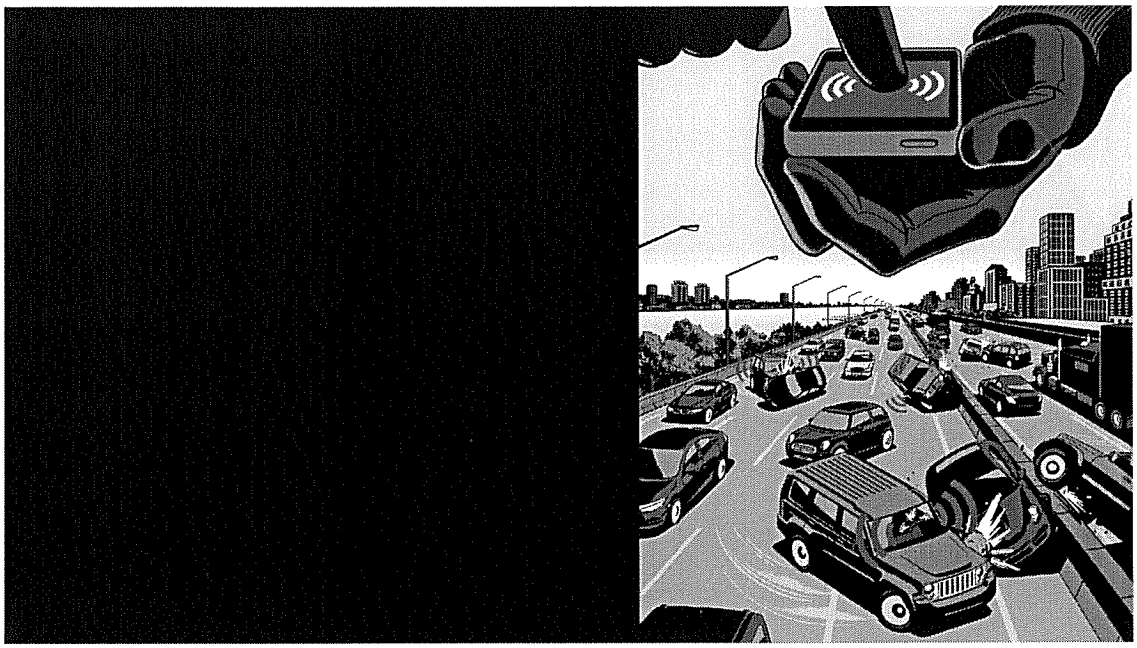
The Big Hack

The day cars drove themselves into walls and the hospitals froze A scenario that could happen based on what already has.

Illustrations by R. Kikuo Johnson



On December 4, 2017, at a little before nine in the morning, an executive at Goldman Sachs was swiping through the day's market report in the backseat of a hired SUV heading south on the West Side Highway when his car suddenly swerved to the left, throwing him against the window and pinning a sedan and its driver against the concrete median. A taxi ran into the SUV's rear fender and spun into the next lane, forcing a school-bus driver to slam on his brakes. Within minutes, nothing was moving from the *Intrepid* to the Whitney. When the Goldman exec came to, his driver swore that the crash hadn't been his fault: The car had done it.1

Moments later, on the George Washington Bridge, an SUV veered in front of an 18-wheeler, causing it to jackknife across all four lanes and block traffic heading into the city. The crashes were not a coincidence. Within minutes, there were pileups on 51st Street, the southbound BQE, as far north as the Merritt Parkway, and inside the Midtown Tunnel. By nine, Canal Street was paralyzed, as was the corner of 23rd and Broadway, and every tentacle of what used to be called the Triborough Bridge. At the center of each accident was an SUV of the same make and model, but as the calls came in to the city's 911 centers in the Bronx and Brooklyn, the operators simply chalked them up to Monday-morning road rage. No one had yet realized that New York City had just been hit by a cyberattack — or that, with the city's water system, mass transportation, banks, emergency services, and pretty much everything else now wired together in the name of technological progress, the worst was yet to come.2

the_real_hacks

The fictional account imagined here is based on dozens of conversations with cybersecurity experts, hackers, government officials, and more. An attack of such scope is unlikely, but each component is inspired by events that can, and in most cases have, happened.

1In 2015, carmakers began paying greater attention to the fact that some new vehicles, now connected to the internet, had become as hackable as laptops. In March, researchers found hackers were able to access the ignition on Audi, BMW, Ford, Honda, Hyundai, Kia, Lexus, Mazda, Mitsubishi, Nissan, Range Rover, Subaru, Toyota, and Volkswagen cars.

2Homeland Security recently estimated that one major cyberattack — the NSA chief has said it's a matter of "when, not if" — could cost $50 billion and cause 2,500 fatalities.

A third-year resident in the emergency room at Columbia University Medical Center in Washington Heights walked through the hospital as a television was airing images from the accident on the George Washington Bridge; that meant several crash victims would soon be heading her way. When she got to her computer, she tried logging into the network to check on the patients who were already there, but she was greeted with an error message that read WE'RE NOT LOOKING FOR BITCOIN THIS TIME.

Columbia, like major institutions across the country, had spent the past few years fighting so-called ransomware attacks, in which hackers locked a hospital or city hall or police department out of its own network until a ransom was paid.3 Hospital security teams had gotten wise to the problem, but every network's defenses had the same vulnerability: the people who used it.4 For weeks, a group of hackers had been sending LinkedIn messages to employees at Columbia pretending to be recruiters from Mount Sinai. When an employee opened an attachment featuring the recruiting pitch — as ten of them did — and enabled the macros as prompted onscreen — four of them did — they unknowingly unleashed malware onto their computer and gave the hackers a beachhead. After months of lurking5, the hackers blocked Columbia's doctors and nurses from accessing their network, including patient files. Doctors couldn't access prescription records telling them which patients were scheduled to take which drugs when and resorted to improvised paper-record keeping6, which many of the younger doctors had never done before. In nearly every corridor, they were consulting with one another in a panic, asking how much of their own expertise was really stored in the cloud and had just disappeared.

3In February, a hospital in L.A. paid 40 bitcoins, or about $17,000, to get back into its system. Russian hackers have even set up English-language call centers to explain to victims how to acquire and send bitcoins.

4Hackers recently sent Pennsylvania drivers fake traffic tickets with malware, using GPS data so the tickets seemed to be from red-light cameras on their route home.

5The average data breach is only identified five months later; hackers were allegedly inside a Ukrainian utility network for six months before shutting off electricity.

6In March, a D.C.-area hospital system was hacked and forced to keep paper records. They got so overwhelmed they turned away cancer patients with radiation appointments.

The crowd in the waiting room swelled and grew more tense as nurses ran by patients, unable to give updates on when they might be seen. Various procedures were taking longer than they should have — one man was kept on a powerful antibiotic for several hours, with serious side effects, before a delayed lab result came back reporting that he should go off the medication — and the staff was having trouble keeping track of patients. A little before noon, a man walked into the hospital looking for his wife, whom he had dropped off early that morning for a simple surgical procedure. A few minutes later, the nurse told him that it appeared his wife had been discharged.

Most New Yorkers were proceeding with their day unaware. But the city's head of cybersecurity7 had begun to connect the dots: Six hospitals had already informed him that their systems had been shut down, and the city had sent out warnings to all the others. One Police Plaza had just reported that it, too, was locked out of the programs it used to dispatch officers and emergency personnel8, which made responding to the traffic accidents around the city that much harder.

7New York's first head of cybersecurity started the job earlier this year.

8In April, Newark's police were locked out of their computer system for three days.

After a few phone calls to friends in the private sector, the cybersecurity chief got more nervous. At the beginning of 2017, one friend told him, she had been called to investigate a mysterious occurrence at a water-treatment plant: The valves that controlled the amount of chlorine released into the water had been opening and closing with unexplained irregularity9. An alarm had gone off, so none of the tainted water had reached consumers, and the company's CEO brushed off the consultant's request to make the news public so others could prepare for similar attacks.

9Investigators recently reported a similar incident at an undisclosed water company.

At MetroTech, New York's cybersecurity chief pulled out the Office of Emergency Management's 42-page booklet on how the city should react to a cyberattack — a copy of which he had printed out and stashed in his desk drawer in case his department's own network was compromised — and was flipping from page to page when he got a call from a reporter.

At 12:30 p.m., the *Times* published a story reporting that "government officials" believed that the city was being hit with a wave of cyberattacks that appeared to be ongoing. A tipster claimed the hackers had caused at least a dozen car crashes and debilitated multiple hospitals and agencies — with more to come. If they could crash a car, could they crash a subway? The *Times* report included a line from a nurse at New York–Presbyterian who said that the initial message announcing that the network was blocked had included a link to a web page that was displaying a timer ticking down to 1 p.m. and text that read MORE PATIENTS WILL BE ARRIVING SOON.

The group of10 European black-hat hackers11 who launched the attack against New York had spent much of the previous decade breaking into American corporate networks — credit-card companies, hospitals, big-box retailers — mostly for profit,12 and sometimes just because they could. When those attacks became routine, the group moved into more politically inclined hacks, both against13 and on behalf14 of various governments, rigging elections15 and fomenting dissent. In the summer of 2016, the hackers received an anonymous offer of $100 million to perform a cyberattack that would debilitate a major American city. The group's members weren't much interested in death and destruction per se, so they declined their funder's request for a "Cyber 9/11."16 But to self-identified anarchists with a reflexively nihilistic will to power, the proposition had some appeal. Causing disruption was something that had been on their minds recently, as their conversations veered toward the problems with global capitalism, the rise of technocentrism, bitcoin, and the hubris required to nominate a man like Donald Trump. Their animus got more personal when American authorities arrested a well-respected white-hat hacker who had broken into an insulin pump in order to show the dangers of connecting devices17 without proper security. The black hats were on the opposite end of the ideological spectrum but had more empathy for their fellow hacker than they did for the American people, who, they felt, deserved a comeuppance — or at least a very loud "Fuck you." The plan was to show how much of modern life in a city like New York could be disrupted by purely digital means. The hackers would get paid, but they also hoped their attack

would dent America's complacent faith in order and in the technology and political authority that undergirded it. As a bonus, their services would be in even greater demand.

10Hackers are often identified by the malware they use: One group is known as Sandworm, because references to the sci-fi series 'Dune,' which features giant desert worms, were embedded in its code.

11The hacker world divides into white hats, who are the good guys, and black hats, who are out to cause havoc or for personal gain.

12According to the FBI, those hit by cyberattacks have paid more than $200 million in ransoms so far this year, compared with just $25 million in all of 2015.

13Earlier this year, Congress was the target of a string of ransomware attacks.

14An Italian company called Hacking Team has been criticized for offering hacking services to dozens of countries, many with poor human-rights records.

15Andrés Sepúlveda, a Colombian hacker, recently told Bloomberg that he had helped rig elections in nine different Latin American countries, including by installing malware on campaign routers to spy on digital and phone communications.

16Last year, a researcher claimed he had hacked into a plane's seat-back entertainment system and could then access the cockpit controls on a Boeing jet flying from Denver to Chicago. Boeing has said this is impossible.

17In 2014, a company tracking medical devices at more than 60 hospitals found malware in every hospital. Last year, another researcher was able to manipulate several drug-infusion pumps so he could, potentially, deliver a fatal dosage of medication.

No one had pulled off an attack of this magnitude, but it was possible to piece together a plan from various hacks that had been executed before, which, taken together, were a sort of open-source blueprint available to anyone with an interest in remote-control terrorism (and the time and manpower it required). This group was small, relatively speaking, and benign, relatively speaking. ISIS, for instance, might have a more pronounced bloodlust but not (yet) the technical capabilities; Chinese or Russian hacking operations would have many more resources and a much more sophisticated strategy that could bring even more targets, like nuclear-power plants,18 into play.

18It took several years for hackers allegedly working for the U.S. and Israel to develop Stuxnet, a computer worm that disabled an Iranian nuclear reactor in 2010.

These hackers decided to start with cars. The team's members found a particular automaker's flagship SUV especially hackable,19 bought one to test their work (to help fund the operation, they had pulled from the millions they had made in several attacks against financial institutions, including a recent hack of the Central Bank of Bolivia20), and, within a month, could shut off the ignition, turn off the brakes, and cause the steering wheel to jerk to the left.

19In 2015, for an article in *Wired*, two hackers in St. Louis took control of a Jeep traveling 75 mph, sprayed wiper fluid so the driver couldn't see, then cut the transmission.

20In February, hackers stole the credentials of several employees in the Bangladeshi Central Bank using malware that tracked keystrokes as the employees entered passwords and were then able to transfer $81 million into private accounts. (They might have stolen more had they not misspelled the word "foundation" in one of the transfers, triggering an alarm.) The underlying system of financial

transactions, known as SWIFT, has since come under scrutiny after similar attempted attacks at other banks.

h

If you don't think the threat of hacking is real, take a look at these eight examples of real, terrifying hacks that have happened right under our noses.

Several other members of the team spent months trawling Shodan, a free search engine, launched in 2009, that allows savvy users to find devices with unprotected connections to the internet, from wind turbines to thermostats21 to Wi-Fi-enabled baby monitors. As they looked for ways to demonstrate vulnerability — to show just how many mundane features of urban life had been opened up to hackers in recent years — they found themselves focusing on something most New Yorkers use every day. The vast majority of the 70,000 elevators in New York City are not connected to the internet, but building managers had begun taking elevator manufacturers up on their offers to install remote-control systems as a way to cut costs. And so, an hour after the SUVs started crashing, a resident who had recently moved into a new tower in Hudson Yards was riding up to her 22nd-floor apartment when her elevator suddenly jerked to a halt. Across town, a bank of elevators in a Downtown Brooklyn office building that had installed the same software stopped working, with several members of a new-media start-up onboard one car. It didn't take long for them to begin sharing their lighthearted grievances on social media. One of them pointed out a remarkable coincidence on Facebook: His friend in a different building had gotten stuck in an elevator too.

21In 2014, an Ohio man remotely accessed the thermostat in the home of his ex-wife, who'd left him for another man. "Since this past Ohio winter has been so cold I've been messing with the temp while the new love birds are sleeping," the man wrote in a review of the thermostat on Amazon. "Doesn't everyone want to wake up at 7 a.m. to a 40-degree house?" He gave it five stars.

By now, officials at U.S. Cyber Command were monitoring the situation in New York. Both the Department of Homeland Security and FEMA had conducted practice operations to see how they would respond to a cyberattack, but this was the first time anyone in the government had been called to respond to a major incident, and it wasn't entirely clear who was in charge.22 American intelligence had long suspected that this particular group of Europeans might have more-than-indirect ties to the Russian government, but Putin wasn't saying so, and the Russians quickly denied any involvement, as did the Chinese,23 the Iranians,24 and the North Koreans.25 If they were all to be believed, there were just a few hacker groups with both the expertise and the resources to pull off a multipronged cyberattack, and this one was near the top of that list. But there was only so much the government could do. The group's members worked separately, and the Defense Department had only the vaguest sense of where they might be. Dropping bombs wasn't an option.26

22In April, the Government Accountability Office reported that the Pentagon lacked a defined "cyber incident" chain of command.

23Chinese hackers are suspected in many attacks, such as the 2015 Office of Personnel Management breach, which disclosed the personal information of 21.5 million people.

24In 2013, seven Iranians allegedly got enough control over a Westchester dam to potentially open the sluice gate.

25North Koreans have been blamed for both the 2014 Sony hack and an attack on a South Korean nuclear-energy company in 2015.

26The U.S. has killed two ISIS hackers in airstrikes. One of them allegedly gave up his location by clicking a link he shouldn't have.



Their networks dark, hospitals fell into chaos. *Illustration: R. Kikuo Johnson*

By the time the FDNY rescued the woman in Hudson Yards from her stalled elevator, and she had walked up seven flights of stairs to her apartment, grabbed a beer, and turned on the television, she found CNN airing footage of Wolf Blitzer stalking around the network's midtown newsroom as befuddled members of the IT department, which didn't have any better ideas, began unplugging every nonessential device they could. Companies started urging their employees to take the stairs, while many simply sent employees home. The mayor decided to continue running the subways, but at a delay to stagger trains and prevent accidents. Some people didn't feel like risking it and trudged home through the snow instead. No one wanted to drive, and Uber, which had a number of drivers who used the targeted model of SUV, added a warning to its app that it couldn't guarantee rider safety. (Still, demand drove surge pricing up to its maximum of 2.8 times the normal fare.) The security consultant who'd found the mess with the water-treatment plant went on TV to tell people that it appeared cyberterrorists had tried to hack the water supply. False reports of attacks on the stock exchange27 and Amtrak and a gas pipeline28 and a factory29 shot around Reddit and Twitter, until nobody wanted to do much of anything but get home, unplug their wireless router, and hope for the best. "With cyberattacks confirmed against cars and several hospitals, it's impossible to say what might happen next — " Blitzer said, before televisions around the city went blank.

27A 2013 report found that more than half of the world's securities exchanges had been hit by a cyberattack.

28In 2008, hackers allegedly caused a pipeline in Turkey to explode by breaking into the network through surveillance cameras, which connected to the pipeline's controls; the hackers were able to raise the pressure in the pipeline until it blew up.

29Several years ago, a German steel mill was hit with an attack that prevented its blast furnace from shutting down properly, resulting in significant damage.

When the power went out, at 1 p.m., hundreds of subway cars carrying thousands of passengers who had decided to risk the ride suddenly found themselves stuck between stations;30 one group

that got trapped in an L train under the East River had to walk more than half a mile underground to get to First Avenue, using the light of their dying cell phones to navigate. Many of them said later they were expecting another threat — a bomb, a gas attack — figuring whatever sinister group was behind all this was sophisticated enough to coordinate that, too.

30When the 2003 blackout hit, there were more than 400,000 passengers trapped on 413 trains throughout the subway system. It took nearly three hours to evacuate the cars and 36 hours to resume full service.

Aboveground, traffic lights were out, so anyone willing to drive a car was crawling slowly through the snow. Many of the stranded were worried that the hackers had targeted their bank accounts, spiriting away their savings to some untraceable, block-chain account, possibly to fund future attacks — which were surely coming, according to the panicked chatter on the street. But all the ATMs were down, which made it hard to check. Credit-card readers didn't work, and neither did Apple Pay, so anyone who'd gone cashless couldn't buy anything. Stores around the city closed, and sporadic bouts of looting cropped up, along with rumors exaggerating the extent of it and the violence associated with it. Wall Street kept trading on backup generators, although most people wished it hadn't: Within minutes of the outage, the Dow had plunged.

For the hackers, getting access to the power grid had been simple enough. They mailed a USB stick31 to engineers at several companies that operate power-generating facilities in the New York area, with an attached letter saying the stick included an explanation of their benefits package for the upcoming year. Most of the engineers plugged the thumb drive into a home computer, but several took it to work and opened the document there.

31A recent study found that nearly half of us will pick up a random USB stick on the street, plug it in, and open whatever we find.

Knowing what to do once they had breached the system32 was, for the hackers, a more difficult matter. In preparation, they had filled out the team with several electrical engineers who had been involved in a 2015 attack that knocked out power for several hours to a region in Ukraine the size of Connecticut.33 After the team got inside the utility's networks, the electrical engineers spent several months poring over the code, examining the particular system and equipment that the utility was using, and chatting online with an engineer from one of the utilities whom they had found grousing about his job on a Reddit forum. After six months of trial and error, working on a mirror system they had built themselves for testing, the engineers were able to develop several pieces of malicious code that, once inserted, were capable of damaging transformers and generators throughout several parts of the grid.34

32Most major utilities are required to follow a set of cybersecurity regulations, considered reasonably robust. (For instance, many require two-step identification to access control systems.) But smaller utilities are often not held to the same standard.

33Two days before last Christmas, a worker at the Prykarpattyaoblenergo control center, in western Ukraine, watched as the cursor on his monitor began moving, then proceeded to shut down 57 different substations, leaving more than 230,000 Ukrainians in the dark. The hackers had used malware called BlackEnergy — common enough that it comes with its own "help" file. The U.S. government has acknowledged that a version of BlackEnergy has already been found inside domestic industrial systems.

34Last year, the Associated Press reported that, about a dozen different times, hackers had gained enough access to control portions of America's power grid.

Power companies are used to handling outages with a variety of causes — hurricanes, squirrels, tree limbs35 — but given the events of the day, Homeland Security36 had already deployed members of its Industrial Control Systems Cyber Emergency Response Team to New York by the time the power went out. As the DHS teams fanned out to the control centers at various utilities, reports had begun to trickle back from engineers who were inspecting substations37 in the field. While some had simply been knocked offline, one worker called back with worse news: Several transformers at one substation were broken.38 Workers at other facilities called back with similar news. The control center had noticed nothing amiss, which didn't make sense, until the team from the DHS realized that the attackers had manipulated the displays on the control-center computers so that they were presenting information from 24 hours earlier, when everything had been fine. It was just a few lines of code, but the damage39 would last: Transformers are expensive pieces of equipment, and the utilities hadn't stockpiled enough to replace every one. Getting certain parts could take months.40

35Just a week before the Ukraine attack, a power plant in Westchester was knocked off-line when some equipment was hit by a particularly large bird dropping.

36The Department of Homeland Security has 691 people working in cybersecurity but has said that it needs many more and that it has difficulty attracting talent.

37In Ukraine, the utility was able to get the power back on by switching to manual operation, something that would be much more difficult in the more modernized American grid.

38In 2007, American hackers working in a government lab were able to destroy a generator simply by writing 21 lines of malicious code that caused it to spin out of control. Some of the generator's parts were found 80 feet away.

39Only three incidents of physical damage caused by cyberattack have been publicly reported: the government-sponsored generator hack, Stuxnet, and the German steel mill.

40Electrical transformers, most of which are built overseas, can weigh more than 200 tons and have to be transported on railcars and barges. One transformer can take as many as 18 months to acquire.

As night fell, the New York City sky was an inky black. Every building with a backup generator became a gathering place, while everyone else curled up with candles at home. (The FDNY had its busiest night of house fires since the '70s.) Several people who lived in homes neglected by slumlords, with only electric heaters to keep them warm, were found suffering from hypothermia, and several more died of carbon-monoxide poisoning from a portable generator. The uncertainty over who was doing the attacking, and what the next attack might be, sent many people to bed with a looming dread. Something worse was coming, they were all sure, and every device they owned could be turned against them and was now a threat.



When the power went out, so did the subways, stranding riders. *Illustration: R. Kikuo Johnson*

As those who were able to sleep began to wake up the next morning, the attacks seemed to have stopped — though no one could say for certain. Security teams at every company and government agency had worked through the night to safeguard their systems, and the Pentagon, joined by intelligence agencies around the world, was trying to track down the offending hackers, who seemed to have decided to stand down and withdraw for a while. Traffic was light in and out of the city, and the subway remained closed as power came back on in spurts: Parts of the city had electricity within 24 hours, but it took days for other areas to come back online. When the subway finally started running again, it did so with delays and was filled with passengers who glanced anxiously at one another whenever the train unexpectedly hit its brakes. The city's head of cybersecurity was fired, as were several of the engineers who had plugged in the USB sticks.

Only a dozen people had died in the attack, but the city had undeniably changed. No buildings had been destroyed, no bombs had exploded, no money had been stolen, but each scenario now seemed not just possible but imminent. The direct economic cost41 was sure to be significant — the Dow dropped a thousand points by week's end — and the personal trauma was still ongoing. The man whose wife had supposedly walked out of the hospital after having her surgery had spent all

day and night searching for her, until his cell phone finally died. He went to the hospital the next morning and pleaded with anyone he could find. Eventually, one nurse, who hadn't slept in 24 hours, found his wife in cardiology, lying down in a hospital bed with an IV still stuck in her arm.42

41In 2015, Lloyd's of London published a report imagining a cyberattack in which 93 million people along the East Coast were left without power for days — a threat it judged to be within the once-in-200-year probability that insurers should prepare for. Such an attack, Lloyd's estimated, could set back the American economy by more than a trillion dollars.

42A similar incident happened earlier this year at the D.C.-area hospital that was hit with a ransomware attack.

But the worst damage was psychological. Because the grid that powers New York is connected with a larger regional grid, the outage affected tens of millions of people and set off a national debate that was more unhinged than most — a fearful swirl of xenophobia, Luddism, and political grandstanding. Everything that had looked like progress over the previous two decades now looked more like a Trojan horse: "Smarthome" devices and driverless-car initiatives became political footballs. For every measure to increase funding forcybersecurity,43 there was a congressman demanding that evenwhite-hat hackers,44 who tried to probe systems as a way to point out vulnerabilities before the bad guys got to them, be thrown in jail. The president's domestic agenda was shelved, as the next 18 months required convincing the American people that their government was capable of protecting them from their own devices, even as security experts acknowledged that there was no way to build a world of interconnected systems that was completely secure. Americans had spent the past decade and a half gradually coming to terms with the fact of anti-American Islamist terrorism,45 mostly by comforting themselves that the perpetrators were far away, separated by not only geography but the massive buffer of America's national-security apparatus. Now even that apparatus seemed vulnerable to malicious redirection. Air-traffic control, a local bank, the iPhone app46 that came with an electroshock function — cracking those seemed suddenly like child's play.

43President Obama has proposed spending $19 billion on federal cybersecurity funding, an increase of 35 percent from last year.

44Some companies have launched "bug bounty" programs, in which third-party hackers are invited to attack a company's system to probe it for vulnerabilities. After starting such a program earlier this year, General Motors reportedly got more than 100 submissions in three days. Soon after, the Pentagon launched a similar program.

45In March, a Justice Department representative said the Islamic State was "actively attempting" to cause major damage in the U.S. by means of cyberattack, and last month, the U.S. government acknowledged that it was conducting cyberattacks against ISIS. A loose coalition of hackers affiliated with ISIS recently announced that they were organizing under the banner of the United Cyber Caliphate. But most of the group's attacks have been rudimentary: This spring, it published the names and addresses of 3,602 of New York's "most important citizens," which turned out to be a seemingly random list of names.

46iPhones are actually relatively secure, as evidenced by the difficulty the FBI had accessing information on the San Bernardino shooter's iPhone, which makes them unlikely targets for hackers.

It was hard to blame people for their anger when they had been told to trust that the devices they brought into their lives were safe, only to find that many of them weren't. Parents who had done

their Christmas shopping on Cyber Monday returned anything with a Wi-Fi connection. Everyone had to be reminded again of all the incredible benefits of a connected world. Doctors had to convince people that their implantable defibrillators47 couldn't be hacked. Americans begrudgingly accepted the inconveniences experts said were necessary — triple verification, firewalls between firewalls, encrypted encryption — but the phrase *cybersecurity theater* soon joined its airport predecessor in the lexicon of nanny-state policies. Copycat attacks sprang up around the world: trains going haywire in Japan; smart thermostats freezing pipes in Minneapolis; Chinese hackers noodling around a water utility in San Francisco. Americans suddenly realized that, although they had spent plenty of time anguishing about how to protect the country's physical borders, with every device they bought, they had been letting more and more invaders into their cities, their homes, and their lives. They had moved everything they did online, thinking they were moving into the future; they woke up the morning after thinking they'd moved into a war zone instead. What frightened people most wasn't the attack itself, but rather what it foreshadowed. The day after, the hackers had sent a drone flying over the city dropping leaflets with a simple message: WE'LL BE BACK. It almost didn't matter whether they would.

47In 2014, security researchers found that they could hack into certain types of Bluetooth-enabled defibrillators and deliver shocks to a patient's heart.

**This article appears in the June 13, 2016 issue of* New York *Magazine.*