THE CYBERSECURITY ISSUE

THE FUTURE OF EVERYTHING

A LOOK AHEAD FROM THE WALL STREET JOURNAL.

THE NEXT TARGETS

Hacks are evolving. Hospitals, schools and kitchen appliances are just the beginning. **R4-5**

PLUS

How companies plan to spend—or not—on security **R8**

Swipe Up to Vote

What would it take to replace ballots with smartphone apps? **R6**

Beating Quantum

Cryptographers vie to protect data from superfast computers **R9**

War and Peace

A former White House official lays out two versions of cyberspace to come **R10**

ILLUSTRATION BY JUSTIN METZ

SOFT HACKS: EXPLOITING HUMAN BEHAVIOR

Campaigns to spread bad information on social media are emerging as a new online security problem for companies. **By Robert McMillan**

An unscrupulous company uses Twitter bots to spread rumors that a competitor is sharing data with China. A short seller spreads lies about a company's business practices in a conspiracy-minded online community to drive down the stock price. Both could cause harm, and both are examples of a new threat poised to hit businesses, cybersecurity experts say.

For years online security has focused on technical problems: Fixing software bugs or concealing data with cryptography. Today, a new front is emerging: Disinformation attacks. Once the near-exclusive provenance of nation-state attackers and activists, they are starting to become a problem for corporations.

"Right now everybody is implicitly assuming that the only possible victim is an election," says David Perlman, a former Twitter Inc. data scientist who is now developing ways for corporations to counter disinformation at the computer security company Leviathan Security Group Inc. "There's no reason that a company couldn't be a victim."

Disinformation is similar to its sister term, misinformation: Both refer to false or misleading information. But disinformation is spread with the intent to deceive.

Disinformation is the newest manifestation of the shady art of mental manipulation, which already has a history in the world of cybersecurity. First there were phishing attacks, where victims would get bogus email messages designed to trick them into divulging passwords or downloading malicious software. These early efforts evolved into more complicated "social engineering" techniques, where hackers first conduct background research and then call employees pretending to be co-workers, for example, and trick them into handing over data granting access to corporate networks.

David Perlman, a former Twitter data scientist, says that companies need to take aggressive steps to fight the spread of disinformation before it goes viral.

Defenses against these attacks are called "cognitive security" or "misinfosec."

A growing group of cybersecurity thinkers believes that disinformation is a new weapon in these psychologically driven attacks—one that will be used by cyberattackers too, perhaps for extortion, market manipulation or to damage a rival's reputation.

"In the last 10 years, the information age has really matured," says Marc Rogers, vice president of cybersecurity strategy with the security company Okta Inc. "Now for just a few thousand dollars you can invest in some infrastructure and you can launch a disinformation campaign that will bring a country the size of America to its knees."

Pablo Breuer, a former Navy officer, was a mission director at the National Security Agency in the early 2000s when a series of global computer worms served as a wake-up call about the importance of cybersecurity. He thinks that companies are on the verge of a similar awakening—this time on the disinformation threat.

Though hackers and nation-states have created disinformation campaigns to sway public opinion around issues, such as the 2016 election, there is no clear evidence that they have targeted companies. Still, potential threats are myriad, cybersecurity experts say.

With few legal restrictions on spreading disinformation and the wide-open nature of social media platforms, these experts worry that adversaries may resort to extreme tactics, such as deepfakes—video, audio and photographs doctored using advanced techniques.

This kind of problem is starting to pop up. So far, attacks don't appear to be criminally motivated.

In July, false rumors started spreading on Twitter and Instagram that the online home-goods retailer Wayfair Inc. was engaging in child sexual exploitation through high-price, industrial-grade cabinets. A Wayfair spokeswoman says that the company acted quickly to debunk the claims and remove the listings of the cabinets in question, but months later, the conspiracy theory continues to generate posts on social media.

The origin of the Wayfair incident—whether part of a strategic campaign to damage the company's brand or an instance of rumors run amok—is unclear. It is possible, Mr. Perlman and Mr. Breuer say, that it was a test run for future attacks. The point is that in the age of social media, hackers, competitors and other bad actors have a new tool to wreak havoc online, without ever needing the technical prowess to break into corporate networks.

Attackers can wreak havoc online without the technical skills to break into corporate networks.

Companies are going to need to take aggressive steps, such as monitoring social media for disinformation and deepfakes, so that they are aware of potential problems before issues go viral. While research is in its early days, they call defenses against these attacks "cognitive security" or "misinfosec."

Companies including Reston, Va.'s Mandiant, New York's Graphika Inc. and Washington, D.C.-based Alethea Group specialize in providing early warnings and analysis of online disinformation, helping their clients get a clear picture of online discussions and how to respond to them. Are they dealing with a grass-roots boycott or something more sinister, like disinformation? Is the information reaching their customers or not?

Mr. Perlman believes that social media companies such as his former employer, Twitter, could one day sell these types of services too.

Social-media companies are used to blocking spam or banning users for inappropriate content. They have been caught flat-footed by efforts to manipulate the platform with conspiracy-minded content that doesn't look like spam, Mr. Perlman says.

Twitter aims to "limit the spread of potentially harmful and misleading content," a spokeswoman says.

Corporations can't simply wait for social-media companies to act and must develop a playbook for thwarting weaponized disinformation, data scientists say.

Businesses will need to do more in the age of disinformation warfare. They will need to be more transparent in disclosing information that could be weaponized—listing political donations, for example, Mr. Breuer says. Disinformation attacks begin with a kernel of truth (a company donated to a candidate) but spin that information to come to a false conclusion (the donation was payback for a political favor). Self-disclosure could help stop disinformation before it spins out of control.

Cyber teams will need to work with communications departments to run exercises where disinformation campaigns are detected and debunked.

To fight back against deepfakes, a defender could seed the internet with intentionally fake photographs of himself, Mr. Perlman says. It is an extreme measure, but it could minimize the impact of further deepfake releases, he says.

"If there are no police, and you are living in the Wild West, then you have to arm yourself," he says.

FROM TOP: JESSICA CHOU FOR THE WALL STREET JOURNAL; PHOTO ILLUSTRATION BY QUINN RUSSELL BROWN FOR THE WALL STREET JOURNAL; ILLUSTRATION BY JASON LEE

FORWARD LOOKING

Safety at Work

In the coming years, professions will emerge to tackle new cyber threats.

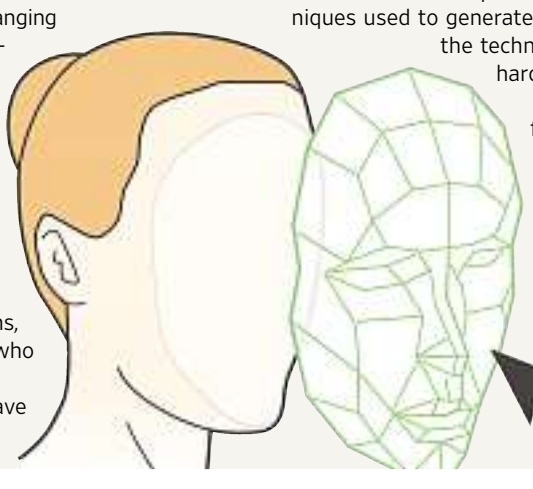
By Benoit Morenne

Deepfake Analyst

A viral video shows a presidential candidate changing her stance on a crucial issue the day before voters head to the polls. A video admitted as evidence in a court case shows a man entering a building where a crime was later committed.

These are some of the ways malicious actors could use deepfakes—video or audio clips manipulated through artificial intelligence—to compromise a business, put innocents behind bars or interfere in the electoral process.

Enter deepfake analysts. Large organizations, news companies and courts will hire experts who use the latest technologies to spot instances where someone's face, voice or movements have been altered using AI.



This role will require an academic understanding of the AI techniques used to generate content but will also be research-intensive as the technology progresses and doctored media become harder to detect.

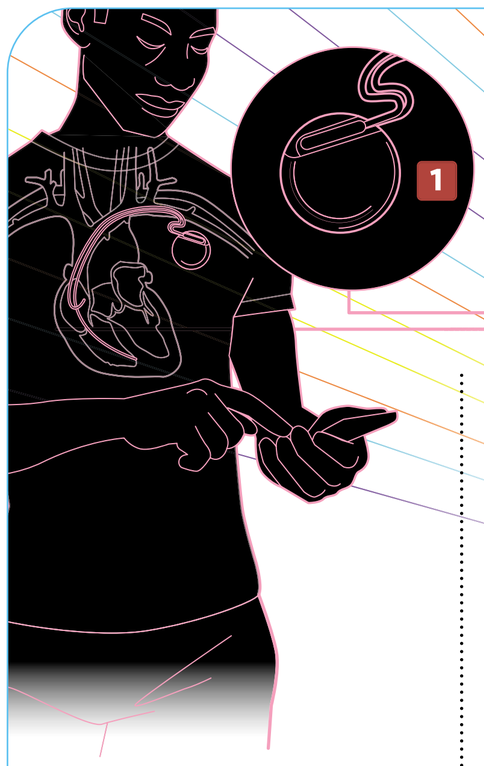
The analysts' toolbox will need to include fact-checking, contextual analysis and visual investigative skills, according to Robert McArdle, a director in Japan- and U.S.-based IT security company Trend Micro's forward-looking threat research team. For instance, do the shadows in surveillance footage match where they should be in relation to the sun?

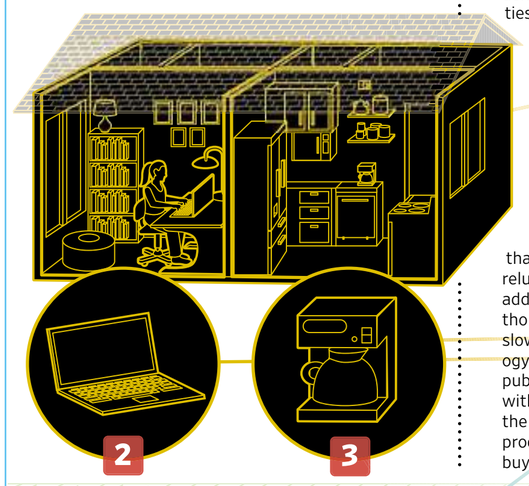
"A good deepfake analysis person should be able to put all of that stuff apart, and not just give you the technical readouts," Mr. McArdle says.

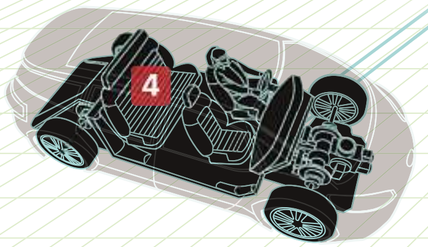
Continues on page R6 ▶▶

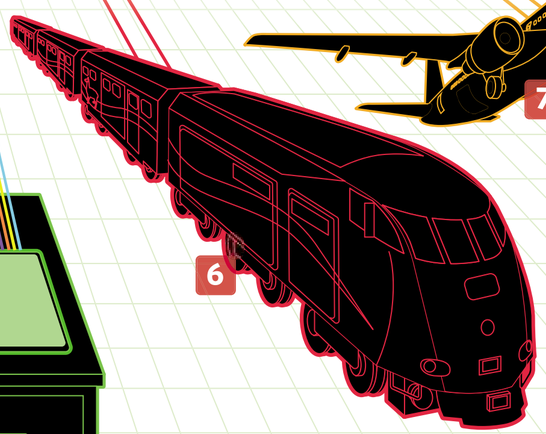
HACKING'S NEXT TARGETS

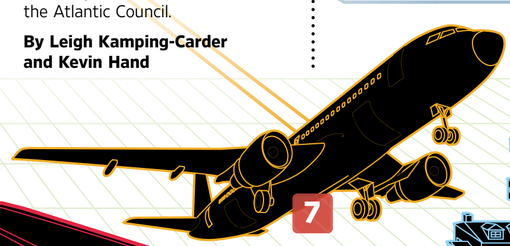
Systems we use every day may not be secure tomorrow.
Here's what cybersecurity experts say could be a future focus for attacks.

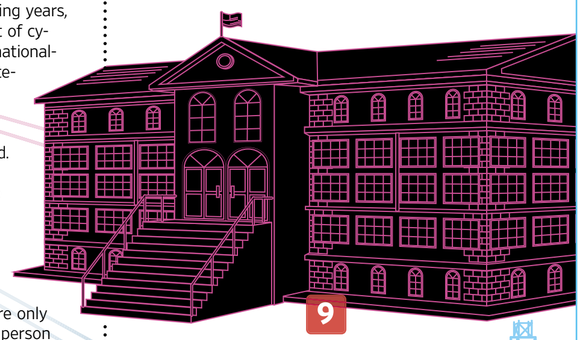


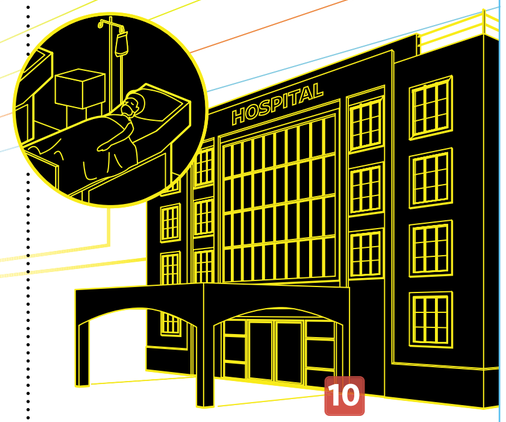


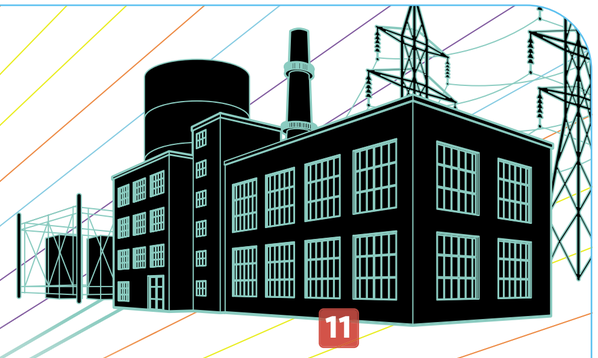












Hackers will tell you that just about anything with software and an internet connection can get hacked. The next decade will test how much that is true, and the challenge it poses to everyday life.

Security experts expect cyberattacks to increase in frequency and severity in the coming years, as more consumer goods are sold with internet connectivity embedded by default. At the same time, cyberattacks have become a commodity—"ransomware-as-a-service," says Keren Elazari, a security researcher and "friendly" hacker, also known as a "white-hat" hacker, who typically hacks to educate or to demonstrate security vulnerabilities rather than commit crimes.

For cyberattackers, hacks are getting more accessible: Attacks that once cost $100,000 go for a mere $1,000 now, says Jeff Moss, founder of DEF CON, an annual conference for hackers. Devices that are secure today may not be tomorrow.

Adding to the problem is that manufacturers have been reluctant to acknowledge and address cybersecurity flaws, though experts say that is slowly changing. Still, technology is advancing faster than public policy, leaving consumers without clear ways to evaluate the relative cyber safety of products. In other words, if you buy a car, you can compare which models have the best crash-safety ratings. And if the car crashes because of a manufacturer error, government agencies, dealerships and even lawyers can help make things right. Equivalents don't exist to, for example, assess the relative vulnerabilities of vehicle infotainment systems, or to assign liability or get compensation if someone hacks that system and immobilizes your car.

"As a society, we haven't figured any of this stuff out," Mr. Moss says. "Over the next decade, I bet we will."

To get a sense of future threats, The Wall Street Journal compiled a list of common devices, equipment and infrastructure vulnerable to attacks in the coming years, based on the assessment of cybersecurity researchers, national-security experts and white-hat hackers.

Keep in mind: This is only a small sample of what could be threatened. Experts consider the following to be likely future focuses for criminals. In some cases, researchers have already demonstrated that they are vulnerable. Attackers are innovative. "Things are only impossible until the first person does it," says Beau Woods, a cybersafety innovation fellow with the Atlantic Council.

By Leigh Kamping-Carder and Kevin Hand

1 IMPLANTED DEVICES

Implanted medical devices, such as insulin pumps, pacemakers and cochlear implants, have been hacked repeatedly, but so far only by researchers, ethical hackers and fictional characters. The risk of criminals targeting these devices is expected to increase as more come equipped with internet connectivity.

The devices also pose a "potential unwitting insider threat to national security," according to research from Virginia Tech. Unlike smartphones or fitness trackers, these devices cannot be removed when members of the intelligence community enter secure facilities, offering a way for malicious actors to remotely gain access.

2 THE HOME OFFICE

The pandemic-related shift to remote work has created more opportunities for cyber attackers, as home offices are typically less secure than corporate workplaces. Even old-school phishing attacks, where a bad actor cons victims into opening malicious links or email attachments to steal data, are poised to become more serious, says Kevin Mitnick, chief hacking officer of KnowBe4, a Clearwater, Fla.-based security-awareness training company. Hackers could gain access to more information by targeting personal email accounts while people are using work computers, he says.

3 SMART-HOME DEVICES

Connected smart-home devices such as doorbells, locks, lights, ovens and coffee makers can be highly vulnerable to cyberattacks. Many lack basic security features, such as the ability to change the default password. Manufacturers, which mostly compete on speed-to-market and price, have little incentive to safeguard their products.

That is changing in some jurisdictions. In 2018, the U.K. passed a list of 13 best practices for smart-device manufacturers, service providers and mobile-app developers to create more secure products. As of Jan. 1, California also began requiring manufacturers of connected devices to include certain security features. Oregon has a similar law.

4 CARS

There doesn't appear to be evidence that criminals have hacked into individual cars yet, but it may happen in the future as internet connectivity becomes standard for vehicles. "Have I ever heard of this being used in the wild? No. Can it be done? Yes," Mr. Mitnick says. Hackers have also exploited weaknesses in dealership software, GPS tracking apps and car-alarm systems.

The fear is that cars could become a target for ransomware. Criminals would disable the car from afar and force people to pay a bitcoin or two to get it moving again, says Andrew Grotto, director of the program on geopolitics, technology and governance at Stanford University and a former senior director for cybersecurity policy in the Obama and Trump administrations.

5 CITIES

Cities are vulnerable as they connect more infrastructure to the internet. In August, Dutch security researchers from a company called Zolder revealed that they could remotely manipulate bike-traffic lights in 10 municipalities in the Netherlands by tricking the lights into sensing a steady stream of cyclists. The vulnerable systems have been taken offline, says Zolder co-founder Erik Remmelzwaal. Still, criminals could target traffic lights if such attacks prove remunerative. "As soon as bad guys figure out how to monetize this, they'll do it," says Mr. Grotto.

6 TRAINS

Trains are like "computers on rails," Mr. Grotto says. They communicate with each other and with stations, and often have their own Wi-Fi networks. "Positive train control" technology, which slows or stops trains to avoid accidents caused by human error, is a particular concern. A nation-state or terrorist group could target this system, causing a train to speed up around a curve instead of slowing down, says Richard A. Clarke, an author and former White House counterterrorism and cybersecurity chief.

7 AIRPLANES

Security researchers and hobbyists have demonstrated hacks on commercial-aviation systems, says the Atlantic Council's Mr. Woods. According to Mr. Clarke, there is no evidence that a commercial aircraft has been criminally hacked, but he says it is possible though difficult, requiring an understanding of the aviation industry. And an airplane's flight-control system isn't the only target. Systems managing ground-crew personnel, air-traffic control, airport kiosks, aircraft catering, baggage claim and plane-to-ground communication could all be attacked—all of which could prevent flights from taking off.

8 5G NETWORKS

Ultrafast 5G wireless networks could open the door to a new world of cyberattacks. First, 5G is expected to bring billions of new devices online, vastly expanding the number of targets for malicious actors, Mr. Grotto says. The distributed nature of 5G networks also provides fewer opportunities to implement cybersecurity measures. Instead of using hardware to manage network functions, 5G uses software, which has historically proven to be more vulnerable. Lastly, artificial intelligence and other automation will be used to oversee more of this complex infrastructure, opening up another avenue of attack.

9 SCHOOLS

Though malicious actors have immobilized schools' systems in the past, they typically didn't steal or expose sensitive information. Lately, they have begun to do both—a trend that experts say will continue as educators are beholden to online technology. Nevada's Clark County School District, which has about 320,000 students, disclosed an attack in August. Officials had refused a ransom demand in return for unlocking district computer servers. In response, hackers released records including employee Social Security numbers and student grades and addresses, the Journal has reported.

10 HOSPITALS

Ransomware attacks have compromised hospitals in the past few years. Experts say attacks could get more dangerous. In September, malware disrupted emergency care at Düsseldorf University Hospital in Germany, and a 78-year-old patient died after her ambulance was diverted to another facility—believed to be the first reported death related to a cyberattack against a hospital.

Attacks on hospitals to date have mostly focused on ransomware, essentially holding the hospital's data hostage by encrypting it, and then releasing it upon payment. In the coming years, attackers could take control of the hospital's online systems to manipulate machines (such as increasing the dosage on intravenous drips) and data (swapping blood types in patient records), Mr. Clarke says.

11 THE ENERGY GRID

The U.S. energy grid is vulnerable to cyberattacks that could destroy generators, transformers, and oil and gas pipelines. Hackers working for foreign governments, including Russia, have penetrated the U.S. grid, U.S. officials have said. So far, however, they haven't flipped any switches, Mr. Clarke says. Systems that use predictive maintenance—which monitors when equipment is degrading so it can be fixed before breaking—are another weakness. Such attacks would likely be part of an ongoing, broader conflict, Mr. Clarke says.

THE PROMISE AND PERIL OF VOTING BY PHONE

Limited experiments in mobile voting are taking place nationwide. Whether they prove secure for wider adoption is an open question. **By Paul Vigna**

Bradley Tusk made millions as an early investor in Uber. Now, he's devoting a chunk of that fortune to a cause he says goes to the heart of democracy: Mobile voting.

Filling out a ballot on a smartphone makes intuitive sense: We already work, bank and socialize through the glowing screens in our pockets. Many Americans can't or don't make it to the polls. Historically, only about half of U.S. citizens who are registered to vote actually do, though election watchers predict higher turnout in November. Staunch partisanship and the electoral college effectively mean that roughly a quarter of American voters determine who gets into the White House. Both trends could be magnified this year by a pandemic that has kept people at home.

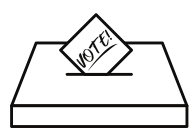
For Mr. Tusk, a better political system means increasing turnout and forcing politicians to respond to the will of the people.

"We have to give them different inputs and incentives if we want different outputs," he says.

Mr. Tusk has financed more than a dozen mobile-voting pilot programs through a nonprofit called Tusk Philanthropies. They and others expect that over the next five to 10 years, the generations that have grown up on their smartphones will demand services for voting as well. They are testing systems now that make use of mobile phones, the internet and blockchain technology, with the goal of having these systems in place in the coming years.

Convincing skeptical election officials won't be easy. There are already well-founded concerns about hacking existing election systems. Carting voting onto mobile devices and the internet opens the ballot box up to the myriad security vulnerabilities. Can phones be secured against malware and other threats? Can voters' identities be protected? Can hackers alter the vote count? Can the system be audited after the election?

Because of that, groups like the nonprofit Verified Voting Foundation, which is focused on modernizing the election system, have taken a hard line against internet-based voting.



More than 10,000

The number of election jurisdictions in the U.S.

At least 8

The number of jurisdictions that has experimented with mobile-voting systems

Roughly 1/2

The number of U.S. citizens registered to vote who actually do

Mobile Voting Experiments

Mobile voting already exists in controlled experiments. At least eight jurisdictions in the U.S. have experimented with mobile-voting systems, mainly for either overseas military personnel or for citizens with disabilities. Several dozen private organizations are dabbling with mobile voting. At least half a dozen countries have tried it as well.

The city of Denver used a mobile-voting system from a Boston startup called Voatz in its 2019 municipal elections. Colorado already allows every registered voter to vote by mail, but the city's director of elections, Jocelyn Bucaro, was looking for a better option to offer voters overseas or with disabilities.

In the May 7, 2019, municipal election, 156 eligible Denver voters in 36 different counties used the Voatz app, and 119 ballots were counted.

The voters returned both a signed affidavit and the ballot. Both are recorded digitally but can be printed out. One particular benefit, Ms. Bucaro says, was that the system separated the affidavit from the ballot in a way that prevented election judges from seeing who voted for whom, keeping the votes anonymous and providing a way to audit the system.

West Virginia started testing mobile voting in 2018, for military personnel overseas, and will use it again in next month's election. Mr. Tusk has also financed mobile-voting pilot tests in Delaware, Umatilla and Jackson counties in Oregon, King County in Washington, and Utah County in Utah. This year, New Jersey used mobile voting for residents with disabilities in its May elections.

Several companies, such as Voatz, Democracy Live and Votem, are trying to build and sell mobile-voting systems to the nation's more than 10,000 election jurisdictions. The essential elements are similar for them all: Users download an app, verify their identity initially with some combination of a driver's license, biometric scan, or PIN supplied by election officials, and then find their election and fill out a digital version of the physical ballot.

The complications are myriad, though. Voatz, for instance, relies on third parties for parts of its system. That opens up doors for malicious actors to force their way through, according to a group from the Massachusetts Institute of Technology's Internet Policy Research Initiative.

Some critics also worry that taking voting out of a physical location allows voters to be coerced. Somebody may be looking over the voter's shoulder, either influencing or outright buying a vote. Physical polling stations will likely endure to serve people who don't have smartphones or lack internet access.

Blockchain's Shortcomings

Blockchain was supposed to solve at least some online-voting issues. The basic idea of a blockchain is to create an open ledger in which a series of transactions are stored publicly for anybody to verify, while protecting the identity of the individual users. For voting, that ostensibly should result in a system where anybody could verify the validity of the election while individual voters' choices are kept private.

On a practical level, though, it may not work. The reason bitcoin, the original blockchain, works isn't necessarily the power of its cryptography, but a number of incentives and disincentives built into the program. Attacking the system is more expensive than participating in it and earning rewards in bitcoin. The entire transaction history is kept public, but it typically isn't worth somebody's time to try to piece together the identities of buyers and sellers.

For voting, these incentives work in reverse. Because there is no cost deterrent, there is no way to dissuade malicious actors from trying to take over the network. Because every vote is valuable, critics fear there is no good way to keep a user's identity and vote separate.

"The thing that intuitively seems like it might help in reality doesn't," says Michael Specter, a researcher at the Internet Policy Research Initiative, which published two reports on the Voatz app.

West Virginia, which had used Voatz in 2018, dropped it for its March primary and went with Democracy Live, which relies on a web-based rather than blockchain-based system. New Jersey used Democracy Live's system in its May primary.

Democracy Live's system revolves around a portal hosted on Amazon Web Services servers, where data is stored and secured. While AWS security has a track record, that hasn't satisfied critics, who still worry about the overall concept.

Mac Warner, West Virginia's secretary of state, says he didn't have security concerns with either Voatz or Democracy Live but wanted to try a different system.

Despite that setback, West Virginia officials were "incredibly helpful," Voatz founder and chief executive Nimit Sawhney says, and the company is planning to run more pilots, despite criticism from MIT and elsewhere.

"The criticism is to be expected," he says. "Our goal is to keep pushing the needle forward."

With mobile voting still in the pilot stage, the risk of swaying an election is minimal. Fewer than 1,000 people in total have voted from their phones in live elections on the Voatz app, Mr. Sawhney says.

It's clear even to proponents of mobile voting that no system is secure enough yet to be trusted for a general election. For it to take off, it's going to have to win the trust of officials, voters and candidates.

"The goal is to convince the loser that they lost," MIT's Mr. Specter says. "If you can't do that, it doesn't matter how much cryptography or research has gone into it."

Driverless-Car Security Specialist

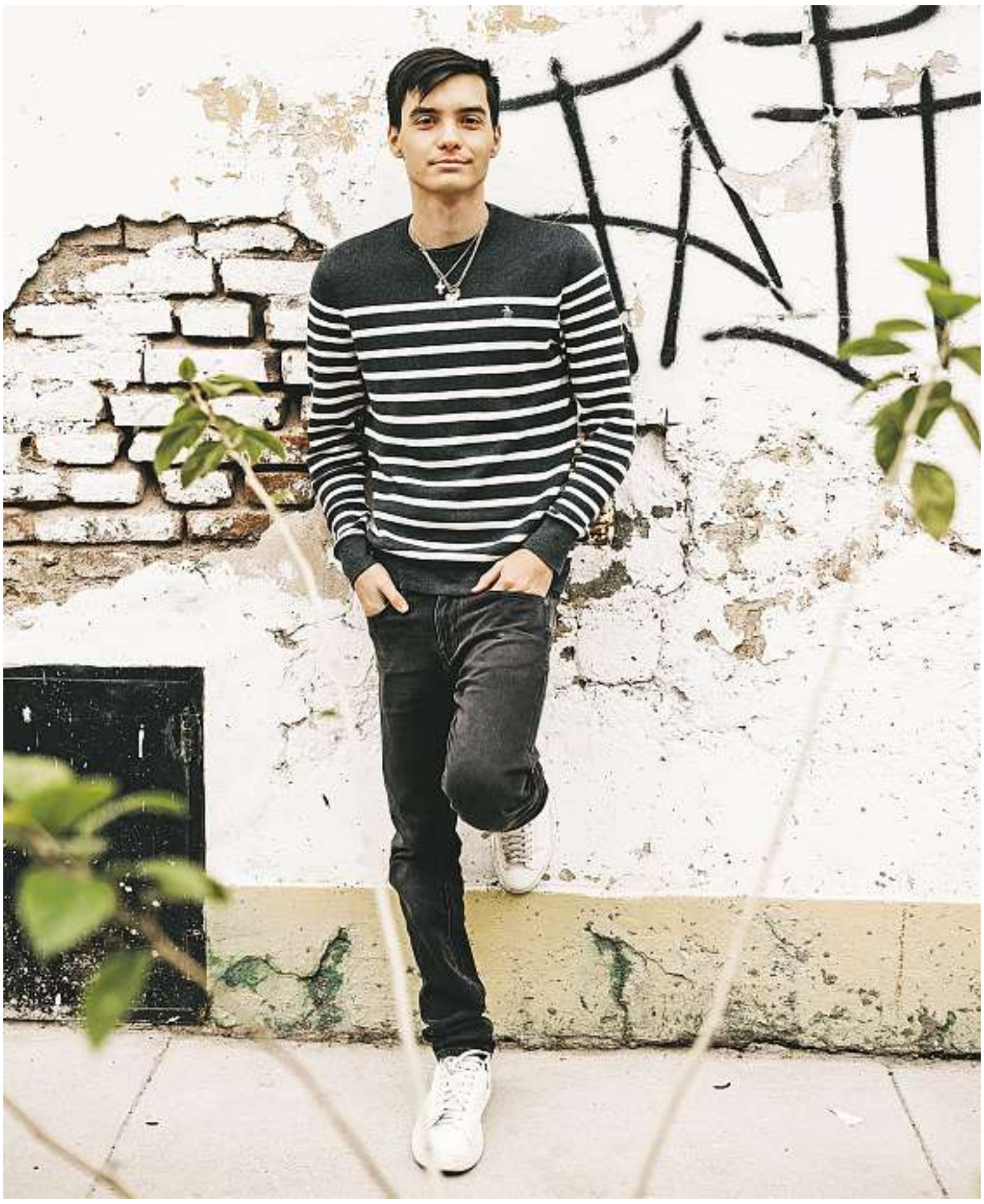
As your self-driving car makes its way through highway traffic at rush hour, it suddenly slows to a crawl in the middle lane. Hackers have just turned the engine off.

Auto makers will hire armies of driverless-car security specialists to avoid this terrifying scenario. These experts will help secure technologies specific to autonomous vehicles—such as lidar sensors, which procure a 3-D laser view of the environment—and will monitor fleets once they hit the road, treating software-related incidents in real time.

"We're dealing with all these new scenarios that simply do not exist in the IT world," says Dan Sahar, vice president of product at Upstream Security, a cloud-based cybersecurity platform for auto makers.

Driverless-car security specialists will be required to have inside-out knowledge of the auto-manufacturing supply chain—cars can be made of up to 30,000 different components—and be proficient at emerging technologies such as 5G, according to Andre Weimerskirch, vice president of cybersecurity and functional safety at auto-parts supplier Lear Corp. ▶▶

FROM TOPL BRIAN STAUFFER, JASON LEE; ISTOCKPHOTO (ICONS)



A HACKER'S LESSONS FOR CORPORATE AMERICA

Santiago Lopez uncovers weaknesses in company networks. Now 21, he expects to keep going for years to come. **By Kim S. Nash**

Santiago Lopez started invading corporate computer systems at age 16, after he learned to hack from YouTube videos and like-minded friends.

Now 21, he says he never wanted to commit crimes. Rather, he is a bounty hunter, invited by companies to find holes in their business networks and burrow into their vulnerable data. The idea is that a company will then fix what's wrong to harden itself against bad actors—"black-hat" hackers—looking to steal data, conduct espionage and disrupt business operations. Like others in a stable of "white-hat" attack experts associated with bug-bounty firm HackerOne, Mr. Lopez gets paid commensurate with the severity of the weaknesses he identifies. He and other members swarm applications and websites to look for security holes missed by customers that contract with the San Francisco-based firm. Big problems pay big money.

Mr. Lopez is good at his job: Last year, he reached $1 million in bounties since he started and is now closing in on $2 million in total, he says.

In a video chat from Buenos Aires, where Mr. Lopez has hunkered down with his family for the coronavirus pandemic, he talked with The Future of Everything about how corporate leaders can up their cybersecurity game.

Mr. Lopez, above, started hacking corporate computer systems at age 16. He has hunkered down in Buenos Aires with his family, right, during the coronavirus pandemic.

$1 Million

The amount that Mr. Lopez made last year in bug bounties, or rewards for finding holes in company cybersecurity shields

Nighttime must be the best time to hack U.S. companies because fewer security teams are awake.
A bit in the afternoon and evening, but preferably at night. I see hacking as a normal job, so I tend to hack between six and seven hours per day.

One large company gave you $10,000 for finding a way to manipulate one of its servers to access data it shouldn't have been able to. Was that challenging?
It took me a full day to close that bug and prepare my report. It wasn't long to identify the area [that was] vulnerable. It took much longer to see what kind of secret information I could access. That can be the most difficult task at times, being able to identify how much information you can access with that failure. And it is what gives the most reward.

Hacking has surged during the Covid-19 pandemic, as the Journal has reported. What effects will that have in the future?
Employees are online and information is more vulnerable. Hackers are trying to get those employees to click to load malicious software. Hackers are learning a lot, some new ways to get people's money. It's getting worse. I have not yet experienced any company where I have not been able to find a bug, no matter how minimal. Even if there is a company where you feel like you can't find a bug, it doesn't mean that someone else can't find it. Without a doubt, companies are struggling to protect themselves. Cybersecurity is advancing year after year, so even if they manage to create a new type of protection or evolve in some way, bad hackers will always be running the race and they will be discovering and preparing different new ways to make companies vulnerable.

You're really effective at what you do. What does this say about corporate cybersecurity?
They're not investing money or time or work in trying to grow their cybersecurity team. A lot of companies, if you report bugs to them, they don't have the expertise to fix them. Software that they build themselves has more bugs but software generally is vulnerable, always. If software has access to important data, then encrypt it.

How do different industries compare?
Banks and companies that are all digital are good. Universities don't care about security because maybe they don't have sensitivity to customers. Health care? They're not investing so much in cybersecurity, but they should. They have private information. Overall, cybersecurity teams need more money.

What kinds of technology changes are coming that will create cybersecurity problems?
Artificial intelligence has helped us a lot to optimize tasks, process data and make decisions much faster than a human being could. However, new technologies, including artificial intelligence, create big cybersecurity risks, as potential vulnerabilities are not fully understood when they are found. This means that with more organizations relying on machine learning to perform business-critical actions, AI systems are sure to become a major target for hackers.

Should companies be worried?
If an attacker had the opportunity to control an AI algorithm, it would be a huge problem since physical objects could be controlled for the first time. An AI attack can transform a stop sign into a green light in the eyes of an autonomous car. The data could also be controlled so that the way it is collected, stored and used can be changed. Imagine an AI attack could control the way that Google or Facebook collects your personal data and the hacker could save or manipulate the data as he pleased.

What about quantum computing, which experts say will be able to crack today's encryption?
That's way in the future. It's not easy to crack encryption code, so for now, that's a good guard against hackers. The larger problem is that people are not being cautioned about cybersecurity. Are all employees having training in cybersecurity? It doesn't seem like it. Employees, when they click on links, make a big hole for a hacker to enter. If you're not training people well, no matter what technology you have, you're only creating future problems. Customers aren't happy when their data is hacked. They will go to a competitor. Make the investment.

This interview has been condensed and edited.

FROM TOP: LUCIA VAZQUEZ FOR THE WALL STREET JOURNAL (2); ILLUSTRATION BY JASON LEE

Anti-Cheat Referee

Billions of online videogame players roam labyrinthine universes, slaying hordes of enemies and collecting in-game currency in environments that have become virtual economies.

Not everyone plays by the rules. Unscrupulous gamers have long exploited bugs and cheated to enrich themselves, trading fictional money against hard cash. "Those systems are abusable in quite a few games," says Kevin Johnson, the CEO of cyber consulting firm Secure Ideas.

As games become more evolved, developers will rely on advanced anti-cheat systems powered by artificial intelligence. But algorithms may generate false positives and miss sophisticated cheats.

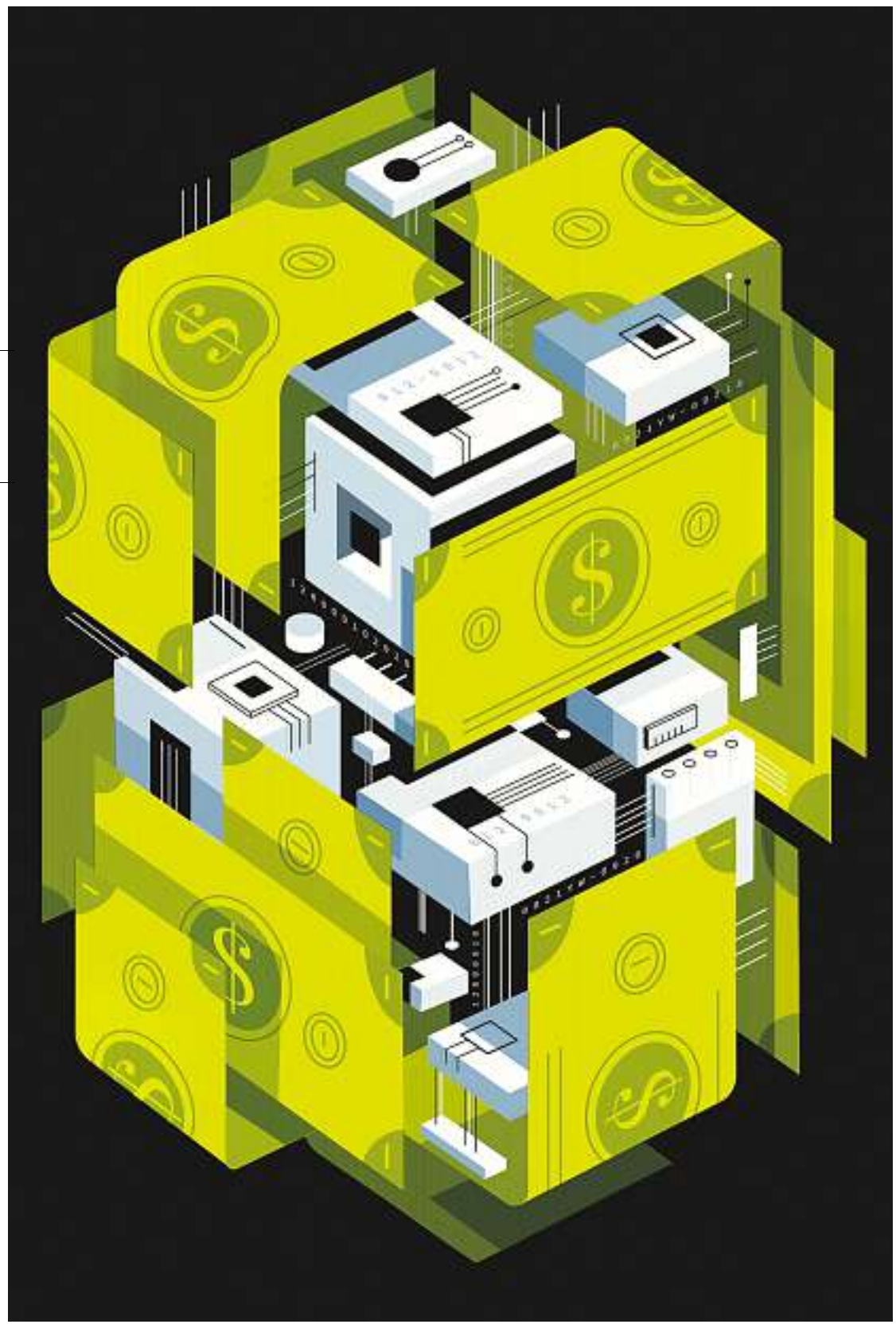
Anti-cheat referees will complement AI to track down suspicious behavior, thinking such as developers to identify flaws in the game. While the referees exist today in a limited capacity, their skill set will evolve to draw heavily on the basics of economics and psychology to identify abusers and ban players who cheat en masse, operating such as law enforcement planning a sting operation.

"Humans have to make the final call on whether a player is cheating or not," says Stijn Volckaert, an anti-cheat expert and assistant professor of computer science at KU Leuven university in Belgium. ▶▶

Where the Smart Money Is Headed

How businesses plan to budget for cybersecurity

By Mike Cherney



Companies face an uncertain future in fighting cyber threats to their systems, and it's going to cost them.

Cybersecurity spending, mostly by companies and governments, is forecast to grow about 9% a year from 2021 to 2024, when it is projected to hit $207 billion, according to one measure from research firm **Gartner** Inc., which updated its estimates in July. Though growth is projected at only 5% in 2020, reflecting disruption from the pandemic, the longer-term rate is high, considering that many companies have already invested heavily in cybersecurity and the market is saturated with security providers, says Ruggero Contu, senior research director at Gartner.

"The growth comes from the need to keep updating security to the newest requirements, given that the threats out there are constantly evolving," Mr. Contu says. Certain sectors, such as big banks, have traditionally invested more in cybersecurity, but companies in industries such as manufacturing are now trying to catch up, he says. The increasing reliance on cloud networks, the proliferation of internet-connected devices and new technologies such as artificial intelligence all pose thorny challenges.

Some companies are considering significant increases, which could mean millions of dollars more in spending at big firms. At Telstra Corp., Australia's biggest communications provider, Chief Executive Andrew Penn says the company could boost its cybersecurity spending by a double-digit percentage in the coming years. One new effort, which could be expanded, involves filtering out scam text messages that purport to be from government agencies before they reach Telstra's cellphone customers.

"It's an arms race between the malicious actors on the one hand, who've become increasingly sophisticated—and there's more of them—and the good guys, who are trying to build the capabilities and the defenses to keep them out," says Mr. Penn, noting that Telstra already employs more than 500 cybersecurity professionals.

Not all companies are planning a large increase. Before the new coronavirus spread, a survey of cybersecurity workers conducted late last year by Isaca, an association for IT professionals, found that 58% of respondents anticipated an increase in their organization's cybersecurity budget over the next 12 months. Now there is some evidence that spending may have been cut at some struggling companies, at least in the short term. In the Australian state of New South Wales, about 20% of cybersecurity workers were laid off, had their salary reduced or hours cut, while about 5% saw an increase in salary or paid work, according to a government-funded survey from the Australian Information Security Association.

"It's an arms race between the malicious actors...and the good guys." —Telstra CEO Andrew Penn

Looking ahead,.however, the shift to remote work has underscored the importance of allowing workers to easily access corporate networks from home. The fastest-growing segment, albeit from a low base, is expected to be cloud security, where spending is forecast to increase by more than 30% a year, according to Gartner.

The cloud can be difficult to secure because the tech companies that provide cloud-based services each configure their servers differently, and companies may need to use multiple vendors for different tasks, says Damien Manuel, chairman of the Australian security association and director of the Centre for Cyber Security Research and Innovation at Deakin University.

Many companies were cautiously moving to the cloud before the pandemic, but now they are learning they should move as much into the cloud as possible, says Kelly Bissell, senior managing director at Accenture Security, which provides cybersecurity services around the globe. "Which means they're going to have to think a little differently about security," he says.

Cloud security is one main focus for Seattle-area health insurer Premera Blue Cross, which agreed to pay about $90 million in legal settlements stemming from a large data breach that occurred in 2014. Adrian Mayers, vice president and chief information security officer, who joined after the data breach, says the company recently invested in what's known as adaptive multifactor authentication to ensure that only authorized users log onto its network.

Such a system asks the user for additional information if it detects anything unusual about a sign on, and will analyze variables such as the location, the time of day and the device, Mr. Mayers says.

"The ability to ramp up—what I like to call turn up the volume—gives us a lot of flexibility," says Mr. Mayers. "We have elements of that capability, but we have invested over the last 60 days in the new capability to take that even farther."

Other companies plan to continue modeling their cybersecurity strategy on so-called zero-trust principles, which is the idea that every user and device must be rigorously authenticated each time they log on. That is particularly important for a company such as Becton Dickinson & Co., which makes some medical devices that transmit data through the cloud.

"To use the analogy of protecting your home, it's like locking your front door, but zero-trust means you're guarding your valuables as if the thief has already broken into the house," says Rob Suarez, vice president and chief information security officer at BD.

Cybersecurity chiefs are also focused on navigating the increasingly blurred lines between the digital and physical worlds, often called the Internet of Things. Each connected device is a potential entry point for a would-be hacker, and many lack sufficient security.

New Jersey-based Covanta runs about 40 power plants world-wide that burn trash to generate electricity. One long-term goal is to further develop its use of network-connected devices to gather data so its power plants can operate more autonomously and be monitored remotely.

For Tammy Klotz, the company's chief information security officer, one key consideration is making sure that any devices inside the power plants are separated from the company's back-office network. That way, if an office worker does fall for a phishing email and the office network is compromised, the power-plant operations won't be affected.

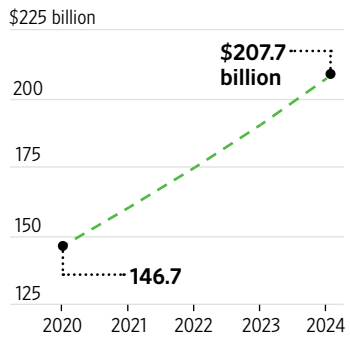
Looking further ahead, Mr. Manuel says companies will also have to protect AI systems from unique threats. One potential danger, Mr. Manuel says, is that a hacker could begin feeding erroneous data to an AI that then creates undesired outcomes. A company's online customer-service chatbot, for example, could be trained to recommend a competitor's products.

But there could be more dire results.

"Imagine you have AI systems used in health care where they can look at X-rays, and they could diagnose tumors," Mr. Manuel says. "Those systems could be manipulated to make mistakes or errors which could then be catastrophic."

Investing in Security

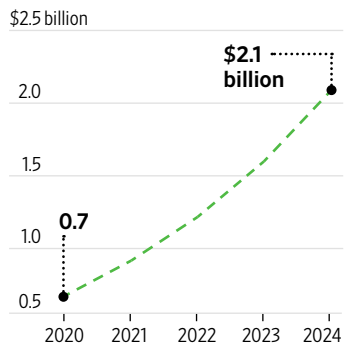
Annual cybersecurity spending by companies and governments world-wide is projected to grow to $207 billion in 2024.



Source: Gartner

Making It Rain

Cloud security is expected to be the fastest-growing segment of projected cybersecurity spending world-wide.



Source: Gartner

Implanted-Device Guardian

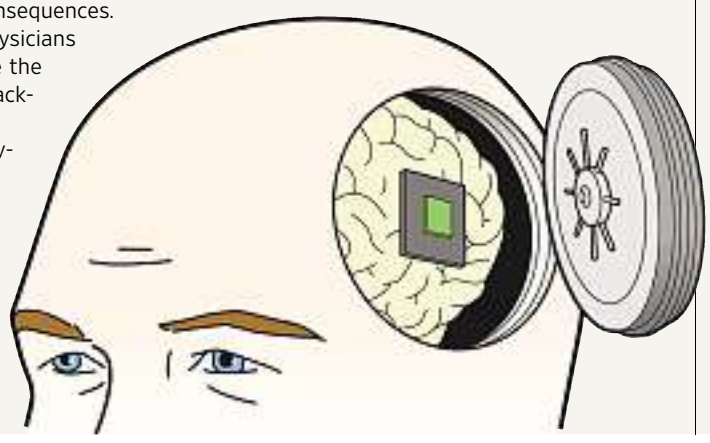
Years from now, when your doctor prescribes a brain-enhancement implant, a cyber analyst will look into the security risks that come with it.

In the future, hackers could use implanted devices such as a memory-boosting brain chip, as a recording device and eavesdrop on sensitive conversations or drain its battery by sending a tsunami of signals from a fake base station, with potentially serious consequences.

"The physicians won't have the relevant background to evaluate cybersecurity risks," says Marie Elisabeth Gaup Moe, a senior security consultant at the Norway-based cyber consulting firm mnemonic, who identified security flaws in her own pacemaker.

Implanted-device guardians will have some medical background and know about the latest cyber threats and malwares. Just such as we consult physicians for routine checkups, we might visit our guardians several times a year to assess our implants' vulnerabilities through tailored body scans, Ms. Moe says.

These technicians will also suggest or recommend against software updates after having conducted a cost-benefit analysis.



Chief Digital Identity Officer

Every time an employee, contractor or third-party logs in to a company-linked platform, it creates an entry point into the organization's network and an opportunity for bad actors to steal information.

In the future, a chief digital identity officer will join the C-suite with a single focus: To make sure users accessing the firm's platforms are who they say they are. They will promote the latest verification technologies—unlocking your smartphone by pressing your ear across the screen, for example—to employees, suppliers and contractors.

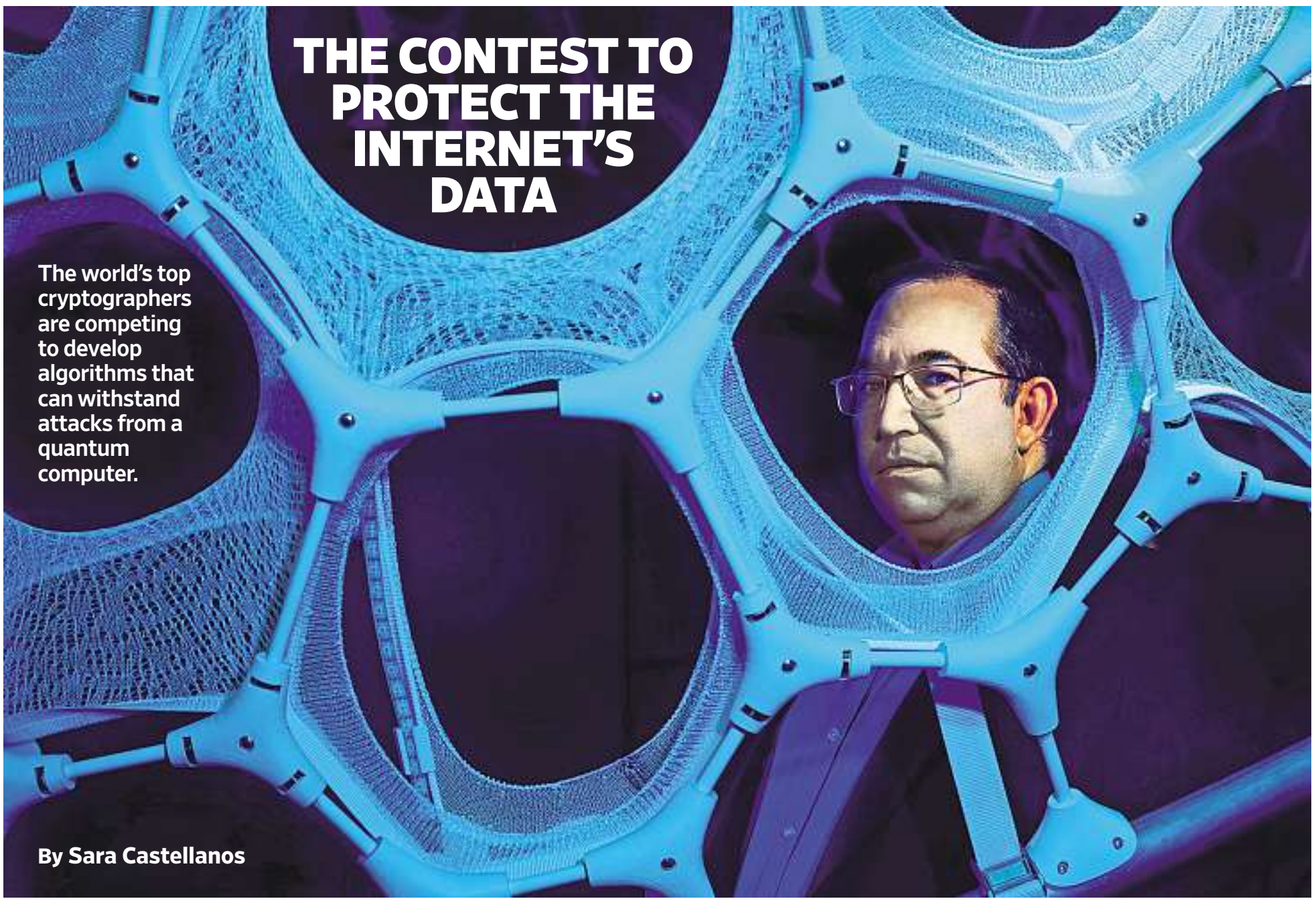
While some of these responsibilities currently fall to chief information security officers, pandemic-inspired remote-work policies will reshape how employees access their workplaces and push the need for strong authentication.

This will require a "spiritual leader" in the company, says Ann Johnson, corporate vice president of business development, security, compliance and identity at Microsoft Corp. "That might not even be the most technical person, but the person that's making sure we have adherence to the policies and standards that are set by the more technical folks."

FROM TOP: HARRY CAMPBELL; JASON LEE (2)

THE CONTEST TO PROTECT THE INTERNET'S DATA

The world's top cryptographers are competing to develop algorithms that can withstand attacks from a quantum computer.



By Sara Castellanos

Cryptographers are in the business of being paranoid, but their fears over quantum computers might be justified. Within the next 10 to 15 years, a quantum computer could solve some problems many millions of times faster than a classical computer and, one day, crack many of the defenses used to secure the internet.

"The worst-case scenario is quite bad," says Chris Peikert, associate professor of computer science and engineering at the University of Michigan, who has been studying cryptography for two decades.

That is why Dr. Peikert and hundreds of the world's top cryptographers are involved in a competition to develop new encryption standards for the U.S., which would guard against both classical and quantum-computing cyberattacks.

This summer, federal officials announced the 15 algorithms that will be considered for standardization, meaning the winners would become a part of the architecture of the internet, protecting people's sensitive data.

Next, researchers will spend about a year trying to break them to see which ones hold up, and test them to get the best balance of performance and security.

Quantum computers are still in the early stages of development. The machines harness the properties of quantum physics, including superposition and entanglement, to radically speed up complex calculations related to finance, health care and manufacturing that are intractable for today's computers. These machines are being built by startups and technology companies such as International Business Machines Corp. and Alphabet Inc.'s Google. They are still several years away from being fully commercialized.

While traditional computers store information as either zeros or ones, quantum computers use quantum bits, or qubits, which represent and store information as both zeros and ones simultaneously.

Some researchers estimate that it would take a machine with 250 million qubits to break today's public-key cryptography. Today's early-stage quantum computers have a tiny fraction of that power.

The initiative is being managed by the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce. NIST has asked entrants to design encryption algorithms that they think could withstand a cyberattack from a quantum computer. The competition began in 2017 with about 70 algorithms.

The 15 remaining algorithms include seven methods that could be standardized by 2023, and eight alternates, which would take more time to study but still show promise.

"We can't prove that they won't ever be broken, but that's the case with all cryptography," says Dustin Moody, a mathematician at NIST who is leading the post-quantum cryptography competition.

Microsoft's Brian LaMacchia, above, is part of a competition to develop new encryption standards. He worked on an algorithm called FrodoKEM, a nod to 'The Lord of the Rings' character Frodo Baggins.

The goal of the competition is to replace today's commonly used public-key cryptography methods, including a popular one called RSA that would be particularly at risk if and when a powerful quantum computer comes to market. Named after its developers Ron Rivest, Adi Shamir and Leonard Adleman, RSA is used to secure things such as email, online banking, e-commerce and electronic communications such as those in the health-care industry.

RSA is vulnerable to quantum computers because it is based on integer factorization, which is essentially reverse multiplication, using numbers that can be about 1,000 digits long.

It is not possible for regular computers, even supercomputers, to quickly factor numbers that are that long. Quantum computers, though, are capable of solving integer factorization problems perhaps many millions of times faster than a classical computer.

If bad actors ever got their hands on a powerful enough quantum computer, they could break into anything encrypted with RSA, representing a huge swath of the internet. The threat is real even now, cryptographers say, because hackers could be collecting massive amounts of data, waiting to attack when a quantum computer comes into existence, a practice known as "harvest and decrypt."

"We got very unlucky that the one thing that quantum computers can have this exponential speedup for is exactly what we based our cryptography on in the 1980s," says Vadim Lyubashevsky, a cryptographer at IBM Research Europe, a security department of IBM. Dr. Lyubashevsky is a co-author on three of the finalist submissions.

Several of the most promising

'We got very unlucky,' says Vadim Lyubashevsky of IBM Research Europe, above. One of today's encryption methods is vulnerable to the ultrafast speeds of quantum computers.

cryptographic systems in the NIST competition are based on so-called mathematical lattices, which can resemble geometric shapes that can have more than 1,000 dimensions.

Researchers to date haven't found an algorithm that can solve, and therefore break, an encryption method based on a secure lattice, either on a classical or quantum computer. It would be surprising if someone did: Lattices have been studied in cryptography for about 25 years, says Rachel Player, a lecturer in information security at Royal Holloway, University of London.

Still, Dr. Player and other cryptographers will spend the next year or so trying to come up with algorithms that attack and test the remaining submissions, including those based on lattices. "It would be really cool to discover this algorithm, but then you spent so long working to build this, it would be a shame to break it," says Dr. Player, who was involved in a lattice-based submission that didn't make it to the finals.

Two of the finalist algorithms are named Crystals Dilithium and Crystals Kyber. Crystals is short for Cryptographic Suite for Algebraic Lattices. Crystals Kyber is used to securely share keys, and Crystals Dilithium is used for authentication. Fans may recognize the names from "Star Wars" (lightsabers are made from kyber crystals) and "Star Trek" (dilithium crystals are used in the warp drive).

"We have some fun with it," says Brian LaMacchia, a distinguished engineer at Microsoft Corp., who leads the Microsoft Research security and cryptography team.

Dr. LaMacchia is a co-author on two of NIST's alternates, including one called FrodoKEM. The name is a nod to Frodo Baggins in J. R. R. Tolkien's "The Lord of the Rings." The cryptographic scheme is based on prior work that used a lattice that included an algebraic ring, Dr. LaMacchia says. Researchers decided to ditch the ring to strengthen the security of the algorithm, and they made another modification in adding a key encapsulation model, or KEM.

Other organizations around the world, such as the European Telecommunications Standards Institute, are researching algorithms that are resistant to quantum computing attacks and are providing industry guidance.

So are private companies, particularly in financial services, including Visa Inc. and JPMorgan Chase & Co. Research in the area of post-quantum cryptography began nearly six years ago, says Rajat Taneja, president of technology at Visa. "The data we have is sensitive, and it is vast in quantity, so protecting that data is job number one for us," he says.

Visa and JPMorgan plan to begin adopting NIST's new standards when they become available, which will require coordination with industry organizations. It can take as long as 15 years for internet activity to be secured by the new encryption methods, experts say.

The NIST challenge is unique because it is mostly theoretical. These experts are trying to design cryptographic systems that will be secure against quantum computers, which they don't know how to build and can only assume will exist, Dr. Peikert says.

For many cryptographers, coming up with new encryption standards by 2023 will represent the culmination of 10 or 15 years of work in the area known as post-quantum cryptography.

"I see standardization as a bittersweet moment," says Dr. Peikert, who was also a co-author on the FrodoKEM submission. "It means we're effectively done with something. It's over. And for researchers like me, who work more on the theoretical side, we're much more excited by what's going to be great 15 years from now."

FROM TOP: QUINN RUSSELL BROWN FOR THE WALL STREET JOURNAL; MATHIAS BRASCHLER & MONIKA FISCHER FOR THE WALL STREET JOURNAL

CYBERWAR OR CYBER PEACE?

Former White House cybersecurity chief Richard A. Clarke outlines two visions of 2030.

The Fates, it sometimes seems, prefer extreme outcomes. While humans usually reject predictions of futures dramatically changed from the present, information technology has produced a never-ending stream of upheavals in the economy, warfare, our very way of life. Thus, cyberspace in 2030 could be a very different place than it is today, for good or ill. How we deploy artificial intelligence and machine learning to attack and to defend networks will make the difference.

Today cyberspace is a hostile environment. Most corporations and governments have security operations centers that look like hospital emergency rooms doing triage, as they are hit by thousands of automated and human-directed attacks every day. To deal with this problem, Silicon Valley startups have created yet more software to prioritize security incidents and automate operational responses. Even with the added software, however, humans cannot always act with the speed and discernment necessary to respond to attacks and remediate vulnerabilities.

One reason humans cannot react quickly enough is that they are already competing against attackers which aren't human, but rather machine-learning algorithms that have incorporated all of the tricks known to hackers and deploy those techniques at machine speed. Think of it as cyber AI that goes on the offensive. After observing network features from the outside, offensive bots make educated guesses about a network's vulnerabilities, persistently try every attack technique until they penetrate the perimeter defenses, and then drop a payload. The payload, lines of self-executing code, defeats internal protections, finds the targeted information, and extracts it. Or, rather than merely stealing data, the algorithm may be designed to eat data, encrypt data in a ransom scheme or cause machines to malfunction or self-destruct.

The Potential of AI

Despite science fiction fears of Skynet and the Borg, AI has the potential to make cyberspace safer for humans. Machine learning holds out the theoretical possibility of humans yielding control of network security management, indeed all network operations, to adaptive algorithms. Thus far, however, machine-learning techniques and narrow AI systems have only been incorporated into anomalous activity detection, fraud prevention, and identity and access management tools. The master AI to "rule them all" hasn't been a project any venture-capital firm nor government grant-giver has been willing to fund.

The biggest barrier has been human distrust. Executives often incorrectly intuit that having humans in the loop will raise the probability of successful defense, even though humans cannot keep up with an automated attack program. No enterprise has been willing to volunteer its operational network as a classroom for machine learning to educate itself on how to make the decisions necessary to protect the organization in real-time at machine speed.

Given the increased advantage that the offense now gets from AI, someday soon someone may feel compelled to let go of the reins, and will develop a master AI for defense. By 2030 such a network-defense and network-control master algorithm might greatly reduce cyber risks. Cyber peace might break out.

Alternatively, by 2030 we may have had our first cyberwar, a hyper-speed conflict involving widespread nation-state attacks on each other's critical infrastructure, including telecommunications, pipelines, financial systems, and electric-power generation and transmission networks. Although this concept was first introduced to most people in movie thrillers like "Live Free or Die Hard" (2007), weaponized software exists and is in the hands of military cyber commands and intelligence units in more than a score of nations, including the U.S.

An Entryway for Broader Conflict

The belief that cyber conflict is antiseptic and creates few casualties may result in leaders around the world being more willing to go to cyberwar than kinetic conflict. Unfortunately, the physical, financial and military damage done by a cyberattack could be so great that it would force the hand of leaders to respond with conventional weapons. Thus, cyberwar may be the entryway for broader conflict.

Some nations have already loaded their cyber weapons. Senior intelligence officials believe that foreign adversaries including Russia and China have secured hidden footholds in the U.S. electric grid and could use that access to cause blackouts in the future.

Moreover, new Congressional authorities backed by presidential directives have given both the Pentagon's Cyber Command and the CIA the authority to lace potential adversaries' networks with a destructive program that can be activated in the event of war. While a strong case can be made for such preparation, many nations existing in this perpetual state of high readiness creates crisis instability and incentives to go first.

If there were to be a full-scale cyberwar, we could expect that many parts of the U.S. would be without networked electric power for months. Swaths of the country would rely on a few small backup generators at hospitals. Stricken regions would descend into chaos as the thin veneer of civilization rapidly deteriorated.

Will either of these outcomes occur? The Fates, it sometimes seems, prefer extreme outcomes.

Richard A. Clarke is the co-author of "The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats," and a former White House counterterrorism and cybersecurity chief.

ILLUSTRATION BY HARRY CAMPBELL