks, or ones that use small filter inserts to stretch scarce materials further. One model created at the facility is a knit mask woven through with copper, which is being used in medical facilities and by the US military. Thanks to its tight fit, it "doesn't fog my glasses," as one of St. Louis's colleagues says, but they have no way to evaluate it more definitively than that.

In July, St. Louis was still scrambling to raise $500,000 to buy machinery that would allow him to test the fabric used in masks. Meanwhile, he refers inquiries about mask testing to a company in Nevada—the lone private laboratory in the US certified by the CDC to perform such tests.

Meanwhile, 40 miles south of Conover, in the town of Belmont, the Textile Technology Center at Gaston College specializes in what the industry refers to as "yarn." Give Dan Rhodes a small sample of a novel polymer, and he'll figure out how to extrude it into a

---

The photographs accompanying this article are part of *Abandoned America*, a multi-decade project documenting derelict sites throughout the country.

The Wilde Yarn Mill in Manayunk, Pennsylvania, closed in 2012. When it opened in the 1880s there were over 800 textile operations in the area. It had been the oldest continually operating yarn mill in the country.

filament, and how to fine-tune the process to see whether the material can be made to work in high-speed manufacturing. Rhodes and his colleagues are working with a manufacturer of coronavirus test kits to make the fiber wicks that siphon saliva samples into a blend of testing reagents. Another client is an Ohio-based manufacturer of cotton swabs that is replacing the cotton with a synthetic equivalent in order to make nasal testing swabs uncontaminated by the plant fiber's DNA.

Vital work. And yet in each case, few American businesses could step up to fill a similar niche. Rhodes told me that most surviving textile companies have long since disbanded the proprietary sampling labs they used to house on site. Many of the senior staff at both centers learned their trade at companies that were picked apart and reconstituted overseas after hostile takeovers by investors like Wilbur Ross, the current secretary of commerce, who made part of his fortune outsourcing textile jobs to Asia in the early 2000s.

That means much of the brain trust for the American textile industry—the Manufacturing Solutions Center's website advertises "300 years of textile experience"—got its training in private-sector jobs that no longer exist in the United States. Rhodes, who is 72, plans to retire at the end of August and jokes that "half the people here collect a Social Security check." St. Louis retired in July; every plant where he ever worked closed long ago.

Rhodes recalls watching from afar as the town of Fort Payne, Alabama, lost its status as "sock capital of the world." "All it takes is one *financier*"—he stretches the word across four venomous syllables—"on Wall Street to call somebody in China and say, 'Send me a million dozen of those black socks with the gold thread in the toe.' He doesn't know how to make any socks, but he can destroy all that expertise."

Why did the sock makers leave Fort Payne? To Jon Clark, who spent 30 years crisscrossing the country from his home in Houston to buy scrap equipment from shuttered factories, the answer is obvious: there's money to be made shifting operations from what he calls "the 30-, 40-, 50-dollar-an-hour zone in the US" to the "three-, four-, five-dollar zone" overseas. The problem, in Clark's view, is that the incentives driving the economy no longer distinguish between profitability and greed. "It used to be that plants closed because they weren't profitable," he says. "Now they close because they're not profitable enough."

Clark, who is 72, began his career in 1965 as an engineer in a Texas fertilizer plant where chemically induced asthma was a daily hazard. He remembers watching birds expire in midair as they flew from one side of the plant to the other. Environmental laws transformed huge

swaths of American manufacturing, but they also gave US corporations a strong incentive to relocate factories to places where they could pollute at will.

Over the same period, seismic improvements in shipping and technology made it possible for corporations to rely on networks of suppliers that stretch across the planet. Modern supply chains are fluid and elaborate, ever shifting to account for minute changes in the price of screws, thread, or copper wire. As a result, manufacturers have continued to bring cheaper goods to American consumers even as the components required to make them come from farther and farther away.

Clark began buying and selling equipment full time in the 1980s, just as these transformations were accelerating the exodus of heavy manufacturing from the US to cheaper labor markets all over the world—China, Mexico, Vietnam. In 2003, he began publishing a biweekly newsletter called Plant Closing News (PCN) as a service for the scrap industry, a way to help auctioneers and equipment brokers chase leads on bargain wire stranders and double-arm mixers across the country. Over the years, his encyclopedic knowledge of the decline—or, more charitably, the evolution—of American industry has crystallized into a kind of lament about the shifting character of the US economy.

"CAN YOU IMAGINE A PLANT THAT DOES NOTHING BUT BREAK A MILLION EGGS A MONTH? THAT'S 500 TONS OF BROKEN SHELLS A YEAR!"

Each PCN listing includes the type of facility and its expected closing date, an address, a phone number, and the name of a contact person for anyone looking to move, buy, or scrap the equipment inside, along with a sentence or two on the number of displaced workers and the reasons behind a plant's shuttering. Compiling the entries is simple, if grueling, work that usually involves extracting the necessary particulars over the phone from employees likely to be losing their jobs. By the time Clark sent out the last issue in December 2019, after a detached retina left him temporarily blind in one eye, he had chronicled the demise of 16,000 factories, plants, and mills in 17 years.

When Clark and I first spoke, he began reading his newsletter aloud to me over the phone in a rich Texas baritone, interspersed with his own idiosyncratic commentary. "Can you imagine a plant that does nothing but break a million eggs a month?" he asked. "That's 500 tons of broken shells a year!"

Clark rattled off all the factory closures he'd compiled for a stretch of July 2019: an aircraft-lock assembly plant, a scrap-metal shredding facility, a conveyor manufacturer, three plastic-bottle plants, a foundry, a glass plant, a South Carolina plant that manufactured textile machinery, a pharmaceutical plant in Wyoming ("The only one," he interjected), a Florida plant that bent tubes into automotive parts, a paint-manufacturing plant in Missouri, a corrugated-cardboard-box plant in New York, and on and on and on. "Those are the ones that I know of," Clark added, when he finally reached the end of the list.

The decision to close a plant often heralds a chaotic time on the ground, as a dwindling team on site shoulders the responsibility of continuing to run a facility slated for closure. There's still inventory to track, maintenance to be done, and product to be pushed out, along with all the paperwork that goes into settling the books before closing a place down. Often, the workers themselves are the last ones to be told.

For the first five years of PCN, Clark's daughter Kristen, then at home with her oldest child, was his main "caller." She took the leads he gleaned from trade publications and industry chatter, contacted the plants, and coaxed the remaining staff into providing the information needed for Rolodex-like entries designed to help contractors gin up business in demolition, secondhand equipment, and environmental remediation. "We got hung up on a lot," Kristen remembers. But there were also moments of pathos. "We got an opportunity to cry with them, and pray with them, and a lot of them got very angry," Jon says.

PCN's run overlapped with a historic decline in manufacturing employment in the United States. From 2000 to 2016, the US shed nearly 5 million manufacturing jobs, or more than a quarter of the total, and one out of every five manufacturing establishments in the country shut its doors. Clark charted this decline in his newsletter, watching as globalization tugged at one thread after another in the tapestry of American industry. In the early 2000s, a wave of sock manufacturers closed, followed by food-processing plants, plastics plants, automotive plants, and lightbulb factories.

In 2013, Walmart rolled out a "Made in the USA" campaign, vowing to shore up domestic manufacturing by spending $50 billion over 10 years on US-made goods. But the company was forced to scale back its ambitions after the watchdog group Truth in Advertising found hundreds of products at Walmart stores falsely labeled as made in the USA. As Clark put it, "We still have 330 million people in this country, most of whom wear socks, but Walmart couldn't find anybody who made socks in America."

Five years ago, Donald Trump campaigned on the argument that manufacturers who offshored American jobs were forsaking patriotism for profit. Fused with racist grievance and conspiracy theory, that message helped propel him to the Republican

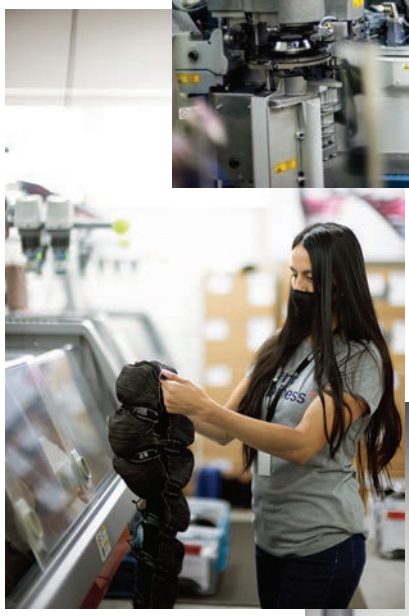
COURTESY PHOTO

nomination and then the presidency. In the 2016 election, Trump's attacks on corporations that "moved [our] jobs to Mexico" were a core element of his pitch to the very same voters—white, male Midwesterners with a high school education—who formed a prominent cohort in America's shrinking manufacturing workforce.

At the time, the prevailing wisdom among economists held that Trump was wrong. Certainly, previous declines in American manufacturing, such as the waves of textile and steel layoffs in the 1980s, could be linked more or less directly to gains in developing countries. Hundreds of new garment factories opened in China, Bangladesh, and Indonesia. Brazil and South Korea aggressively expanded steel production. But while the decline in the 2000s appeared to have a similar explanation—now China's and South Korea's economies were expanding by leaps and bounds, and American stores were filling with Korean TVs and Chinese toys and electronics—many economists and commentators looked at the data on manufacturing's share of GDP and concluded that imports couldn't be the major culprit behind so many lost jobs.

A typical example: Michael Hicks, an economist at Ball State University, coauthored a widely cited report arguing that "import substitution"—Americans' choices to buy cheaper foreign-made products instead of more expensive goods made domestically—accounted for only about 750,000 lost jobs, or roughly one-seventh of the total. What took away the rest? Layoffs of redundant workers once protected by unions; robots and automation; and reliance on more efficient maintenance and service contractors in place of part of the former labor force, he argued. After all, even as the number of manufacturing jobs shrank dramatically, the dollar value of US manufactured goods continued to grow. "I call it productivity," Hicks told me.

For years, Susan Houseman, a labor economist at the Upjohn Institute for Employment in Kalamazoo, Michigan, watched a parade of pundits explain away those 4 million lost jobs in similar terms.



This page
North Carolina's Manufacturing Solutions Center prototypes and tests new fabrics and other materials, working with renewed urgency because of the pandemic.

Opposite
Jon Clark, publisher of Plant Closing News, and his wife, Donna.

CHRIS EDWARDS

Bancroft Mills, a fabric mill in Wilmington, Delaware, had been vacant since the early 2000s and was largely destroyed by a fire in the autumn of 2016.

Houseman didn't buy it. Beginning in 2007, she published a series of papers arguing that the basic tools the federal government uses to generate manufacturing, import, and export statistics were misleading and frequently misinterpreted.

If a television manufacturer that sells $1,000 TVs relocates production overseas, and Americans start buying $500 imported TVs instead, the amount of economic activity "displaced" by offshoring shows up as $500, not $1,000. But the American town that hosted the old factory lost $1,000 worth of work. Even if the TV is still made in the US, but complex components start being sourced abroad, productivity statistics don't account for labor done by foreign suppliers. If a TV assembled in Ohio takes nine hours of Vietnamese labor and one hour of Toledo labor, as opposed to all 10 hours coming from Toledo, federal statistics will show that American manufacturers are suddenly able to produce 10 times as many TVs with the same amount of labor. "Productivity" jumps. It appears as though technology improved, when what really happened is that jobs were shipped abroad.

Furthermore, Houseman adds, for several decades, the speed and power of the chips and semiconductors churned out by one small slice of American manufacturers advanced so rapidly that increases in "output" from that sector alone accounted for the vast majority of productivity gains among US manufacturers. Leave computers out of it, and all of a sudden US manufacturing appeared to be in very bad shape.

"Research that has looked at the automation story, the robot story—there's really no evidence that that could have precipitated such a large decline in manufacturing employment," Houseman says. "Trump resonated to some people because what he was saying seemed true to them, and to a very large degree, he was right."

After the pandemic hit, one ingredient in China's remarkable recovery was its ability to turn the rudder of its enormous industrial engine to the needs of the moment. By one estimate, Chinese production of N95s and other surgical masks grew 30-fold in less than three months, reaching nearly half a billion a day. By contrast, 3M, the largest domestic US manufacturer of N95s, has received enough government funding to nearly triple its output and currently produces just over 1.5 million a day.

Willy Shih, a professor of management practice at Harvard Business School, says part of this chasm stems from the loss of the "industrial commons"—the combination of expertise, infrastructure, and networks of mutually dependent businesses that help foster efficiency and innovation. Over time, Shih argues, outsourcing has cannibalized not only the assembly line jobs we associate with the factory floor,

but the whole chain of intellectual effort that makes those jobs possible.

This arrangement has given American corporations unparalleled freedom to swap contractors, minimize tax burdens, and make things using inventory someone else pays to insure and maintain. But all that flexibility, meant to guard against financial risks to shareholders, turns out to be flexibility of the wrong kind for 2020. Any manufacturer that built in wiggle room to better weather a pandemic would have had "Wall Street analysts all over their case," Shih says, saying: "Look at how inefficiently you're using your capital."

Clark, the founder of Plant Closing News, blames this pathological pursuit of efficiency in large part on Jack Welch, the iconic late CEO of General Electric. When I visited Clark in Houston in February, he summarized Welch's gospel as follows: If you have 10 employees, no matter how well they're doing as a group, rank them 1 to 10, and get rid of number 10. (The company abandoned this "rank and yank" policy a few years after Welch stepped down in 2001.) "And if you have 60 manufacturing plants, and the smallest one is in North Carolina, and they're pretty good but they're always near the bottom of that list … when I call, the plant manager starts crying: 'I been here for 40 years. This is my family.' Why? Because you have 59 other plants that can make this stuff and 'we don't need you'?" Clark winced.

He turned his attention to the stack of copies of PCN on the table and scanned through an issue from June 2019. A vehicle seating manufacturer was laying off 28 employees near Kalamazoo and shifting production to Mexico and Kentucky; a plastic-molding plant in Illinois was shutting down and consolidating its operations in Mexico and China; a medical-device manufacturer in Southern California was moving its plant to Malaysia. "This is not uncommon—this is every one of these," Clark said. "If you're making money and your people are doing a decent job, why would you move it somewhere cheaper so you can hire foreigners and put your own people on welfare? That's never made any sense to me."

One hallmark of our era in capitalism is the rise of companies that are both everywhere and nowhere at once. Today, multinational corporations—registered in Delaware, paying taxes in Ireland, sourcing materials on five continents—drive the majority of worldwide trade. "Why wouldn't you have the business community up in arms about [offshoring] undermining their competitiveness in the United States?" Susan Houseman asked me. "Because it may not be undermining their competitiveness."

But it may be undermining the US national interest. Because the American manufacturing sector is more consolidated and narrower in scope than it once was, it's also less diverse, less resilient, and less able to respond to a crisis.

According to Behnam Pourdeyhimi, the director of the Nonwovens Institute at North Carolina State University, the current wait for a machine that can produce the melt-blown polypropylene used in N95 respirators is about 14 months. The technology for the machines was developed in the United States, but these days, Pourdeyhimi says, aside from a small manufacturer in Florida and a sprinkling of others in Europe and China, German companies enjoy a near monopoly, simply because their machines are so good. The machines used to "convert" melt-blown into wearable PPE are somewhat easier to come by, he says, but 90% of them—both for N95s and for pleated surgical masks—are made in China.

However, recovering the ability to make machines that make PPE is not impossible, Pourdeyhimi says. He estimates the necessary investment to be in the tens of millions of dollars. It should be doable in months.

During World War II, President Franklin D. Roosevelt's War Production Board famously redirected huge swaths of the American economy to make things the military needed. Factories contributing to the war effort jumped to the front of the line for scarce raw materials. "The entire capacity of the laundry industry will be devoted to war," the board's chairman announced in 1942: brass and steel would be conserved by putting an end to washing-machine production. Nylon was reserved for parachutes. Typewriter factories were converted to produce rifle barrels, while those that couldn't went on making typewriters exclusively for the government. Technology was put to work where it was most needed.

All through the spring of 2020, there were stories of vegetables being plowed under and manure ponds filled with fresh milk because the US lacked the proper packaging and processing infrastructure to convert cafeteria and wholesale food into products that could be sold in grocery stores—or even, perhaps, given away.

Even if individual firms are flexible today in ways they weren't in the past—a consequence of the transformations Shih describes—the system as a whole cannot effectively pivot as it did during the last crisis of this scale. Though Trump did not create the decades-long decline in American manufacturing, that the president is—to say the least—no FDR is a not insignificant factor in America's anemic response. Whatever credit Trump deserves for articulating the role of trade in weakening American manufacturing, he has managed to squander a generational opportunity to throw the weight of the federal government behind securing its vitality.

In recent months, the Trump administration has waved away the need for legislation aimed at "re-shoring," arguing that a presidential charm offensive will be enough to awaken CEOs' sense of patriotism. Clark doesn't see it that way. "It's all about where these companies make the most money," he says. "'If you want us to manufacture in the US, you're gonna pay for it.'"

This year is the second time Clark has decided to retire. The first time, he lasted six months. He still bids on equipment every month or two. Why? "For my own entertainment. Because I'm crazy …" He pauses. "Because a peanut plant closed in Georgia and they have two 30,000-gallon propane tanks and I've got a buyer that wants them. So why not?"

Rowan Moore Gerety, the author of Go Tell the Crocodiles, is a writer based in Phoenix, Arizona.

5

for the bookshelf

How do governments shape technology, and how does technology shape governance? These interactions are far more complicated than free-market advocates realize. The libertarian consensus that government holds back innovation, which has circulated in Silicon Valley for decades, is particularly damaging. The books excerpted here investigate how government decisions affect science and technology in ways not widely appreciated.

—Konstantin Kakaes

STEFAN ELBE

2018

Pandemics, Pills, and Politics

Governing Global Health Security

"When it comes to pandemic influenza, then, governments are actually left confronting a quite unsavory and thorny political scenario. In the event of a new flu pandemic, they would initially have to let the virus run its course for many months while they wait for a virus-specific vaccine to gradually become available—provided, that is, they even have production capacity or are at least able to secure orders from elsewhere. This long period of delay could have devastating social, economic, political, and public health ramifications. During this period, governments would also run the political risk of being seen as weak, even negligent, in their core duty to protect the welfare of their populations …

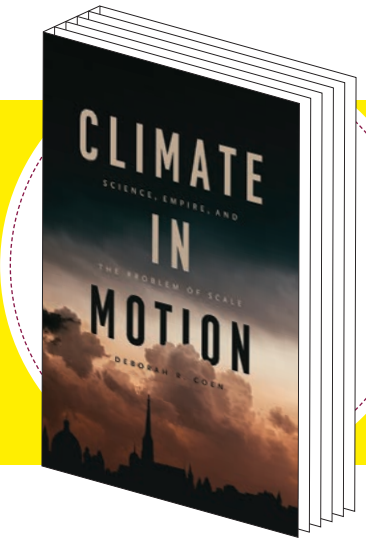
Precisely that political realization ushered in Tamiflu's second life as a prominent medical countermeasure against pandemic flu. Moving forward, government considerations around the drug would be governed less by strict cost-benefit considerations and more by security logics and political imperatives … Shifting out of the context of seasonal flu and into that of pandemic flu fundamentally transformed the financial arithmetic around Tamiflu."

DEBORAH R. COEN

2018

Climate in Motion

Science, Empire, and the Problem of Scale



"Until the twentieth century, theories of the global circulation of the atmosphere ignored motions smaller and shorter-lived than a major tropical cyclone. The circle of scientists around [19th-century meteorologist Julius] Hann bridged that gap, developing a picture of the interaction of small scale and large that still underwrites the climate models of today. Arguably, what makes modern climate science modern is its integration of phenomena of radically different dimensions …

Working without the aid of digital computers, Habsburg scientists invented creative ways to detect, model, and represent atmospheric motions. These included turning plants into measuring instruments, imagining riverbeds as models of atmospheric waves, and inventing new literary and cartographic genres … The scientific institutions of the supranational state formed a unique lens onto the natural world. Unlike administrators in Washington or Saint Petersburg, the emperor's ministers in Vienna saw good reasons, both practical and ideological, to support the study of climate down to the details of the smallest scales."

COURTESY IMAGES

DAVID EDGERTON

2006

The Shock of the Old

Technology and Global History since 1900

"The most innovative nations of the twentieth century have not been the fastest growing.

So powerful has this innovation-centric view been, especially in its nationalistic versions, that all evidence to the contrary has been studiously ignored … national rates of economic growth did not correlate positively with national investments in invention, research and development, or innovation. It has not been the case that countries that innovate a lot, grow a lot …

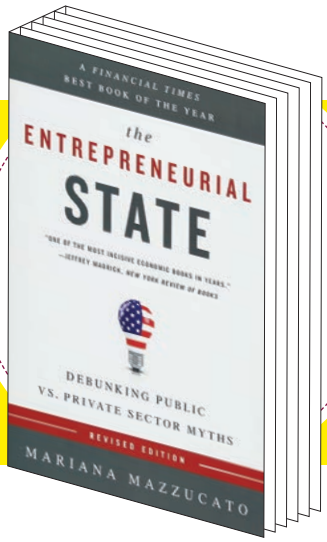
Why does the techno-nationalist assumption about innovation and growth not hold? The link between innovation and use, and thus economic performance, is far from straightforward. Yet the techno-nationalist assumption implies that the things a nation uses derive from its own invention and innovation, or at the very least that innovating nations have early leads in the technologies they innovate. Yet the site of innovation is not always the major site of even early use of the technology … Most technologies are shared across national boundaries; nations acquire more new technology from abroad than they innovate themselves."

MARIANA MAZZUCATO

2013

The Entrepreneurial State

Debunking Public vs. Private Sector Myths



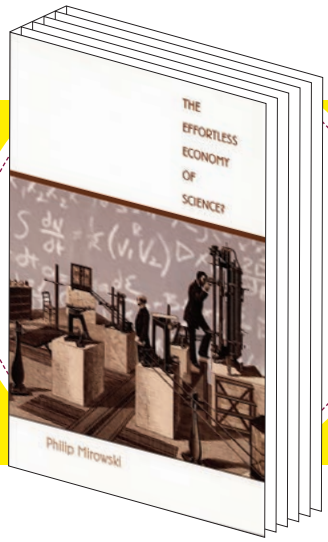
"This conventional view of a boring, lethargic State versus a dynamic private sector is as wrong as it is widespread … It creates a self-fulfilling prophecy: the less big thinking a government does, the less expertise it is able to attract, the worse it performs, and the less big thinking it is allowed to do and capable of doing …

If the State is so important to funding high-risk investments in innovation, it should follow that the State should earn back a direct return on its risky investments. Such returns can be used to fund the next round of innovations, but also help cover the inevitable losses that arise when investing in high-risk areas. So rather than worrying too much about the State's in/ability to 'pick winners,' more thought should be dedicated to how to reward the wins when they happen so that the returns can cover the losses from the inevitable failures, as well as funding new future wins. Put provocatively, had the State earned back just 1 per cent from the investments it made in the Internet, there would be much more today to invest in green tech."

PHILIP MIROWSKI

2004

The Effortless Economy of Science?



"If I had to summarize the experience of the last century, it seems to have consisted of one of the two root options: one says that science operates just like a market, so don't worry and be happy; while the other insists that science is the antithesis of the market, and must be approached with the reverence appropriate to a mystery, altogether denying the grubby details … [In fact] the economy is not merely an external agency which funds (or not) a free-standing immortal but independently constituted science … The new move to privatize and re-engineer university science had at its core a fundamental contradiction: *intellectual property in the larger society was no longer being structured primarily to foster personal innovation* … changes in intellectual property in the last two decades were rather primarily aimed at creating and engrossing intellectual property where it had not previously been dominant, and subsequently controlling and sequestering it for strategic corporate purposes … No one was thinking about the implications for science when they set about protecting Mickey Mouse … yet now do we reap the whirlwind."

A new book on the history of "people analytics."

By CHRISTINE ROSEN / Illustration by Andrea D'Aquino

The cult of human simulation

If you work for Bank of America, or the US Army, you might have used technology developed by Humanyze. The company grew out of research at MIT's cross-disciplinary Media Lab and describes its products as "science-backed analytics to drive adaptability."

If that sounds vague, it might be deliberate. Among the things Humanyze sells to businesses are devices for snooping on employees, such as ID badges with embedded RFID tags, near-field-communication sensors, and built-in microphones that track in granular detail the tone and volume (though not the actual words) of people's conversations throughout the day. Humanyze has trademarked its "Organizational Health Score," which it calculates on the basis of the employee data its badges collect and which it promises is "a proven formula to accelerate change and drive improvement."

Or perhaps you work for one of the health-care, retail, or financial-services companies that use software developed by Receptiviti. The Toronto-based company's mission is to "help machines understand people" by scanning emails and Slack messages for linguistic hints of unhappiness. "We worry about the perception of Big Brother," Receptiviti's CEO recently told the Wall Street Journal. He prefers calling employee surveillance "corporate mindfulness." (Orwell would have had something to say about that euphemism, too.)

Such efforts at what its creators call "people analytics" are usually justified on the grounds of improving efficiency or the customer experience. In recent months, some governments and public health experts have advocated tracking and tracing applications as a means of stopping the spread of covid-19.

But in embracing these technologies, businesses and governments often avoid answering crucial questions: Who should know what about you? Is what they know accurate? What should they be able to do with that information? And is it ever possible to devise a "proven formula" for assessing human behavior?

Such questions have a history, but today's technologists don't seem to know it. They prefer to focus on the novel and ingenious ways their inventions can improve the human experience (or the corporate bottom line) rather than the ways people in previous eras have tried and failed to do the same. Each new algorithm or app is, in their view, an implicit rebuke of the past.

If Then: How the Simulmatics Corporation Invented the Future

By Jill Lepore

W.W. NORTON, 2020, $28.95

COURTESY PHOTO

Today's "people analytics" is fueled by an age-old reductive conceit: the notion that human nature in all its complexities can be reduced to a formula. We know enough about human behavior to exploit each other's weaknesses, but not enough to significantly change it.

But that past can offer some much-needed guidance and humility. Despite faster computers and more sophisticated algorithms, today's "people analytics" is fueled by an age-old reductive conceit: the notion that human nature in all its complexities can be reduced to a formula. We know enough about human behavior to exploit each other's weaknesses, but not enough to significantly change it, except perhaps on the margins.

If Then, a new book by Jill Lepore, a historian at Harvard University and staff writer at the New Yorker, tells the story of a forgotten mid-20th-century technology company called the Simulmatics Corporation. Founded by a motley group of scientists and advertising men in 1959, it was, Lepore claims, "Cold War America's Cambridge Analytica."

A more accurate description might be that it was an effort by Democrats to compete with the Republican Party's embrace of the techniques of advertising. By mid-century, Republicans were selling politicians to the public as though they were toilet paper or coffee. Simulmatics, which set up shop in New York City (but had to rent time

on IBM's computers to run its calculations), promised to predict the outcome of elections nearly in real time—a practice now so common it is mundane, but one then seen as groundbreaking, if not impossible.

The company's name, a portmanteau of "simulation" and "automatic," was a measure of its creators' ambition: "to automate the simulation of human behavior." Its main tool was the People Machine, which Lepore describes as "a computer program designed to predict and manipulate human behavior, all sorts of human behavior, from buying a dishwasher to countering an insurgency to casting a vote." It worked by developing categories of people (such as white working-class Catholic or suburban Republican mother) and simulating their likely decision-making. (Targeted advertising and political campaigning today use broadly similar techniques.)

The company's key players were drawn from a range of backgrounds. Advertising man Ed Greenfield was one of the first to glimpse how the new technology of television would revolutionize politics and became convinced that the earliest computers would exercise a similarly disruptive force on democracy. Ithiel de Sola Pool, an ambitious social scientist eager to work with the government to uncover the secrets of human behavior, eventually became one of the first, prescient theorists of social networks.

More than any other Simulmatics man, Pool embodied both the idealistic fervor and the heedlessness about norm-breaking that characterize technological innovators today. The son of radical parents who himself dabbled in socialism as a young man, he spent the rest of his life proving himself a committed Cold War patriot, and he once described his Simulmatics work as "a kind of Manhattan Project gamble in politics."

One of the company's first big clients was John F. Kennedy's presidential campaign in 1960. When Kennedy won, the company claimed credit. But it also faced fears that the machine it had built could be turned to nefarious purposes. As one scientist said in a Harper's magazine exposé of the company published shortly after the election, "You can't simulate the consequences of simulation." The public feared that companies like Simulmatics could have a corrupting influence on the democratic process. This, remember, was nearly half a century before Facebook was even founded.

One branch of government, though, was enthusiastic about the company's predictive capabilities: the Department of Defense. As Lepore reminds readers, close partnerships between technologists and the Pentagon were viewed as necessary, patriotic efforts to stem the tide of Communism during the Cold War.

By 1966, Pool had accepted a contract to oversee a large-scale behavioral-science project for the Department of Defense in Saigon. "Vietnam is the greatest social-science laboratory we have ever had!" he enthused. Like Secretary of Defense Robert McNamara (whom Barry Goldwater once referred to as "an IBM machine with legs" and who commissioned the research), Pool believed the war would be won in the "hearts and minds" of the Vietnamese, and that it required behavioral-science modeling and simulation to win. As Lepore writes, "Pool argued that while statesmen in times past had consulted philosophy, literature, and history, statesmen of the Cold War were obligated to consult the behavioral sciences."

Their efforts at computer-enabled counterinsurgency were a disastrous failure, in large part because Simulmatics' data about the Vietnamese was partial and its simulations based more on wishful thinking than realities on the ground. But this didn't prevent the federal government from coming back to Pool and Simulmatics for help understanding—and predicting—civil unrest back home.

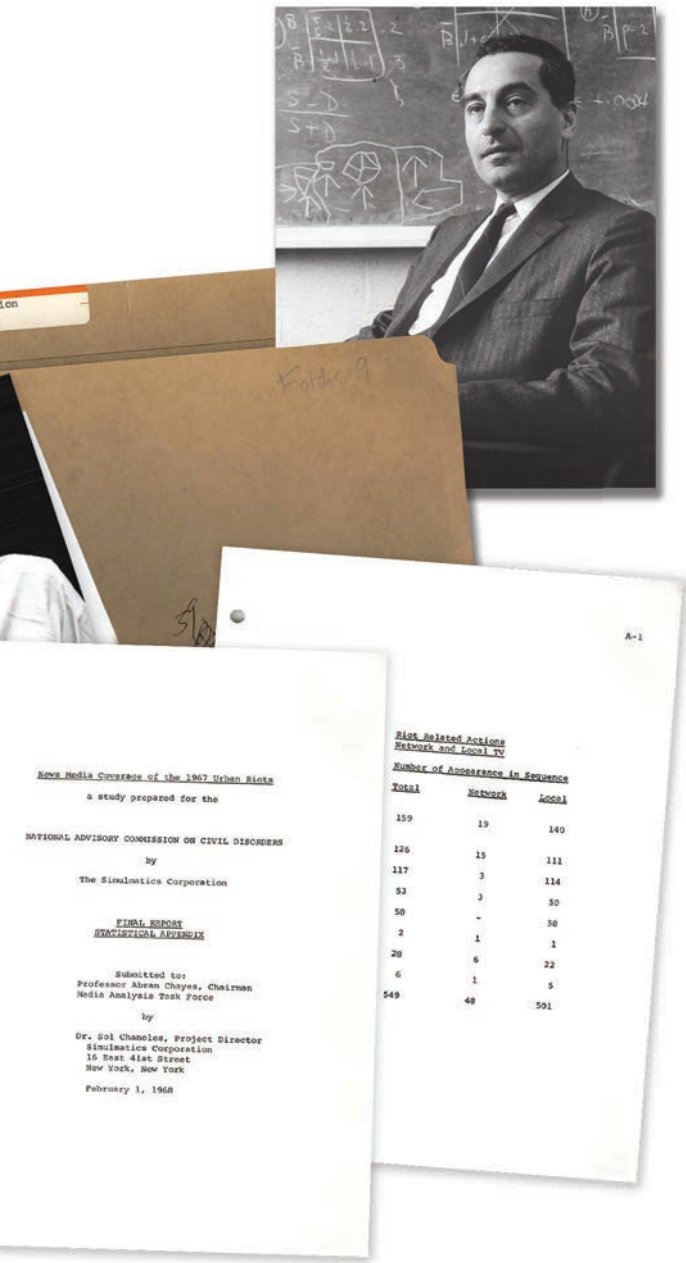
The Kerner Commission, convened by President Lyndon Johnson in 1967 to study the race riots that had broken out across the country, paid Simulmatics' Urban Studies Division to devise a predictive formula for riots to alert authorities to brewing unrest before it devolved into disorder. Like the predictions for Vietnam, these too proved dubious. By the 1970s, Simulmatics had declared bankruptcy, and "the automated computer simulation of human behavior had fallen into disrepute," according to Lepore.

Simulmatics "lurks behind the screen of every device" we use, Lepore argues, and she claims its creators, the "long-dead, white-whiskered grandfathers of Mark Zuckerberg and Sergey Brin and Jeff Bezos and Peter Thiel and Marc Andreessen and Elon Musk," are a "missing link" in the history of technology. But this is an overreach. The dream of sorting and categorizing and analyzing people has been a constant throughout history. Simulmatics' effort was merely one of many, and hardly revolutionary.

Far more historically significant (and harmful) were 19th-century projects to categorize criminals, or early 20th-century campaigns to predict behavior based on pseudoscientific categories of race and ethnicity during the height of the eugenics movement. All these projects, too, relied on data collection and systematization and on partnerships with local and state governments for their success, but they also garnered significant enthusiasm

Above: Simulmatics cofounder Ithiel de Sola Pool once described his work as "a kind of Manhattan Project gamble in politics."

Below: The Kerner Commission, convened by President Lyndon Johnson in 1967 to study the race riots that had broken out across the country, paid Simulmatics' Urban Studies Division to devise a predictive formula for riots.



News Media Coverage of the 1967 Urban Riots

a study prepared for the

NATIONAL ADVISORY COMMISSION ON CIVIL DISORDERS

by

The Simulmatics Corporation

FINAL REPORT
STATISTICAL APPENDIX

Submitted to:
Professor Abram Chayes, Chairman
Media Analysis Task Force

by

Dr. Sol Chanoles, Project Director
Simulmatics Corporation
16 East 41st Street
New York, New York

February 1, 1968

A-1

Riot Related Actions
Network and Local TV

Number of Appearance in Sequence

Total	Network	Local
159	19	140
126	15	111
117	3	114
53	3	50
58	-	58
2	1	1
28	6	22
6	1	5
549	48	501

MIT MUSEUM (POOL); RICHARD RODSTEIN | WIKIMEDIA VIA CC SA 3.0 (POOL, 1983); LBJ PRESIDENTIAL LIBRARY (FOLDER: RECORDS OF THE NACCD, SERIES 39, BOX 7)

"The profit-motivated collection and use of data about human behavior, unregulated by any governmental body, has wreaked havoc on human societies."

from large swaths of the public, something Simulmatics never did.

What is true is that Simulmatics' combination of idealism and hubris resembles that of many contemporary Silicon Valley companies. Like them, it viewed itself as the leading edge of a new Enlightenment, led by the people best suited to solve society's problems, even as they failed to grasp the complexity and diversity of that society. "It would be easier, more comforting, less unsettling, if the scientists of Simulmatics were villains," Lepore writes. "But they weren't. They were midcentury white liberals in an era when white liberals were not expected to understand people who weren't white or liberal." Where the Simulmatics Corporation believed that the same formula could understand populations as distinct as American voters and Vietnamese villagers, today's predictive technologies often make similarly grandiose promises. Fueled by far more sophisticated data gathering and analysis, they still fail to account for the full range and richness of human complexity and variation.

So although Simulmatics did not, as Lepore's subtitle claims, invent the future, its attempts to categorize and forecast human behavior raised questions about the ethics of data that are still with us today. Lepore describes congressional hearings about data privacy in 1966, when a scientist from RAND outlined for Congress the questions it should be asking: "What is data? To whom does data belong? What obligation does the collector, or holder, or analyst of data hold over the subject of the data? Can data be shared? Can it be sold?"

Lepore laments a previous era's failure to tackle such questions head-on. "If, then, in the 1960s, things had gone differently, this future might have been saved," she writes, adding that "plenty of people believed at the time that a people machine was entirely and utterly amoral." But it is also oddly reassuring to learn that even when our technologies were in their rudimentary stages, people were thinking through the likely consequences of our use of them.

As Lepore writes, Simulmatics was hobbled by the technological limitations of the 1960s: "Data was scarce. Models were weak. Computers were slow. The machine faltered, and the men who built it could not repair it." But though today's people machines are "sleeker, faster, and seemingly unstoppable," they are not fundamentally different from that of Simulmatics. Both are based on a belief that mathematical laws of human nature are real, in the way that the laws of physics are—a false belief, Lepore notes:

> [T]he study of human behavior is not the same as the study of the spread of viruses and the density of clouds and the movement of the stars. Human behavior does not follow laws like the law of gravity, and to believe that it does is to take an oath to a new religion. Predestination can be a dangerous gospel. The profit-motivated collection and use of data about human behavior, unregulated by any governmental body, has wreaked havoc on human societies, especially on the spheres in which Simulmatics engaged: politics, advertising, journalism, counterinsurgency, and race relations.

While Simulmatics failed because it was ahead of its time, its modern counterparts are more powerful and more profitable. But remembering its story can help clarify the deficiencies of a society built on reductive beliefs about the power of data, and illuminate a path toward a dignified, vibrant, human future.

Christine Rosen is senior writer at Commentary magazine and a senior editor at The New Atlantis: A Journal of Technology & Society.

Fiction

The First Murder

When did the shadow begin to follow you?

It did not touch you as a child, on those summer days spent climbing the pecan tree in your parents' backyard. Nor did it touch you as a student seated in the wood-paneled lecture halls of law school. It kept its distance as the years passed, as you matured into responsibilities, habits, tastes.

You are given to formal attire. You are even-tempered and good at compartmentalizing. You do not speak more than you need to. You credit this to growing up an only child in the company of reticent adults. You have achieved what you are supposed to achieve—an office job, a house, a car. You have kept the same sedate occupation for two decades, parceling out the wealth of the dead amongst the living. You live in a semi-detached colonial with a gabled porch in a neighborhood of lawyers and professors. When you are not walking, you drive a Volvo—a solid, unpretentious vehicle. Only in establishing a family have you fallen short. Your wife became disturbed by your equanimity, mistaking your composure for lack of sentiment. In fact, you were deeply hurt when she left, though perhaps you did not show it.

But with time the abandonment hurts less and less, especially as you find pleasure in your solitude. You follow your routines religiously. Weekend mornings begin with an unhurried breakfast, the Daily Inquirer, a walk. Once a week you drive to the allotment on the edge of the city where you grow marigolds and petunias, tomatoes and broad beans. The company of your plants is as stimulating to you as that of friends, of which you have very few, as most of them left with your wife. But your true passion is the opera. You attend a performance twice a month, an indulgence which marks the passing of the weeks. Your emotions find catharsis in the opera—circumspectly, in the darkness.

The opera house is as familiar to you as your own home. There are 11 rows of seats curving around the balcony where you like to sit. If it is available, you always purchase seat 56A, third row from the front, which affords as good a view as the first row but for a lesser price. It is an aisle seat, close to the exit, which means that you can be quick about leaving when the opera ends.

The opera adds variety to your schedule. You know you will see an opera, but you do not know what you will feel, though you know that you will always feel something.

The shadow first descends upon you on the night of a performance. You go to see *Il Primo Omicidio*. Alessandro Scarlatti, 1707. You read the pamphlet. "Evil has no recourse. Cain kills

BY FATIN ABBAS
ILLUSTRATIONS BY DANIEL ZENDER

The stage is mostly bare, except for when God appears, a pixelated white shadow against a dark backdrop.

his brother Abel and commits the first murder in the history of humankind …"

A biblical opera is not normally to your taste. You prefer the passions of the great love affairs. Is it because you have failed at your own? And yet you go because you have heard of the world-renowned director. His name is Castellucci—a genius, or so the papers say. You were lucky even to find tickets.

You ensconce yourself in the familiar darkness of the theater, though not in your usual seat, which has been booked by someone else. However, at 63B you are not far from your accustomed vantage point. You settle in, feeling a thrill of anticipation in spite of the biblical genre.

And indeed when the curtain rises you are taken aback. The first surprise is that Cain and Abel are women. Or, rather, women cast as men. Modern dress—slacks, dress shirts, the uniform of casual businessmen. Hair short and slicked sideways. The singers' movements are protracted, drawn out. Biblical, epic gestures. The first murder is epic not only because it is the first, but also because it is brother upon brother.

The stage is mostly bare, except for when God appears, a pixelated white shadow against a dark backdrop. There is a glittering gold altar. It descends upside down, like a giant knife, above Cain and Abel. There is the scene of the sacrifice. Steam rises from two machines. And then, one stops. Cain's sacrifice to Yahweh does not take. At the end of the opera you sit blinking until people trip over your legs. You stand, let them pass. You sit down again and stare at the stage, enthralled by the magic wrought on you.

When you find your parked car, you notice the smashed taillight. Accident or vandalism, it does not dampen your mood, though you instruct yourself to take the car to the shop in the coming days.

Shop lights whirl about you on the drive home. Laughter filters in from restaurant tables set out in the warm night. As you wait for lights to change, your eye falls upon a billboard. White letters illuminated by floodlights against a black backdrop. Trans-migration. Painless. Quick procedures. Human-animal. Male-female. Animate-inanimate. 777-7777. The letters fog and fade out toward the top, miming a transmigration into the billboard. The light changes and you press on the gas.

At home, you prepare for bed, still basking in the glow of the beautiful evening. Out of habit, you turn on the news. A video loops. A man, in the cage of his skin, running. A silent shot. Death. You are struck by the movements of the police officers and the man, which are hasty, inelegant. You think of the opera. The man's end is neither epic nor biblical.

The magic of the evening gives way to the video. The feeling of contentment leaves you. Even when you turn off the news, the image of the man hangs in the emptiness. As you brush your teeth you pace up and down the hallway. You spit into the sink, wash off the foam around your lips. You think of how far removed your life is from that of the man in the video. You live in the good part of town, hold steady, well-compensated employment. You attend the opera, even travel to Europe on occasion. Your life is circumscribed. You go to bed, reassuring yourself that sleep will efface the image from your mind.

But when light breaks your first thought is of the man.

As you drink your coffee you guide your mind back to the opera, the cross-dressing Cain and Abel, the upside-down altar. You recall the wonder it evoked in you. You forget the video long enough to make the mistake of turning on the morning news. The video appears. You turn off the television. You switch on your phone but there, too, it plays.

Over the next days you go to the office. You have gleaned from the news that the man in the video has left behind unpaid rent, traffic fines, credit card bills. To whom will this inheritance of debt pass?

You drive to the allotment and attend to your flowers and vegetables. You cook lamb braised in wine. You read a biography of Michel de Montaigne. But as you go about your routines, you find that the man runs after you. In your sleep and in your waking moments, he runs toward you. Always he is present on the edge of your vision, or directly before your eyes. When he falls, he falls on top of your chest.

One night you wake up gasping for air. You mistake the dampness along your neck for blood. When you go to the bathroom to splash water on your face, you look in the mirror and see that the skin has begun to crack. Hair's-breadth cracks, almost invisible. It is age—you are growing old—but you sense that the disintegration runs deeper.

You decide you must pull yourself together. A week after *Il Primo Omicidio*, you go to the opera again. When the bell rings you find your seat in the balcony. This time it is a light opera, befitting the mood you wish to enter. The singers under the spotlight divert your attention. Bewigged sopranos and men in tights. The lead baritone hits a

depth in his throat that reverberates in your ribs. But, unusually for you, the opera leaves you cold.

At home, you make yourself a tea. You sink into an armchair and stare at the wall. You pick up your phone and play the video. You play it again and again. You cannot get enough. The clumsy escape, the raised gun. The death is real, and yet the movements seem like a pantomime, awkward and inadequate.

You have always thought only of yourself. But why should you not? What has come over you? The man is dead. What use is it to dwell on it? It does not concern you. You are here, walking about the world. And yet each time the man runs, dread rises in your chest. Why did he not stay put? He would have been better off if he had.

The next morning is a Saturday. To avoid encountering more news of the man, you do not open the paper. Instead you go for your walk earlier than usual. The air is fresh outside; it has been raining. But even outside there is no relief. You sit on a park bench and stare at a desolate playground. Rain has swept children away. You think of the opera. Not the frivolous one you attended last night, but the other one.

The women dressed as men come back to you. The billboard with the transmigrating print. You are familiar with the movement. People who enter into other bodies, selves—the bodies of animals, or the poor, or of women, or of men. A rebirth into a new identity. Those who transmigrate into the bodies of the less fortunate are accused of tourism, voyeurism. Less is known about those who choose to go the other way.

On Monday, from the office, you dial the number on the billboard. You explain what you want. The voice on the other end is briskly helpful—you are given an appointment.

In the meantime you make arrangements. You give notice at work, making up a family emergency that requires you to move to the opposite coast. You have enough saved to get you through the next year at the very least. The opera is your one extravagance; otherwise you are parsimonious.

Ten days later you arrive at a bare, white office space. You sit opposite a woman who flicks the pages of a magazine too quickly. You wonder what transmigration she is about to undertake—does she seek to accompany the dog that sits quietly panting at her feet?

Before long an attendant calls you into a room. You change into a hospital gown behind a curtain.

You put on glasses. Then you are instructed to lie on a hard bed—it looks like a sun bed. There is a cushion for the crooks of your knees, though not one for your head.

You think of what you have glimpsed in the news this morning. The video has caused such an uproar that the policemen have been taken into custody. There are investigations. Politicians and police chiefs have been standing somberly before the press. The man's mother and his wife weep in front of the cameras.

The attendant draws the lid closed and you are cocooned in light. The bed hums and vibrates beneath your limbs. You close your eyes.

When you wake up, you can feel a tingle along the skin between your fingers. The bed slides out and the attendant tells you to rise. She leads you to a mirror. You take off your glasses. A man stares back at you. His skin is not your own. His hair is dark, though peppered with gray at the crown. He mimics your movements—when you turn left, so does he. When you lift your chin, he follows. When you touch your shoulder, he reaches for his.

But not everything has changed. You are still thin. You speak in the voice and register that belongs to your old self—well-enunciated, resonant, its statements infiltrated by a formal, lawyerly vocabulary. You feel familiar thoughts and impulses stir in you, and yet already you sense the effect of the mirrored reflection upon yourself, a reflection to which you are attracted, and from which, simultaneously, you recoil.

After you pay, you step out into the street. You blink, turn left and right, adjusting to your new body. You look boldly at those who walk past. An unmistakable spark comes into the eyes that flicker over you. A woman gives way on the pavement as you approach. A man barrels forward, seemingly oblivious to you, and you are forced to step aside.

Your new identity involves much bureaucracy—driver's license, passport, health insurance card must be updated, and so you stop to have your photo taken. You pose in front of a white background. Keep your lips closed, the photographer tells you. A flash. You put an envelope into your pocket. At home, you are startled anew at the strange face staring back at you, its tight smile melding into the regard of two mysterious eyes.

Over the next few days the knowledge grows on you that you are mostly invisible. And when you are visible, eyes glance at you with a mindful apprehension—different from what you experienced in your other body. You have sensed it all along, even before your transmigration—there is a fear that gives strength and a fear that takes it away.

You look for your likeness in the world. You are present and absent in ways that are new to you. You pay attention to the cadences of the voices that address you. You brush against strangers in the street and see what reaction your touch evokes. You attend a neighborhood council meeting, just to see what happens when you rise to speak.

You go to places you have frequented, and others you have never been to. You visit the sour clerk at the coffee shop at which you are a regular. You have always wondered if his ill humor is reserved for you or is all encompassing. You step into an expensive restaurant and anticipate the hostess's response. Will she give you the table by the window?

On a walk, you wander into an unfamiliar neighborhood. You immediately sense the air thick with hostility. People stare at you. Is it the video looping in the news? You wait for the lights to change, resisting the temptation to look over your shoulder. You think of the man running. He had been strolling, too, when he had lost track of his surroundings and strayed into a neighborhood of elegant columned houses. A police car—lights whirling silently—had drawn up beside him.

You hurry out of the neighborhood, across the avenue that divides one section of town from another, relieved when you reach home. You have crossed over. Was it to rewrite the fate of the man in the video or to rewrite your own?

A month into your transmigration, you read that *Il Primo Omicidio* has moved to a city two hours away. It is a final run. You are seized by the impulse to see it again. The opera, the video, the crossing over. They are mixed up together in your mind. Another viewing feels fitting, like the conclusion to a ritual.

The opera house in the next city is larger. There are many hallways and entryways and balconies, and you get lost trying to find your way. You take your seat just in time and wait for the darkness to swallow you up. The curtain rises. A vast blue horizon comes into view. Cain and Abel march onto the stage. Again you experience the magic of the scenery, the upside-down altar sparkling under spotlights, the steam machines, the God on the projection screen. In the darkness, you forget who you are, what you have become. The lights come up.

On the highway, the darkness is as complete as that in the theater. You cannot see your hands nor the tip of your nose, which is normally how, during those rare moments when you forget, you recall that you have crossed over.

There are few cars on the road. Fluorescent lane markings dart out at you hypnotically. You think of the murder scene—Abel sleeping in a field under starlight, blades of grass frozen in mid-motion as though snapped in a photograph on a windy day. Cain stealthily approaching, carrying a rock.

Your hands on the steering wheel turn red, then blue. You glance at the rearview mirror. It takes you a moment to realize that the whirling lights are for you. You are confused only for an instant. The taillight. In the tumult of the previous weeks, you never visited the car garage. As you slow down you are tense with expectation. You have been waiting for this, or something like it.

You come to a stop on the hard shoulder. The police car parks behind you. Your hands continue to flicker red and blue. You see a door open, an officer step out. You roll down your window. The noise of the highway washes away the cozy atmosphere of the car. The officer walks toward his own silhouette reflected in your side view mirror. The beam of his flashlight dances ahead of him. Finally he is at your window. The light is blinding. It hovers over you, dashes briefly into the car, then returns to your face.

He asks for license and registration. And your moment of truth arrives.

Fatin Abbas's first novel, The Interventionists, is forthcoming from W.W. Norton. She lives in Berlin.

MIT Technology Review

GIVE THE GIFT OF INNOVATION

Share MIT Technology Review's award-winning tech coverage with a friend, colleague, or recent grad.

- Bi-monthly print and digital issues
- Paywall-free website access
- Subscriber-only content
- The Download email newsletter
- The Algorithm, weekly AI email newsletter (subscriber-only)
- *Deep Tech* podcast (subscriber-only)

Learn more at trsub.com/fall2020

No, we can't all just get along

The current trend toward technonationalism feels fairly recent, yet this publication has been returning to the problem in some form or another for almost 90 years.

January 1931

From "Machine-Age Politics": The technological drive in government has broken down historical relations between political units, just as it has changed the linkage between governors and governed. To be sure, the custom of parceling off the world and each country into little areas under separate rule continues unabated. In the United States this habit is responsible for the fierce battle always raging over states' rights. In general it is responsible for the spirit of nationalism which so often sets the world aflame. But the cable, the railway, the radio, air mail, and their companions of iron and steel are steadily raising new questions respecting political boundaries. How far is ancient sectionalism compatible with the operating requirements of modern technology? Here is a big issue for the future to face.

December 1965

From "The Pressure of Numbers": How can human behavior be directed into channels of concern for man to replace parochial group rivalries and hates? Clearly new patterns of thought are needed as never before to meet the crises of our time. Most of the beliefs we hold so strongly are established by accident of birth and what we learn, hit or miss, before we are seven years old. Emotionally charged prejudices are propagated from generation to generation by parental and adult authority and by the use of myths and symbols. The strongest beliefs one holds may bear little relation to the facts and realities of life as related to the common good. Irrational aspects of human behavior—chauvinistic nationalism and racial intolerance—keep us locked in patterns of conduct highly dangerous in the nuclear age, and dangerous in relation to other changes brought about by science.

February/March 1985

From "Charting the Way the World Works": At some level nearly everyone understands how the world works, yet governments do not often operate in accordance with their understanding. While knowing that the world is an interdependent, richly varied system, we act as if it were made up of simple, separate pieces. Knowing that cooperation works better than competition, we continue to compete. Knowing that short-term results often differ from long-term ones, we go for the short-term payoff. Knowing that the environment flows through us with every drink, breath, and meal, we still think of nature as distinct from humanity. The earth is a diverse, abundant planet. However, the assumption that most pervades decision making in our era is scarcity. The reaction is to hoard and try to increase short-term production.

MIT Technology Review (ISSN 1099-274X), September/October 2020 issue, Reg. US Patent Office, is published bimonthly by MIT Technology Review, 1 Main St. Suite 13, Cambridge, MA 02142-1517. Entire contents ©2020. The editors seek diverse views, and authors' opinions do not represent the official policies of their institutions or those of MIT. Periodicals postage paid at Boston, MA, and additional mailing offices. Postmaster: Send address changes to MIT Technology Review, Subscriber Services, PO Box 5001, Big Sandy, TX 75755, or via the internet at www.technologyreview.com/customerservice. Basic subscription rates: $59.94 per year within the United States; in all other countries, US$69. Publication Mail Agreement Number 40621028. Send undeliverable Canadian copies to PO Box 1051, Fort Erie, ON L2A 6C7. Printed in USA. Audited by the Alliance for Audited Media.

MIT Technology Review

ATTENTION MAGAZINE SUBSCRIBER!

Access more content as part of your subscription

Activate your account to avoid that pesky paywall and start enjoying...

- *Deep Tech* podcast
- The Algorithm, weekly AI email newsletter
- Exclusive stories and content
- MIT Technology Review mobile app
- Digital-version of the print magazine

Stay ahead. Stay connected.
technologyreview.com/SubOnly

MIT Technology Review
Global Panel

Share your opinion about today's top tech trends. Join our Global Panel.

As a member of MIT Technology Review's fast-growing group of executives and innovators, you can take part in surveys and weigh in on the impact of AI, blockchain, and other technologies—plus get in-depth news and analysis to inform business strategy.

Apply today and get our latest research report free:
insights.technologyreview.com