Tabs | dinsdag 8 maart 2016 13:00:47

P.3

For Netflix, Discontent Over Blocked VPNs Is Boiling | WIRED
http://www.wired.com/2016/03/netflix-discontent-blocked-vpns-boiling/

P.7

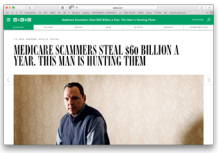
Google's Nifty New Tool Helps Designers Pick the Right UI | WIRED
http://www.wired.com/2016/03/googles-nifty-new-resizer-tool-helps-designers-pick-right-ui/

P.8

Hack Brief: Ransomware Strikes Apple's OS X for the First Time | WIRED
http://www.wired.com/2016/03/hack-brief-ransomware-hits-mac-os-x-first-time/

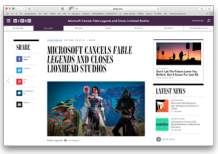
P.11

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED
http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/



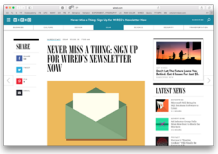
P.18

Medicare Scammers Steal $60 Billion a Year. This Man Is Hunting Them | WIRED
http://www.wired.com/2016/03/john-mininno-medicare/



P.24

Microsoft Cancels Fable Legends and Closes Lionhead Studios | WIRED
http://www.wired.com/2016/03/lionhead-fable-legends-canceled/



P.25

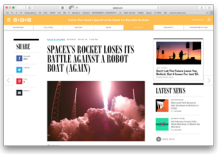
Never Miss a Thing: Sign Up for WIRED's Newsletter Now | WIRED
http://www.wired.com/2016/03/never-miss-thing-sign-wireds-newsletter-now/

P.26

New Tech Could Give Coal a Scrubbing Until Renewables Are Ready | WIRED
http://www.wired.com/2016/03/new-tech-give-coal-scrubbing-renewables-ready/

P.28

Poor Ted Cruz Doesn't Even Get a Funko Election Figurine | WIRED
http://www.wired.com/2016/03/funko-candidate-figurines/

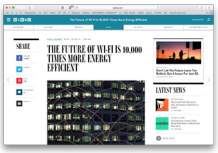


P.30

SpaceX's Rocket Loses Its Battle Against a Robot Boat (Again) | WIRED
http://www.wired.com/2016/03/spacexs-rocket-loses-battle-robot-boat/

P.32

The 4 Most Important Things MythBusters Taught the World | WIRED
http://www.wired.com/2016/03/4-important-things-mythbusters-taught-world/



P.35

Passive Wi-Fi Could Make Your Internet 10,000 Times More Efficient | WIRED
http://www.wired.com/2016/03/future-wi-fi-10000-times-energy-efficient/

P.38

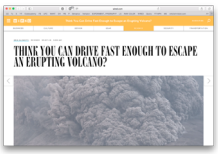
The Master of Drones Turns Flying Machines Into Performers | WIRED
http://www.wired.com/2016/03/master-drones-turns-flying-machines-performers/

P.42

The Untold Story of Silk Road, Part 2: The Fall | WIRED
http://www.wired.com/2015/05/silk-road-2/

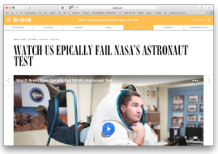
P.82

The White House Wants You to Build Tools to Improve Our Cities | WIRED
http://www.wired.com/2016/03/white-house-wants-build-tech-tools-data/



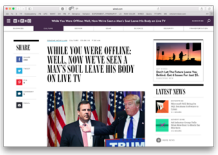
P.84

Think You Can Drive Fast Enough to Escape an Erupting Volcano? | WIRED
http://www.wired.com/2016/03/think-can-drive-fast-enough-escape-erupting-volcano/



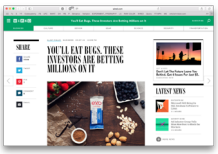
P.89

Watch Us Epically Fail NASA’s Astronaut Test | WIRED
http://www.wired.com/2016/03/watch-us-epically-fail-nasas-astronaut-test/



P.91

While You Were Offline: Well, Now We’ve Seen a Man’s Soul Leave His Body on Live TV | WIRED
http://www.wired.com/2016/03/internet-week-61/



P.100

You’ll Eat Bugs. These Investors Are Betting Millions on It | WIRED
http://www.wired.com/2016/03/investors-bet-millions-wont-balk-eating-bugs/

For Netflix, Discontent Over Blocked VPNs Is Boiling

In January, Netflix announced it would begin blocking a popular tech workaround known as a VPN, or virtual private network, that allowed customers beyond the US to access the same shows and films as American audiences. But as Netflix has aggressively pursued an ever-bigger global audience, simmering unhappiness over the ban is reaching a boil. An online petition demanding that Netflix change its policy has more than 36,000 signatures. And a new survey reveals that the crackdown may lead to piracy.

For years, paying Netflix subscribers abroad have used VPN proxies to disguise their location to access more content. There aren't any reliable estimates of how many Netflix subscribers use VPNs, but VPN services say they have massive user bases, in a few cases specifically for accessing Netflix. Netflix CEO Reed Hastings has said the company does not expect the block will impact subscriber numbers. But even if they don't leave Netflix, VPN users aren't happy.

"A massive number of people are affected," says Jordan Fried, the CEO of Buffered VPN, in an email. He claims to have found a tech fix to get around Netflix's block. "We are in touch with hundreds of people daily about the VPN block. Many of our users are coming to us from other VPN providers who no longer work."

For Netflix, the issue is a fragile one. The company, after all, is dependent on studios

and networks for much of the content that it streams on its platform. The crackdown is a way to show Hollywood studios that Netflix respects its regional licensing agreements—in essence, that it will only let people who it's paid to let see certain shows and movies see them.

> @julia_greenberg @WIRED I guess Netflix don't want my money then. Lots of other ways to watch movies and shows for free. Goodbye netflix
>
> — Mark (@mdluk199) 5:47 PM - 15 Jan 2016

But paying Netflix subscribers don't care what, say, Sony or the CW want: they want (and expect) to see what they want to see. They also want to be able to use a VPN for privacy and practical reasons. Until Netflix can offer the same content everywhere to everyone who pays for it, many users—especially the overseas users the company most covets—won't be happy.

Privacy, Practicality, Content

Netflix subscribers say there are a few key reasons to use a VPN: privacy, practicality, and content.

Digital rights group Open Media says that Netflix is putting users at risk by forcing them to access the service without VPNs. "If Netflix does need to enforce, as we would see it as, content restriction, there have to be better ways to do it," says David Christopher, the communications manager of Open Media, which is behind the online petition. "Many people rely on VPNs as a privacy tool."

But the reasons for VPN use aren't always so noble. One Canadian Netflix user tells WIRED he uses a VPN to watch Netflix when he isn't at home. "I am unable to watch Netflix at work on my break because my company Wi-Fi will not allow it," he said in a Twitter message. The same goes for watching at a coffee shop. "I used to use a VPN to get around this, and now I can't."

More subscribers, however, seem upset that Netflix is limiting the shows and films they can see. Dublin resident Alan Dempsey said in a Twitter message that his VPN service still sometimes works, but not always. While he continues to subscribe to Netflix, he says he's already seen most of the movies and documentaries he wants to without the VPN. "If it continues or gets worse, I will probably cancel my Netflix subscription altogether as the content for the UK and Ireland simply is not good enough."

Others feel similarly frustrated with their local Netflix offerings. Jay Sanchez says in Mexico he misses watching British shows like *Broadchurch* and Asian films that are "quite scarce on my local Netflix." "I can use the local Netflix," Sanchez wrote in an

email, "I can also browse other versions of Netflix, but can't stream anymore. I get a 'you are using a proxy' error message."

In Poland, even some Netflix originals are cut, tweets Grzegorz Mikos. He laments, for example, that there's no *House of Cards* available on the Polish service, which launched earlier this year. "We have one-third of the USA content for 10 Euros. I waited so long and got this."

Meanwhile, Netflix isn't yet available in China, but some people use VPNs there to disguise their location to watch it anyway. Catherine Hewett, an American living in China, does just that. "Being able to use Netflix was just a bonus, but eventually it became the China-censored website that I use the most," she said in an email, adding that she's only recently been affected by the VPN crackdown.

"Occasionally, [my] workaround isn't always successful, and then I get Netflix rage. I've become so reliant on Netflix that I stopped using all the other ways of watching TV shows and movies."

'Money Is Not The Issue'

Not all VPNs have stopped working for Netflix subscribers. Some proxies remain unaffected, others have built workarounds, and some have stopped working for now. Shaun M. says the proxy service he pays for works fine. "I live in central Ontario, Canada, which is dominated by two TV carriers," he explained in an email. (He did not want his full name used for fear of breaking Netflix's terms of use.) "Both services are very expensive, offering overpriced packages in order to access decent content."

So he uses a VPN service to get Netflix, Hulu, and Amazon Prime. "I pay the fees, as any red-blooded American would do. I just happen to live north of the border," he says. He says if the VPN service did stop working, he'd lose the chance to watch many CW shows ("we're huge superhero nerds") as well as some FOX and NBC shows.

'I pay the fees, as any red-blooded American would do. I just happen to live north of the border.'

Maique Madeira of Portugal says his VPN still works just fine as well, but if it stops, he has no problem going back to torrenting shows and films. "I'm using a VPN because I feel I should get access to the same catalog as the US customers, or any other country's user," he said in an email. "We pay the same amount and yet we get a fraction of the content available elsewhere."

"Money is not the issue," he adds. "It's unfair. That's my issue with it."

Netflix wants to be TV for the world. But as the company tries to convince people across 190 countries to sign up, it will have to prove that it has what they want. "I

cancelled as a paying customer," Johan Stindt, who lives in Austria and the Netherlands, said in a Twitter message. He says he travels throughout Europe and doesn't want to be restricted by what he's able to see. And he believes Netflix's policy will encourage piracy.

"Piracy is made by the greed of the entertainment industry and stockholders," he adds. "I am a normal man willing to pay for content and they are making that almost impossible."

GOOGLE'S NIFTY NEW TOOL HELPS DESIGNERS PICK THE RIGHT UI

Google

Not long after Google debuted Material Design across all its products and platforms, it started publishing tutorials on how other designers could do the same. Material Design, if you need a refresher, is Google's visual design language. It's a comprehensive and growing set of rules that dictates how Google's user interfaces look and behave. As technology evolves, so does Material Design. There are mandates for how animated objects should simulate believable acceleration and deceleration, how to choose a color palette, and how responsive UIs should flex across different screen sizes.

Resizer is a new tool from Google, created to help designers with that last bit—responsive layouts. Google is calling it an "interactive viewer to see and test how digital products respond to Material Design breakpoints across desktop, mobile, and tablet." Enter any URL into the search bar at the top of Resizer's page, and the tool can populate that website into a variety of layouts. You can see anything—your local newspaper, your blog, Facebook—rendered in real time. The idea is to see which layout patterns work best for each screen size. It's a tricky but crucial part of the design process. Zach Gibson, the Google designer who wrote the introduction post for Resizer, explains:

> As designers and developers of digital products, one of our greatest challenges is figuring out how to serve the right UI to our users at the right time. No matter how they're using an application, be it a phone or through VR, manipulating it with gesture or a mouse, on the latest and greatest tech or a hand-me-down 2G, it is our responsibility to make our products accessible to everyone—and that's a pretty tall order. There's no simple design solution to fit every need.

Resizer's most useful feature is how clearly it shows breakpoints. Material Design specifies the column and width specifications that Google believes will create the best user experience, but they change dramatically across devices. Simply scaling down a desktop design for a phone screen won't do the trick; navigation patterns and the amount of information being presented will all need adjustments. With Resizer, it's as if you have a digital ruler measuring out how a URL performs in each instance. For designers and developers—at least, those who wants to emulate Google's design—Resizer makes responsive UIs a cinch.

Hack Brief: Ransomware Strikes Apple's OS X for the First Time

While ransomware has been a growing cause for concern—including one recent high-profile incident at a Hollywood hospital—until now Apple devices hadn't had the distinction of being vulnerable. That changes with KeRanger, an application poised to shake down a large number of Mac owners in the coming days.

The Hack

According to researchers Claud Xiao and Jin Chen, who first reported the existence of KeRanger, the ransomware infected the Transmission BitTorrent client installer for OS X for the first time on March 4. While they're not sure how Transmission became infected, the two note that it's an open source project. "It's possible that Transmission's official website was compromised and the files were replaced by re-compiled malicious versions, but we can't confirm how this infection occurred," they wrote in a post outlining their discovery.

More troublingly, KeRanger was signed with a valid certificate, meaning it snuck through Apple's built-in safeguards. It's unclear how that happened, as well, though F-Secure security expert Mikko Hyppönen suspects it was simply a stolen code-signing certificate.

Macs are officially drawing serious attention from bad actors.

"This arrives to you from the official download site of an official application vender. It was signed with a valid developer certificate," says Hyppönen. "It's a ransom trojan. It wants to gain access to your files, the user's files, not root access."

It doesn't need root access, because it's not trying to take over your computer; rather, it's looking for the kinds of files that you care about most—the photographs, the spreadsheets, the invoices—so it can then attempt to sell them back to you. Once installed, KeRanger lays dormant for three days, then starts to encrypt documents and files on your system. Specifically, it looks for 300 different extensions, ranging from .doc to .mp3 to .jpg to .txt.

Victims can regain access to their machines for one bitcoin, which equals a little over $400. The researchers also note that KeRanger is "under active development," and that the next step in its evolution may be to encrypt Time Machine files, so that if you're infected you can't simply call in their backups.

Who's Affected?

Anyone who downloaded one of two installers of Transmission version 2.90, between

the hours of 11 a.m. PST on March 4 and 7 p.m. PST on March 5, is potentially affected. It's not clear currently how many people that is, but if you downloaded that BitTorrent client recently, you should be aware of what's coming.

Fortunately, there's a way to project yourself, according to Xiao and Chen. From their report:

> 1. Using either Terminal or Finder, check whether /Applications/Transmission.app/Contents/Resources/ General.rtf or /Volumes/Transmission/Transmission.app/Contents/Resources/ General.rtf exist. If any of these exist, the Transmission application is infected and we suggest deleting this version of Transmission.
>
> 2. Using "Activity Monitor" preinstalled in OS X, check whether any process named "kernel_service" is running. If so, double check the process, choose the "Open Files and Ports" and check whether there is a file name like "/Users//Library/kernel_service" (Figure 12). If so, the process is KeRanger's main process. We suggest terminating it with "Quit -> Force Quit".
>
> 3. After these steps, we also recommend users check whether the files ".kernel_pid", ".kernel_time", ".kernel_complete" or "kernel_service" existing in ~/Library directory. If so, you should delete them.

Also, as Apple has revoked the certificate in question, your system should warn you, if you attempt to open Transmission, that it may do harm. If so, trash the application.

How Serious Is This?

If you're affected, it's serious to the tune of $400. The 72-hour clock expires starting this afternoon and runs through tomorrow night, so all affected people should know by Wednesday morning what kind of trouble they're in.

The bigger concern, says Hyppönen, is that Macs are officially drawing serious attention from bad actors. Many Apple enthusiasts may assume that their devices have superior virus protection. In truth, Macs simply haven't historically been a popular target because of their small market share. Likewise, most malware practitioners don't have a core competence in Macs, because they've invested so much time and energy attacking Windows machines.

"It's not just a question about market share," says Hyppönen. "It's also a question of existing know-how. Most of the ransom code gangs have all their existing know-how on Windows platforms, so for them to start targeting any other platform, whether it's Android or OS X, is an investment from them. They're not likely to do that for as long as

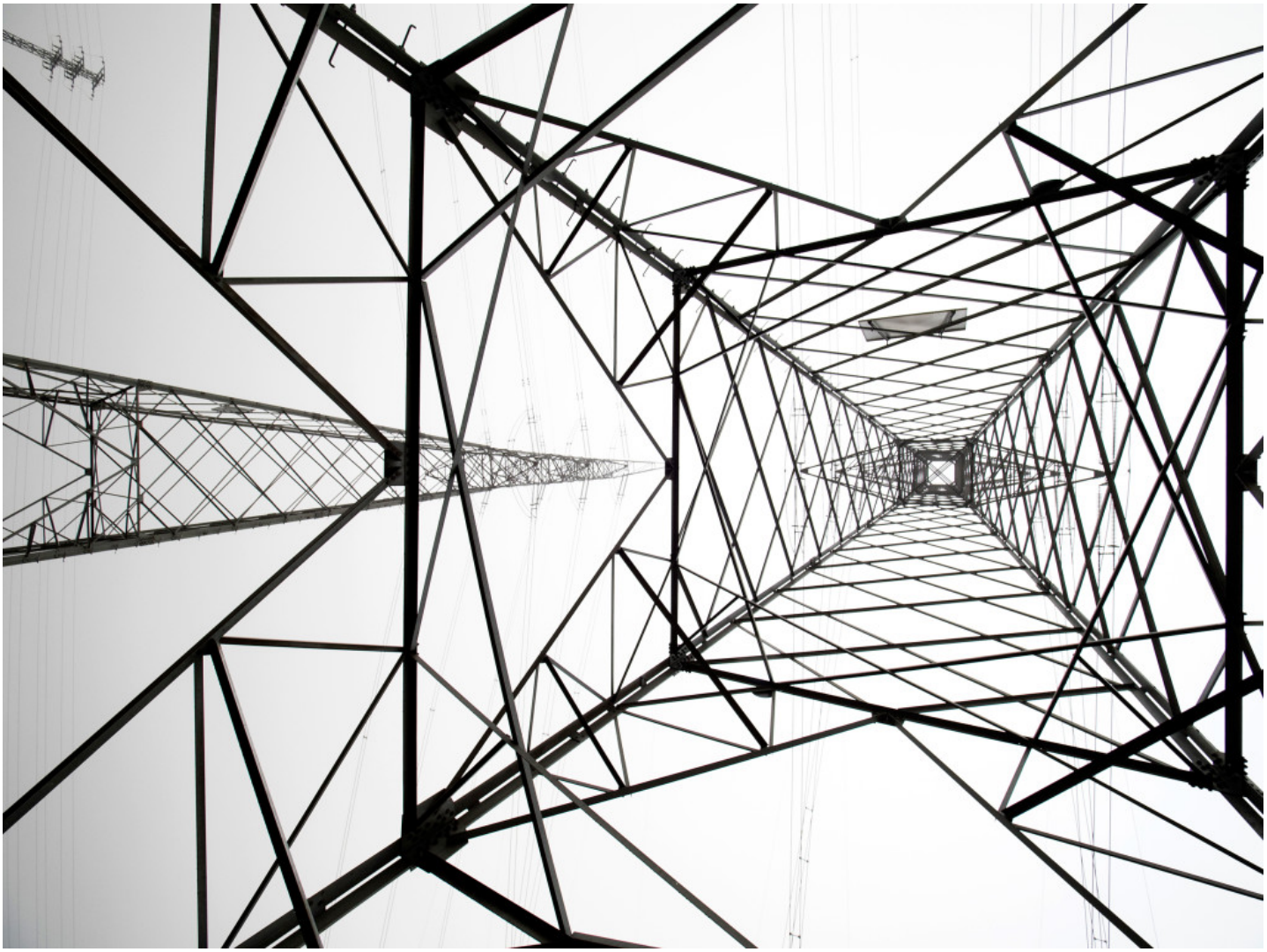
they have enough easy targets on a Windows platform."

In the case of KeRanger, it could be that one gang grew tired of competing with several others over the same Windows devices, and opted for clearer pastures. "Right now there is no competition on ransom trojans on Mac," says Hyppönen.

If KeRanger turns out to be a successful haul, that could change quickly. And even if it's not, the growing size of the OS X install base may make increased attacks inevitable. According to the most recent figures from IDC, Apple accounted for 7.9 percent of all personal computers last quarter, and increased shipments by 2.8 percent year over year. That may not sound like a huge jump, but consider that the industry as a whole was down over 10 percent.

So yes, it's a big deal that OS X has its first ransomware. The bigger issue, though, is that it's going to be far from the last.

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid



It was 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

He watched as it navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline. A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm. Somewhere in a region outside the city he knew that thousands of residents had just lost their lights and heaters.

The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive. Then as the cursor moved in the direction of another breaker, the machine suddenly logged him out of the control panel. Although he tried frantically to log back in, the attackers had changed his password preventing him from gaining

re-entry. All he could do was stare helplessly at his screen while the ghosts in the machine clicked open one breaker after another, eventually taking about 30 substations offline. The attackers didn't stop there, however. They also struck two other power distribution centers at the same time, nearly doubling the number of substations taken offline and leaving more than 230,000 residents in the dark. And as if that weren't enough, they also disabled backup power supplies to two of the three distribution centers, leaving operators themselves stumbling in the dark.

A Brilliant Plan

The hackers who struck the power centers in Ukraine—the first confirmed hack to take down a power grid—weren't opportunists who just happened upon the networks and launched an attack to test their abilities; according to new details from an extensive investigation into the hack, they were skilled and stealthy strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, then launching a synchronized assault in a well-choreographed dance.

"It was brilliant," says Robert M. Lee, who assisted in the investigation. Lee is a former cyber warfare operations officer for the US Air Force and is co-founder of Dragos Security, a critical infrastructure security company. "In terms of sophistication, most people always [focus on the] malware [that's used in an attack]," he says. "To me what makes sophistication is logistics and planning and operations and … what's going on during the length of it. And this was highly sophisticated."

Ukraine was quick to point the finger at Russia for the assault. Lee shies away from attributing it to any actor but says there are clear delineations between the various phases of the operation that suggest different levels of actors worked on different parts of the assault. This raises the possibility that the attack might have involved collaboration between completely different parties—possibly cybercriminals and nation-state actors.

"This had to be a well-funded, well-trained team. … [B]ut it didn't have to be a nation-state," he says. It could have started out with cybercriminals getting initial access to the network, then handing it off to nation-state attackers who did the rest.

The control systems in Ukraine were surprisingly more secure than some in the US.

Regardless, the successful assault holds many lessons for power generation plants and distribution centers here in the US, experts say; the control systems in Ukraine were surprisingly more secure than some in the US, since they were well-segmented from the control center business networks with robust firewalls. But in the end they still weren't secure enough—workers logging remotely into the SCADA network, the

Supervisory Control and Data Acquisition network that controlled the grid, weren't required to use two-factor authentication, which allowed the attackers to hijack their credentials and gain crucial access to systems that controlled the breakers.

The power wasn't out long in Ukraine: just one to six hours for all the areas hit. But more than two months after the attack, the control centers are still not fully operational, according to a recent US report. Ukrainian and US computer security experts involved in the investigation say the attackers overwrote firmware on critical devices at 16 of the substations, leaving them unresponsive to any remote commands from operators. The power is on, but workers still have to control the breakers manually.

That's actually a better outcome than what might occur in the US, experts say, since many power grid control systems here don't have manual backup functionality, which means that if attackers were to sabotage automated systems here, it could be much harder for workers to restore power.

Timeline of the Attack

Multiple agencies in the US helped the Ukrainians in their investigation of the attack, including the FBI and DHS. Among computer security experts who consulted on the wider investigation were Lee and Michael J. Assante, both of whom teach computer security at the SANS Institute in Washington DC and plan to release a report about their analysis today. They say investigators were pleasantly surprised to discover that the Ukrainian power distribution companies had a vast collection of firewall and system logs that helped them reconstruct events—an uncommon bonanza for any corporate network, but an even rarer find for critical infrastructure environments, which seldom have robust logging capabilities.

According to Lee and a Ukrainian security expert who assisted in the investigation, the attacks began last spring with a spear-phishing campaign that targeted IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine. Ukraine has 24 regions, each divided into between 11 and 27 provinces, with a different power distribution company serving each region. The phishing campaign delivered email to workers at three of the companies with a malicious Word document attached. When workers clicked on the attachment, a popup displayed asking them to enable macros for the document. If they complied, a program called BlackEnergy3—variants of which have infected other systems in Europe and the US—infected their machines and opened a backdoor to the hackers. The method is notable because most intrusions these days exploit a coding mistake or vulnerability in a software program; but in this case the attackers exploited an intentional feature in the Microsoft Word program. Exploiting the macros feature is an old-school method

from the 90's that attackers have recently revived in multiple attacks.

The initial intrusion got the attackers only as far as the corporate networks. But they still had to get to the SCADA networks that controlled the grid. The companies had wisely segregated those networks with a firewall, so the attackers were left with two options: either find vulnerabilities that would let them punch through the firewalls or find another way to get in. They chose the latter.

Over many months they conducted extensive reconnaissance, exploring and mapping the networks and getting access to the Windows Domain Controllers, where user accounts for networks are managed. Here they harvested worker credentials, some of them for VPNs the grid workers used to remotely log in to the SCADA network. Once they got into the SCADA networks, they slowly set the stage for their attack.

First they reconfigured the uninterruptible power supply[1], or UPS, responsible for providing backup power to two of the control centers. It wasn't enough to plunge customers into the dark—when power went out for the wider region they wanted operators to be blind, too. It was an egregious and aggressive move, the sort that could be interpreted as a "giant fuck you" to the power companies, says Lee.

Each company used a different distribution management system for its grid, and during the reconnaissance phase, the attackers studied each of them carefully. Then they wrote malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations (the converters are used to process commands sent from the SCADA network to the substation control systems). Taking out the converters would prevent operators from sending remote commands to re-close breakers once a blackout occurred. "Operation-specific malicious firmware updates [in an industrial control setting] has *never* been done before," Lee says. "From an attack perspective, it was just so awesome. I mean really well done by them."

The same model of serial-to-Ethernet converters used in Ukraine are used in the US power-distribution grid.

Armed with the malicious firmware, the attackers were ready for their assault.

Sometime around 3:30 p.m. on December 23 they entered the SCADA networks through the hijacked VPNs and sent commands to disable the UPS systems they had already reconfigured. Then they began to open breakers. But before they did, they launched a telephone denial-of-service attack against customer call centers to prevent customers from calling in to report the outage. TDoS attacks are similar to DDoS attacks that send a flood of data to web servers. In this case, the center's phone systems were flooded with thousands of bogus calls that appeared to come from Moscow, in order to prevent legitimate callers from getting through. Lee notes that the

move illustrates a high level of sophistication and planning on the part of the attackers. Cybercriminals and even some nation-state actors often fail to anticipate all contingencies. "What sophisticated actors do is they put concerted effort into even unlikely scenarios to make sure they're covering all aspects of what could go wrong," he says.

The move certainly bought the attackers more time to complete their mission because by the time the operator whose machine was hijacked noticed what was happening, a number of substations had already been taken down. But if this *was* a political hack launched by Russia against Ukraine, the TDoS likely also had another goal Lee and Assante say: to stoke the ire of Ukrainian customers and weaken their trust in the Ukrainian power companies and government.

It wasn't enough to plunge customers into the dark–they wanted operators blind, too.

As the attackers opened up breakers and took a string of substations off the grid, they also overwrote the firmware on some of the substation serial-to-Ethernet converters, replacing legitimate firmware with their malicious firmware and rendering the converters thereafter inoperable and unrecoverable, unable to receive commands. "Once you … rewrite the firmware, there's no going back from that [to aid recovery]. You have to be at that site and manually switch operations," Lee says. "Blowing [these] gateways with firmware modifications means they can't recover until they get new devices and integrate them."

After they had completed all of this, they then used a piece of malware called KillDisk to wipe files from operator stations to render them inoperable as well. KillDisk wipes or overwrites data in essential system files, causing computers to crash. Because it also overwrites the master boot record, the infected computers could not reboot.

Some of the KillDisk components had to be set off manually, but Lee says that in two cases the attackers used a logic bomb that launched KillDisk automatically about 90 minutes into the attack. This would have been around 5 p.m., the same time that Prykarpattyaoblenergo posted a note to its web site acknowledging for the first time what customers already knew—that power was out in certain regions—and reassuring them that it was working feverishly to figure out the source of the problem. Half an hour later, after KillDisk would have completed its dirty deed and left power operators with little doubt about what caused the widespread blackout, the company then posted a second note to customers saying the cause of the outage was hackers.

Was Russia the Cause?

Ukraine's intelligence community has said with utter certainty that Russia is behind the attack, though it has offered no proof to support the claim. But given political tensions

between the two nations it's not a far-fetched scenario. Relations have been strained between Russia and Ukraine ever since Russia annexed Crimea in 2014 and Crimean authorities began nationalizing Ukrainian-owned energy companies there, angering Ukrainian owners. Then, right before the December blackout in Ukraine occurred, pro-Ukrainian activists physically attacked substations feeding power to Crimea, leaving two million Crimean residents without power in the region that Russia had annexed, as well as a Russian naval base. Speculation has been rampant that the subsequent blackouts in Ukraine were retaliation for the attack on the Crimean substations.

But the attackers who targeted the Ukrainian power companies had begun their operation at least six months before the Crimean substations were attacked. So, although the attack in Crimea may have been a catalyst for the subsequent attack on the Ukrainian power companies, it's clear that it wasn't the original motivation, Lee says. Lee says the forensic evidence suggests in fact that the attackers may not have planned to take out the power in Ukraine when they did, but rushed their plans after the attack in Crimea.

"Looking at the data, it looks like they would have benefited and been able to do more had they been planning and gathering intelligence longer," he says. "So it looks like they may have rushed the campaign."

He speculates that if Russia is responsible for the attack, the impetus may have been something completely different. Recently, for example, the Ukrainian parliament has been considering a bill to nationalize privately owned power companies in Ukraine. Some of those companies are owned by a powerful Russian oligarch who has close ties to Putin. Lee says it's possible the attack on the Ukrainian power companies was a message to Ukrainian authorities not to pursue privatization.

That analysis is supported by another facet of the attack: The fact that the hackers could have done much more damage than they did do if only they had decided to physically destroy substation equipment as well, making it much harder to restore power after the blackout. The US government demonstrated an attack in 2007 that showed how hackers could physically destroy a power generator simply by remotely sending 21 lines of malicious code.

Lee says everything about the Ukraine power grid attack suggests it was primarily designed to send a message. "'We want to be seen, and we want to send you a message,'" is how he interprets it. "This is very mafioso in terms of like, oh, you think you can take away the power [in Crimea]? Well I can take away the power from you."

Whatever the intent of the blackout, it was a first-of-its-kind attack that set an ominous precedent for the safety and security of power grids everywhere. The

operator at Prykarpattyaoblenergo could not have known what that little flicker of his mouse cursor portended that day. But now the people in charge of the world's power supplies have been warned. This attack was relatively short-lived and benign. The next one might not be.

[1]*Correction 3/03/16 8:17 a.m. ET: UPS here stands for uninterruptible power supply, not universal power supply.*

Medicare Scammers Steal $60 Billion a Year. This Man Is Hunting Them

John Mininno slaps two pieces of paper onto an overhead projector. “Look at this,” he says. “You see how one form is a photocopy of the other—with just the date changed? It’s exactly the same paper!” The printouts are mere insurance forms, but Mininno is genuinely pissed off about them. “They’re allowed to bill for that procedure again six months after they first provide it. That date is six months to the day!”

Not everyone can get this worked up about insurance forms. But to Mininno, these are a combination of smoking gun and a slap in the face. Together they clearly show that someone is ripping off Medicare. But perhaps what’s worse is that someone is being really lazy about it.

If Willie Sutton had to choose a criminal career today, he’d be ripping off Medicare too. As the bank robber supposedly said: That’s where the money is. The program spends more than $600 billion a year on health care for 54 million people, most of them seniors. It is a massive pool of underguarded funds ripe for skimming. By the government’s own accounting, fraudsters scammed $60 billion from Medicare in 2014, and the losses are growing. Since 2007 more than 2,300 health care providers have been charged with fleecing Medicare, and more than 1,800 defendants have been convicted of felony offenses, ranging from claiming phantom services to performing unnecessary surgeries.

Finding a whistle-blower requires a nose for mischief, a gift for persuasion, and the technical chops to identify patterns in thickets of diagnostic codes and billing data.

Scams are run so often, by so many people, that dedicated government investigators can’t keep up: In 2014 prosecutions initiated by the government led to a mere 31 settlements yielding $88 million in fines. Luckily, there is another defense against Medicare fraud: whistle-blower lawsuits. Under the federal government’s false claims statute, any insider can sue a company that’s providing fraudulent services, on the government’s behalf. If the whistle-blower lawyers are successful, the plaintiffs collect 15 to 30 percent of the settlement as a bounty. In 2014 there were 469 of these health care fraud settlements—many involving huge pharmaceutical corporations and hospital networks—resulting in $2.2 billion in fines.

The problem is that even with this financial incentive, whistle-blowers can be skittish about coming forward and often are ill-prepared to present solid evidence. “When a whistle-blower goes to the government by himself,” says Patrick Burns, an antifraud activist in Washington, DC, “the whistle-blower is disorganized. They’re hot, and they don’t stick to just the facts. He’s pissed off because he was fired, and when angry

people call you up, you just assume, 'Crazy loser, you're a nut job.'"

Professional whistle-blower lawyers are much better at arguing a convincing case. But lawyers aren't always the best investigators. Sometimes finding an insider requires a nose for mischief, a gift for persuasion, and the technical chops to identify nonobvious patterns in impenetrable thickets of diagnostic codes and billing data. Sometimes it takes a bounty hunter. Someone like John Mininno.

A broad-shouldered former college linebacker who speaks in the blue-collar brogue of central New Jersey, Mininno is an unlikely big-data entrepreneur. After working his way through law school, he spent 18 years representing victims of medical negligence. What he saw made him angry. "I had a wrongful death case, a woman who went into a nursing home for rehab on a hip fracture," he says. While under the facility's care, the woman suffered a host of injuries, from a fractured tibia and ankle to severe pressure sores. Mininno argued in court that her death was preventable, had anyone simply repositioned her from time to time. "They put her in a room, they billed her insurance, and they didn't pay attention to her. It became clear to me that these were large corporations trying to monetize people's insurance. It's disgusting."

Over the years, Mininno developed a reputation as a lawyer who knew how to find evidence of fraud in billing patterns, and in 2011 he was approached by a financier who needed help vetting some investments in health care companies. Were these companies really profitable, or were they padding their financials with fake Medicare billings? He asked Mininno to shine a light and see if any cockroaches scurried out of those company records.

Around this time, a mountain of information on health care providers was becoming publicly available. In response to a Freedom of Information Act verdict, the Centers for Medicare and Medicaid Services (CMS) released data on tens of thousands of medical practices. It was a detailed catalog of all the procedures those practices provide to seniors and what they're paid to provide them. At the same time, various citizen journalists and data scientists were using Freedom of Information Act requests to get CMS data on physician referrals, which they assembled into a map of doctors who refer patients to each other—a network with 50 million connections—and the prescribing patterns of those doctors.

As a lawyer, Mininno looked at this trove and thought, "This is a massive business opportunity." Whistle-blower law firms have to advertise, because they need informants to come out of the woodwork. Then they need to qualify those sources—do they have enough evidence? Then they have to figure out whether the scale of the fraud (and thus the likely payout) justifies the work they'll have to plow into it, because they don't get paid unless they win. This is time-consuming and expensive.

From his days as a lawyer and his work looking through company medical records, Mininno knew what kind of footprints to look for in the data: what the scams are and how those scams are coded up for reimbursement. Without this knowledge, algorithms will churn up thousands of false positives. For example, you can't look at just medical practices that administer high volumes of pricey medications—there are doctors who legitimately administer extremely expensive injectable drugs, like chemotherapy, in their offices. There are clinics in areas where patients are sicker, and therefore more expensive to care for, than the general population. In other words, there are plenty of legitimate reasons for outliers to be outliers.

People skip doctor visits during heavy snowstorms, so insurance claims should drop in bad weather.

Fraudsters aren't necessarily the biggest billers—it's a bit of a myth that fraud lives at the end of a bell curve. But they do have some distinctive ways of doing business, if you know what to look for. Mininno realized he could build a business around using data to find certain patterns, identify likely informants (usually former employees), and turn them into false-claims plaintiffs. He didn't have to wait for whistle-blowers to walk through his door—or advertise like the big whistle-blower law firms. He could use analytics to troll for sketchy providers and insiders, transforming that rare, long-odds game into a quantitative, target-rich discovery process with gumshoe work on the back end. Mininno pitched the idea to his Wall Street client, who became his angel investor. The National Healthcare Analysis Group was born.

If you're hunting for a big-game trophy, the first thing you've got to do is eliminate the targets that have already been tagged—only the first plaintiff to file gets a payout. So Mininno designed a system for combing through SEC filings to eliminate health care organizations that were already being investigated.

To identify potential informants, his developers assembled a database of 70,000 health care workers and their employment histories, scraped and extracted from publicly available sources. The ideal informants are well-qualified nurses who worked for a suspicious clinic, but only for a few months, then immediately got another job. They were obviously good employees, but something they saw on the job likely made them leave. Mininno cold-calls them. "For the most part," he says, "people are open and honest and want to tell their story."

To wrangle Medicare billing data, he became the first paying customer of a Portland, Oregon, startup called Carevoyance, which had cross-linked dozens of databases to identify referral networks. If a practice has been investigated, it's worth knowing who sends them patients, or vice versa.

To catch a crook, it helps to think like a crook. And crooks cut corners. Sometimes, they're too cheap to resolve contradictions between their Medicare claims and what

they tell state tax authorities. So when Mininno sees a practice where, according to Medicare records, nurses never miss a day's work, he pulls unemployment claims. Because when aides are laid off, they file for unemployment. But their bosses, who've been billing for the services of these never-absent, superproductive health workers, try to duck unemployment claims by asserting they were fired for not showing up for work. The billing data, which shows indefatigable employees, and the employers' claim that these same nurses were absent and unproductive can't both be right. Such a practice is a likely candidate for investigation. There are ways, Mininno says, to "poke holes in the perfect paperwork and the perfect data."

But data, algorithms, and geeks weren't enough. To get his venture going, Mininno needed his first insider, one willing to put their lips on the whistle and blow. Then he had a lucky break. A source from his days working for that Wall Street investor called and said: "There's a gentleman who's been sharing some stories with me. You might want to talk with him."

Mininno walked through the double glass doors of a Midwestern diner. He was meeting Alex, the nurse his source had hooked him up with. The guy was built like a refrigerator. He hadn't shaved in days, and he was hungry for pancakes.

"You must be John," he said. Mininno nodded. They followed the hostess back to a table where they sipped coffee and made small talk. As Alex demolished an extratall stack of blueberry pancakes with powdered sugar, Mininno described his company's mission: Nail the bad guys and compensate people who step forward with the evidence to make that happen.

A weight seemed to lift from the informant's mind. He'd been working at a home health clinic that sent nurses to help people after they'd been released from the hospital, and the clinic was essentially stealing money from the government, he said. He knew what he'd seen was wrong. But he hadn't known there was anything he could do to stop it. And now Mininno was offering a share of the settlement if he could help prove the company had engaged in fraud.

"I'm in," Alex said. (Some names and identifying details in this story have been changed.) Over the next three hours, he laid out the machinations of a Medicare profit mill: Nurses were instructed to skip patient assessments and provide services whether seniors needed them or not. Patients who needed more visits didn't get them, because repeat visits lowered profitability. The practice plied retirees with free trips to casinos and paid doctors kickbacks for referrals.

"Dirtbags," Mininno thought. "This is incredible. But I need the nuts and bolts." Was there anyone else with access to records that could prove this? "The IT guy," Alex

replied. “He lives in Atlantic City. He runs all the computers.”

A few weeks later, Mininno shuffled into a casino. He stood in the doorway as poker players stared at their cards. He had no idea which one to look for. Then, from the table closest to the door, a sharp set of eyes in a sharp-featured face looked straight at him. It was his guy, a computer programmer named Oscar. He was conspicuously alert, intelligent, the kind of guy who thinks a hundred miles a minute and doesn’t need much sleep. At night, he played poker. By day, he ran the IT infrastructure for Alex’s erstwhile employer, which had mushroomed into a multimillion-dollar operation.

Over steaks, Mininno gave his pitch some torque. “Listen,” he said, “if I’m here talking to you about your employer—if our little company can find this—it’s only a matter of time before someone goes to the authorities.” There were two options: Help the investigation before the company was busted and collect a slice of the settlement, or be interrogated later as the head geek of a fraudulent organization.

“I need some time to think about this,” the programmer said.

“Take all the time you need.”

A month later Mininno got a data file from Oscar. The numbers showed systematic gaming of Medicare reimbursement rules. One part of the scheme allegedly worked like this: Medicare pays a provider based on the number of visits to a patient’s house in a 60-day period. If the provider makes up to nine visits, it gets reimbursed $2,200. For 10 visits or more, the provider gets an additional $2,200, because the case is assumed to be more severe and complex. A chart of visits per patient in 2007 showed that five times as many patients were getting 10 visits than were getting nine visits. When Medicare changed its rules in 2008 to set payment thresholds at six, 14, and 20 visits, the frequency distribution shifted dramatically to maximize revenue at the new thresholds. Jacking up the number of visits just to get over those thresholds is fraud, because the only legal basis for Medicare reimbursement is medical necessity—not profit maximization.

Meanwhile, Mininno was using the employment database to find nurses who could confirm they’d been instructed to visit each patient once a week, regardless of whether the patient needed those visits (or required more frequent visits). Ultimately, Mininno worked with a law firm, which filed a false-claims lawsuit against the company in the spring of 2012. The Department of Justice reviews such cases and triages through them, looking for cases with merit. After two years of bureaucratic review, a Department of Justice task force pulled a warrant for a raid in 2014, and the case is now grinding through the settlement process. Since 2012, Mininno and the lawyers he works with have filed around 40 lawsuits, which means more raids, prosecutions, and

settlements are likely in the coming months and years.

Back at his office in a rented Victorian in New Jersey, Mininno is talking about snow days. His practice is expanding (he's currently searching for a data scientist with a public health background), and he's looking into potential new cases. His staff also includes a part-time private investigator, and he has software developers and statisticians on contract. One of the latter, Brandon Cosley, has written a query for Medicare claims during weather emergencies.

On snow days, people usually reschedule nonemergency appointments. They stay in bed instead of driving to the doctor. Emergency rooms will see an uptick in visits because of car accidents and cardiac events triggered by snow shoveling, while regular doctors' offices will see a drop. But providers filing for phantom services make the same number of claims in the middle of Snowpocalypse as they do the day before and the week after. They bill as if the day was totally normal, even if it was not a normal day at all. If there's a hallmark of fraud, it's a lack of variability—the missing randomness of people and their bodies and behaviors. Fraud is algorithmic and invariable because it's optimizing revenue, not meeting human needs.

This is the kind of thinking—a sense for where billing patterns don't match the practice of medicine—that can differentiate legitimate providers from billing mills that are ripping off Medicare and, by extension, taxpayers. It's a marriage of convenience between the government and the bounty hunters, explains Patrick O'Connell, who headed up the Texas Medicaid fraud division from 1999 to 2007, before becoming a whistle-blower attorney. "The government has a tendency to not like whistle-blowers who are just in it for the money. They prefer someone pure," he says. But in reality the government can't afford pure. It doesn't have enough lawyers to take on the teams of $1,000-an-hour attorneys that big health care operations tend to hire. These lawsuits, he says, are "the greatest outsourcing program in American history."

A gigantic government operation is always going to be an appetizing target for skimmers, rule benders, and straight-up crooks. Data science is part of the answer. Lawyers are still necessary. But to extract the dirt from the data, you need to understand how human beings might be tempted to manipulate the truth—and where they fail to cover their tracks. There is no app for that.

J. C. Herz (@jcherz) *is the author of* Learning to Breathe Fire.

This article appears in the March 2016 issue.

Microsoft Cancels Fable Legends and Closes Lionhead Studios

Microsoft will shutter its UK game development unit Lionhead Studios, canceling its Xbox One game *Fable Legends*, it said today.

Lionhead, founded by developer Peter Molyneux in 1996, created the simulation game *Black & White* and the Xbox RPG *Fable*. Microsoft acquired the company in 2006, and from then on it exclusively created games in the *Fable* series. The latest, *Fable Legends*, was a five-player action role-playing game in which a team of four "hero" players would join forces against a single "villain" player.

In development since 2012, *Legends* had a public beta test in 2014 but had been delayed bit by bit ever since. The latest news had the Xbox One and Windows 10 game shifting to a free-to-play model, and a demo showed up at last year's E3 Expo.

In addition, Microsoft also said that it would shutter Denmark-based studio Press Play, and cancel its planned Xbox One game *Project Knoxville*.

Never Miss a Thing: Sign Up for WIRED's Newsletter Now

Getty Images

Even with the latest social platforms and push notifications, it’s hard not to miss the days when the news was delivered right to your doorstep. Charming, right? That’s why we select the best of WIRED—from unparalleled security reporting and business analysis to exclusive details about the latest in design and technology—and send you one (just one, we swear!) email each day.

Sign up to get WIRED’s biggest stories delivered right to your inbox.

New Tech Could Give Coal a Scrubbing Until Renewables Are Ready

No matter how you feel about coal, you can't deny that it is very dirty stuff. Nor can you argue that our electrified society is anywhere near ready to run without it. Until renewables scale up and become storable—available after sunset and between breezes, in other words—coal will continue to supply a big part of the world's energy.

And don't let recent reports of its death fool you, either. Sure, Oregon's legislature just passed a law promising to quit coal, but they gave themselves until 2030 to complete the wean. And that's in a state with beaucoup hydroelectric energy and a booming renewables industry. If you really want to know how coal is doing, look to growing economies (and massive populations) in places like India and China. The two countries may have greener ambitions, but both are still burning heaps of the dirty dark stuff. Renewables need time to take over, during which the coal industry is going to keep coughing up greenhouse gases and poisonous pollutants.

In the interim, coal is struggling to get cleaner. The problem isn't just that burning the stuff releases planet-warming CO_2—that's a whole other problem. Coal is full of things like mercury, sulfur, and harmful particulate matter that cause acute and chronic health problems. Collectively, let's call them pollutants. A lot of people have been focusing on the postcombusion—filters and scrubbers that capture the smoke before it leaves the stack. But these technologies range between prohibitively expensive and, uh, nonexistent. Another option is purifying the coal itself, so it burns cleaner and produces more energy per lump.

Imaginatively-named Clean Coal Technologies, Inc. approaches coal as though it were a different type of fossil fuel. "I came out of the oil business, and my philosophy has always been you refine and then burn," says Robin Eves, CCTI's CEO. His business does this with heat. Not enough to set the coal aflame, but enough to coax out moisture and impurities. "By drying the coal we automatically increase its BTU value," says Eves. Think of it this way: If a single lump of coal produces more energy, then a power plant needs to burn less of it to meet its energy goals. Producing, therefore, fewer greenhouse gases and pollutants.

Optionally—depending on the regulations and emissions goals wherever the coal is being sent—CCTI removes impurities with further rounds of heating. Heavy metals like mercury slag off. "It comes out as a chemical soup and then the makeup of that soup are the volatiles in the coal," says Eves.

Eves says his company's process also addresses ash, which is probably the most

pernicious of all coal's health ills. "If you burn anything you'll get particles small enough to cross lung barriers and into blood stream," says Susan Buchanan, clinical associate professor in environmental and occupational health at the University of Illinois. Doctors now recognize that these small particulates are strongly linked to cardiovascular diseases.

But Buchanan says she is not convinced that CCTI's process is capable of eliminating these heart-attacking particulates. Not to mention the fact that the increased efficiency from the dehydration is barely mentionable when considering the necessary cuts that the world's governments are going to have to make to meet their Paris promises.

And it's not like the other impurities like mercury and sulfur just disappear. Eves says CCTI ships the chemical slag off to oil refineries, where it gets blended in with fuel feedstock, eventually becoming gasoline or jet fuel. "Nobody is pretending the oil is clean, but you're making coal a cleaner more efficient fuel," he says.

Currently, the company's Oklahoma test facility is only capable of making two to three tons of clean coal an hour. Its modular commercial plants will be able to process up to 30 tons, once energy buyers come online. Eves says he has seen substantial interest in the US and abroad, from both the private and public sector. "We're already seeing a very, very different attitude from Washington, the Department of Energy, and even the Environmental Protection Agency, to embrace companies who have tech to help the coal industry in the US," he says.

Poor Ted Cruz Doesn't Even Get a Funko Election Figurine

Presidential campaign merchandise is usually perfunctory at best: T-shirts, buttons, maybe the odd novelty belt buckle. Someone With Tiny Hands has his "Make America Great Again" hats. Bernie Sanders offers "Feel The Bern" mugs. And until recently, Ted Cruz had the nightmare fuel that are the posters of conservative street artist Sabo. But this summer will see another tchotchke to commemorate the indelible 2016 presidential campaign, and it's fantastic.

Funko, the toy company behind the increasingly popular Pop! vinyl figures, announced Friday that it will release a "Pop The Vote" line featuring three candidates for president: Hillary Clinton, Bernie Sanders, and Someone With Tiny Hands. (It's also releasing an intentionally revolting Garbage Pail Kids-themed figures named "Donald Dumpty" and "Billary Hillary.")

Funko owns hundreds of licenses, from Marvel and DC characters to movie characters to people like Conan O'Brien and John Oliver. The company has grown rapidly in recent few years, with Pop! figures and bobbleheads driving most of that business. But this reaction to the pop-culture zeitgeist is a new venture. (It's not *entirely* without precedent: Funko offered a Wacky Wobbler Obama bobblehead during his first campaign.)

Making a new figure typically means a lengthy, even months-long approval process, especially when working with licensors like *Star Wars* or Marvel. But the "Pop The Vote" line went from inspiration to reality in barely a month after a Funko staffer pointed to Bernie Sanders' emerging cultural impact. "It was around the time he was on *Saturday Night Live* and Larry David's impersonations were taking off," says Mark Robben, Funko's director of marketing. "It was just clear that from a pop culture perspective, this was something."

It wasn't the first time the company made a quick turnaround. When *Guardians of the Galaxy* hit theaters a few years ago, Funko riffed on each character—but hadn't yet seen the post-credits scene featuring the dancing baby Groot. Once everyone saw it, the course of action was clear. "We had it sculpted and into prototype within a few weeks, and then it was available as a pre-order on Amazon," says Robben. "It was the most pre-ordered toy of all time on Amazon, and then shipped a few months later."

Once the company knew it wanted to do something around Sanders, the conversation expanded to include other candidates, ultimately adding Clinton and Someone With Tiny Hands. Robben says that doesn't reflect the company's stand on politics—"it's just which candidates we thought are resonating within popular culture"—and isn't worried about any of the candidates winning the nomination. "Even if Someone With

Tiny Hands or Sanders dropped out of the race tomorrow," he says, "they're still going to have fans."

Unlike previous figures for real people, like the Robertson family from *Duck Dynasty*, the Pop The Vote concept didn't require a license or approval. "It's a fine line when it comes to real people," Robben says, "but politicians generally fall under fair use because it's considered a parody." And since the company is operating under fair use, it didn't contact any of the campaigns or candidates before Friday's announcement.

But what about the other Republican candidates, like Ted Cruz, Marco Rubio, and John Kasich? We reached out to their campaigns for comment, but got no response. (Presumably all the candidates were too busy staring longingly out a window during a rainstorm, wishing they had been reduced to a 3.75-inch vinyl figure with oversized all-pupil eyes and no mouth.)

Funko won't release the Pop The Vote line until June, and the images it released last week are only 3-D renderings from KeyShot—the figures haven't been physically produced yet. But the dual rise of political engagement during an election year and the popularity of Funko's products is evident—some stores are already accepting pre-orders.

SPACEX'S ROCKET LOSES ITS BATTLE AGAINST A ROBOT BOAT (AGAIN)

SpaceX

The rocket never had a chance. Rocket: zero. Boat: five.

On the fifth encounter between Space's Falcon 9 rocket and its autonomous drone barge, the rocket's first-stage booster tried valiantly to land upright on its rocking, football field-sized landing pad, a barge called *Of Course I Still Love You*. The odds weren't in its favor, after three failed landings and one catastrophic explosion in the air before it got to try. Today, it turned out, was no different.

> Rocket landed hard on the droneship. Didn't expect this one to work (v hot reentry), but next flight has a good chance.
>
> — Elon Musk (@elonmusk) 1:48 AM - 5 Mar 2016

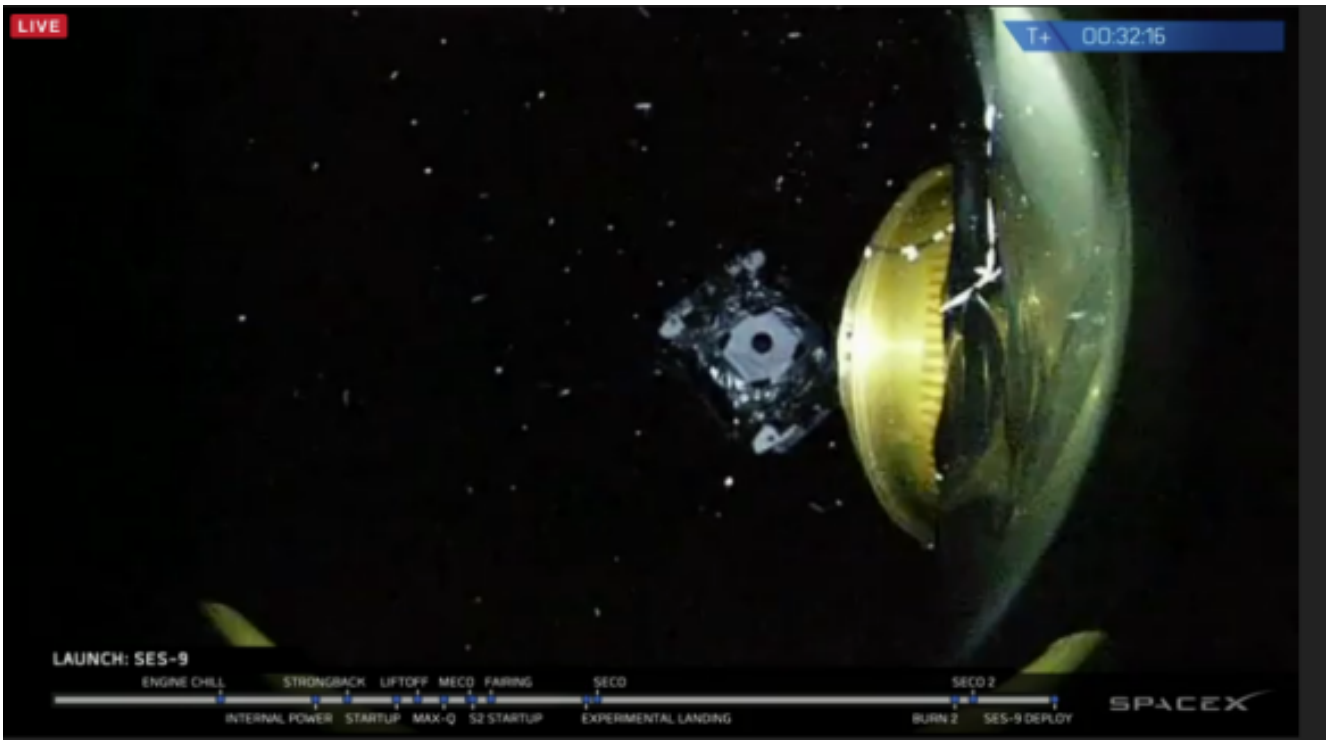
SpaceX kept expectations low for today's landing attempt. (The launch itself had been delayed multiple times, thanks to difficulties superchilling liquid oxygen for the rocket's propellant and an errant boat during Sunday's attempt.) The commercial space company has successfully landed a Falcon 9 on the ground, a historic achievement in December that points toward a future of cheaper, reusable rockets. But landing on a waterborne barge is a different feat altogether. CEO Elon Musk estimated average rocket landing odds back in January:

> My best guess for 2016: ~70% landing success rate (so still a few more RUDs to

> go), then hopefully improving to ~90% in 2017
>
> — Elon Musk (@elonmusk) 5:11 AM - 19 Jan 2016

Despite the failed landing, today's launch *was* a success—because the real mission was getting a communications satellite, SES-9, into geostationary orbit. Recent Falcon 9 launches have only targeted low Earth orbit, like where the International Space Station is. But today's launch sent the satellite into a higher ellipse, locked over a single spot on Earth. Reaching a target altitude of 40,6000 km required greater speeds—8,000 or 9,000 kilometers per hour, compared to previous speeds of 5,000 or 6,000 kph.

You can see the satellite just after the successful deploy below:



SpaceX

The match-ups will just keep coming this year—and every time, the odds of a successful landing get a little higher. (We hope.) Keep watching.

The 4 Most Important Things MythBusters Taught the World

The *MythBusters* have been testing crazy myths since 2003—but now the show is coming to an end. Instead of despair, let's look back at some of the great things we (myself included) have learned from the show.

Everyone Can Be a Scientist

The only MythBuster that had a technical degree was Grant Imahara, with B.S. in electrical engineering. Adam Savage and Jaime Hyneman have a background in special effects for movies. This is what makes them such epic builders.

But here is the awesome part—you don't need a science degree to do science. In fact, I think that science is part of what makes us human (I adopted this from Chad Orzel). Science is just like other activities that make us human: art, music, and emoji (actually, just kidding about the emoji).

Even if you don't know it, science is about building models (conceptual, mathematical, computational) and comparing them to real life. This is exactly what the MythBusters do in each episode. They usually start with a model—such as a conceptual model that says you can play *Fruit Ninja* in real life (yes, that can be a model). Next they compare this model to real data by building an elaborate setup of real-life *Fruit Ninja*.

Finally, this leads to one of three possible results:

- **Busted**: There was evidence collected that leads to believe that the model does not agree with real life.
- **Plausible**: There was not enough evidence to convincingly state if the model agrees with real life.
- **Confirmed**: There was convincing evidence that the model agrees with real life.

Yes, you can make the claim that some of the MythBuster's results weren't thorough enough to make a statement. Again, they aren't professional scientists—that's what adds charm to the show. Imagine redoing the same myths with PhD scientists. I would surely like the show, but it might send the message that "science is stuff *those* people do".

It's OK to Fail

Adam Savage is famous for his quote:

> "Failure is always an option."

In science, you have to build a model. Of course it's unreasonable to expect that our initial models always agree with real life. Just look back at the history of science and see all the times we got things wrong. In fact, being wrong is the norm and not the exception.

The same can be true in the process of learning science. It's just as unreasonable to expect that a student will understand everything right away. This leads to my favorite saying:

> "Confusion is the sweat of learning."

If a learner doesn't get confused, there are a couple of options. Either the person already understood the new material, or they didn't learn anything. You have to be confused to learn just like the MythBusters have to accept the possibility that they will fail. It's part of life. So we should salute the MythBusters and their many epic failures (hello JATO rocket car explosion).

You Can Get Surprising Results

Who would have thought you could get a balloon made of lead to float—but you can. Or what about firing bullets into the air? Are they dangerous? Surprisingly, no one had really tested this before the MythBusters (well, yeah—except for reported injuries, but that wasn't *straight* up). Did you know that elephants might actually be afraid of mice? Yup, the MythBusters did that one too.

The same thing is true in all of science. You never know what is going to happen until you actually try it. Can we detect gravitational waves? Yes, but it took LIGO about 20 years to get it to work. What about falling faster than the speed of sound? Again, yes this is in fact possible.

But it doesn't have to be a grand and exciting experiment to find something new. Just take some sensors and start measuring stuff, you never know what you will find. Here is an other example looking at the energy stored in different batteries (yes, some are cheaper but they also store less energy).

If we always knew what was going to happen in an experiment, why would we do it? That's why I would like to seem different types of projects in the science fair. We shouldn't punish students for trying something that didn't turn out awesome—that gives the wrong impression of science.

MythBusters Episodes Can Lead to Some Fun Blog Posts

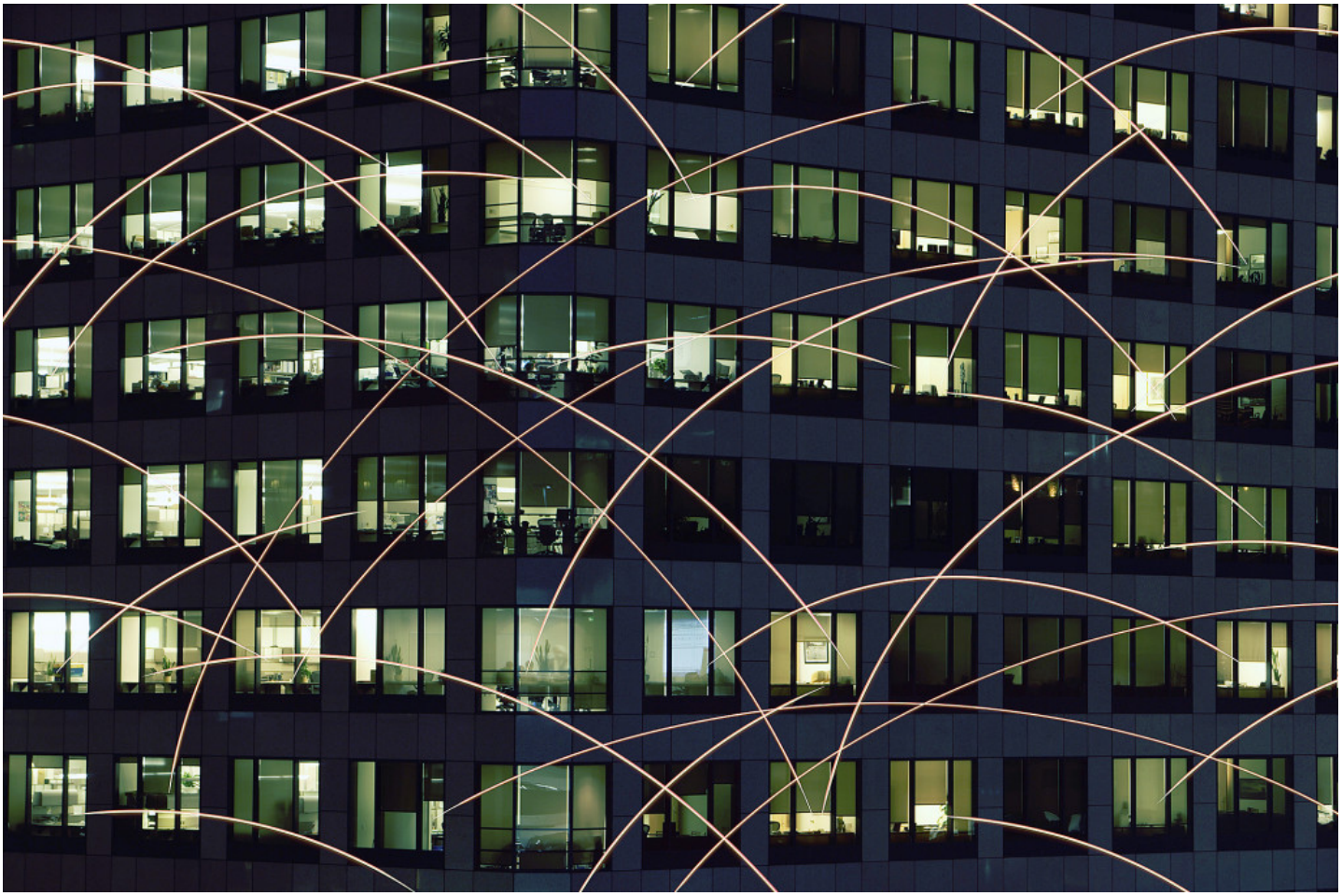
What do you get when you combine excellent building skills and nice cameras (high

speed cameras)? You get the start of some cool blog posts. Yes, I have written about MythBusters quite a few times. Here are some of my favorite posts.

- Make Your Own Tanker Implosion With a Soda Can. This is a simple and mostly safe demonstration of the power of atmospheric pressure. It's fun too.
- What Went Wrong With the MythBusters' Newton's Cradle? Everyone knows of Newton's Cradle as that fun executive clacking balls toy. What happens when you make it really big? It doesn't work—but why?
- Why Did the Rocket Car Break the Ramp? When the MythBusters put a rocket on a car, it broke the ramp as it went up. Why? The answer has to do with momentum.
- MythBusters Physics Homework: Whips and Pendulums. Here is a great example of all the cool questions you can answer from just one episode of the show.
- What Happens When You Double the Speed in a Collision? This is a classic—which would be worse, a 50 mph head collision with another car going 50 mph or a 100 mph collision with a wall?.

That's it. Thanks for all the great physics examples!

The Future of Wi-Fi Is 10,000 Times More Energy Efficient



Get ready to send a thank-you note to students at the University of Washington, where a group of electrical engineers is trying to solve the eternal struggle of Wi-Fi battery drain. It's a problem that's rapidly getting worse as more and more devices require access to the cloud, not to mention the constant strain of searching for a good signal or boosting a weak one.

The student researchers invented a new type of hardware that uses 10,000 times less power than traditional Wi-Fi networking equipment. It's called Passive Wi-Fi, (you can read their paper here) and it works just like a home router, just more efficiently. To give some perspective, the state of the art in low power Wi-Fi transmissions today consume 100s of milliwatts of power, whereas the technology the student researchers developed consume only 10-50 microwatts—10,000 times lower power.

Wi-Fi typically requires two radios to communicate back and forth, and it takes a lot of energy to discern the signal from the noise because there may be several devices using the same frequency (2.4 GHz or 5 GHz). Each device has an RF transmitter that creates a radio wave and a baseband chip that encodes that radio wave with data. With Passive Wi-Fi, instead of each device using an analog radio frequency to receive and transmit a signal, just one produces a radio frequency. That frequency is relayed to your Wi-Fi-enabled device via separate, passive sensors that have only the

baseband chip and an antenna and require almost no power. Those sensors pick up the signal and mirror it in a way that sends readable Wi-Fi to any device that has a Wi-Fi chipset in it.

This may sound a lot like a mesh network, with the signal bouncing from antenna point to antenna point, but it's not. A mesh network uses multiple routers, with full analog RF transmitters and digital baseband chips to receive and rebroadcast a signal.

"The low power passive device isn't transmitting anything at all. It's creating Wi-Fi packets just by reflection," says Vamsi Talla, another student working on the project. "It's a transmission technique that's ultra low-powered, as opposed to a network device."

That "reflection" happens via a process called "backscatter," and the students at UW have created Wi-Fi equipment that sends out a signal via backscatter instead of using a full radio signal.

Right now most devices do not have the backscatter hardware inside of them to send Wi-Fi packets back to the Internet-connected router. But if this technology takes off, it could increase the amount of devices that are connected to the Internet because it nearly nullifies previous energy constraints of making a device Wi-Fi compatible.

To be clear, Passive Wi-Fi still requires running one Wi-Fi router, and Wi-Fi routers aren't super energy efficient. The Environmental Projection Agency even created an Energy Star certification for home networking devices in 2013 to try to encourage the manufacture of less energy intensive devices. According to the EPA's website, "If all small network equipment sold in the United States were ENERGY STAR certified, the energy cost savings would grow to more than $590 million each year and more than 7 billion pounds of annual greenhouse gas emissions would be prevented." The energy savings with Passive Wi-Fi come from the Wi-Fi transmission chipset in devices that communicate via wireless Internet, not the router connected to the initial uplink.

It's hard to say what this will do for your battery life, because there are so many components in a device that impact that—like the screen, for example. "But using Passive Wi-Fi would improve battery life by about as much as turning your Wi-Fi off would," said Bryce Kellogg, an electrical engineering graduate student at UW who co-developed Passive Wi-Fi.

In the future, these passive sensors may even end up in our devices themselves, reflecting packets to send back to the router instead of broadcasting new transmitter waves. For now, using the hardware can reduce the energy used to spread Wi-Fi to devices.

“Our passive Wi-Fi devices now talk up to 11 megabits per second,” said Kellogg. For comparison’s sake, that’s 11 times faster than Bluetooth. One of the main selling points of devices communicating via Bluetooth rather than Wi-Fi has been Bluetooth’s comparatively low energy consumption. But Passive Wi-Fi is 1,000 times more energy efficient than Bluetooth, and the network can be secured like any Wi-Fi signal can, unlike Bluetooth.

11 megabits per second might be faster than Bluetooth, but it’s slower than most home broadband connections. “While backscatter radio technology typically has less range and reliability and lower data rates than active radios, you wouldn’t use this type of communication to watch a YouTube video,” Chris Valenta, an engineer at the Georgia Tech Research Institute told WIRED. “For many Internet of Things applications, however, this technology is perfect. Radios typically account for the largest power draw of any cell phone.”

Wi-Fi hasn’t always been the best choice for connecting our Internet-ready smart devices because of its power constraints. “Communication tends to be a big portion of smart home devices’ power budget,” said Kellogg.

For now, Passive Wi-Fi is a laboratory-controlled research project, but in the future, these passive sensors may end up as part of the ubiquitous hardware construction of Wi-Fi connected devices. That would mean that our electronics would be reflecting packets to send back to the router instead of always broadcasting new transmitter waves to communicate via Wi-Fi. But even now, using the students’ hardware can reduce the energy used to spread Wi-Fi to devices.

“Passive Wi-Fi uses only a few simple components, so it would be very cheap and easy to integrate into existing devices like smartphones or tablets. Additionally, it could even reuse the antenna already inside those devices,” Kellogg added.

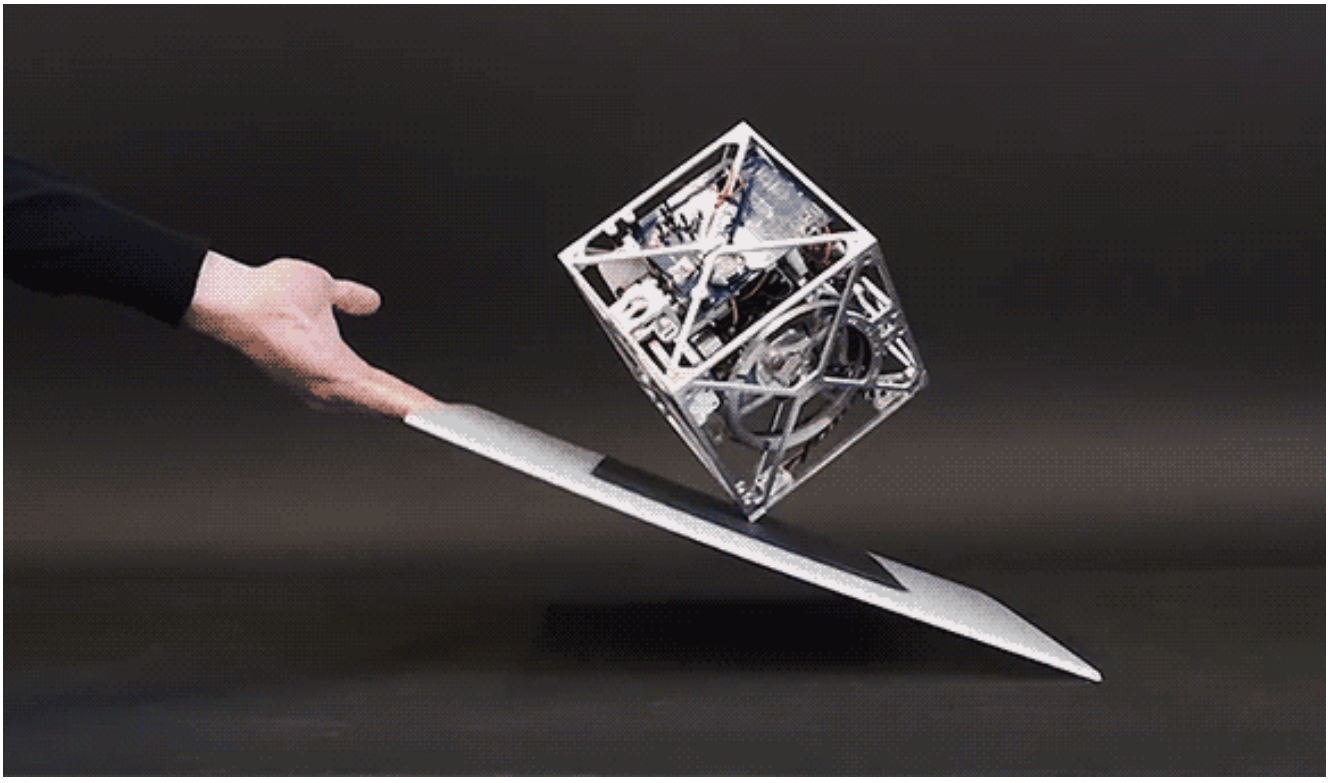
“This type of technology is really meant to reduce the power consumption of the transmitter to enable IoT devices to send small amounts of data back and forth,” says Valenta. As more and more of our smart devices rely on batteries instead of needing to be plugged directly into the wall, conserving battery power will continue to be an important issue with how we use our electronics. And according to the student researchers, companies are already tapping them on the shoulder to see if their vision of a less energy consumptive, increasingly networked world might one day be a reality.

The Master of Drones Turns Flying Machines Into Performers

The TED stage has, for better or worse, become a throne on which our society anoints its intellectual royalty. But Raffaello D'Andrea deserves your attention. At last month's TED conference, he inspired genuine wonder with an 11-minute presentation on "the dazzling flying machines of the future"—that is, drones. His "performers" ranged from an airborne marvel with one moving part, to an eight-propeller juggernaut that could move in any direction it pleased.

D'Andrea, a professor at the Swiss Federal Institute of Technology (ETH Zurich) and the founder of the automation startup Verity Studios, has been experimenting with robots since the '90s. After studying Engineering Science at the University of Toronto and Systems and Control at Caltech, he became a professor at Cornell, where he not only cofounded the university's systems engineering program, but established himself as a dominating presence at RoboCup, the international robot soccer competition. D'Andrea led the university's team to an unprecedented four world championships. He later launched Kiva Systems, a robotics company that was bought by Amazon for $775 million in 2012. Now called Amazon Robotics, the company helps automate much of the company's distribution system.

"I love creating things that move," says D'Andrea, whose childhood science experiments, he says, were frequently of the finger-, hand-, and limb-endangering variety.



The Cubli: the jumping, balancing cube. TED

Today, D'Andrea remains obsessed with objects in motion—though the devices he's known for are decidedly innocuous. Since its formation in 2008, his research lab at ETH has produced, among other things, a robotic chair that falls apart and puts itself together again; and Cubli—a small, metallic cube (pictured above) that can tip itself onto a corner and stay there. By 2009, however, D'Andrea's attention has shifted skyward."The technology had finally caught up to what I dreamed it could do," he says. It was finally time to experiment with drones.

In 2009, the ETH lab demonstrated its "Distributed Flight Array," in which groups of hexagonal drones moved as one, seeming to communicate like birds in a flock. The group's "Flight Assembled Architecture" exhibit, at the FRAC Center in Orléans, France, starred a swarm of flying machines that assembled, brick-by-brick, a 20-foot-tall tower from 1,500 prefabricated polystyrene foam modules. In the "Flying Machine Arena," D'Andrea and his students debuted drones capable of high-speed flips, balancing objects, building more structures (like a rope bridge), and even playing paddle-ball.

D'Andrea's TED presentation, which you can watch in its entirety above, was a taste not only of his work's increasing sophistication and breadth, but of the varied and potential-rich future of drones. None of the prototypes D'Andrea presented on stage was manually controlled. Rather, each was pre-programmed (ETH and Verity built the hardware and software), and equipped with on-board sensors to determine its location in space.

The first drone, the Tail-Sitter, combines the efficiency of a fixed-wing aircraft and the maneuverability of a helicopter. Through a series of algorithms, D'Andrea's team taught it to recover from "disturbances"—an ability he demonstrated on stage by hurling the machine through the air. After each toss, the Tail-sitter would right itself and resume flying as though nothing had happened.

The second drone, a device D'Andrea calls the Monospinner, uses brains over brawn to account for a major handicap: It possesses just one propeller, and no other moving parts. D'Andrea's third creation, the Omnicopter, is the foil to the Monospinner; its eight propellers allow it to travel in any direction without changing where it's orientation, accounting for all possible axes and movements. A fourth invention, the Fully Redundant Multicopter, comprises two double-propeller flying machines joined at the middle to increase performance. A surprise advantage: if one half fails, the drone can stay aloft.

For his finale, D'Andrea presented not one drone, but a "Synthetic Swarm" of 33 tiny, coordinated micro-quadcopters fitted with LEDs, sophisticated programming, and sensors. As they glided soundlessly around the room, they resembled a troupe of

twirling fireflies, artfully syncing their movement and lighting through astounding choreography.

D’Andrea’s flying machines demo at TED. Bret Hartman/Ryan Lash/TED

D’Andrea says his final demonstration was a harbinger of where Verity, which now has 17 employees, is heading: Entertainment, which he sees not only as a lucrative drone business, but a way to ingratiate robotic flight to a skeptical public.

“What better way to show how safe and reliable something is than when it’s engaging people?” he said.

Verity set the stage for drones in entertainment in 2014, by coordinating with Cirque de Soleil on Sparked, a four-minute film in which a team of colorful, lampshade-covered quadcopters dance, hover, and flicker around a stunned performer.

Verity is planning to go much further, says D’Andrea, but the he won’t reveal more details, at the risk of hemming in his research. “I want to be free to create,” he says. Besides, “If you’re doing something that’s cutting edge you shouldn’t be telling people it’s cutting edge,” he says. “People will hear about it.”

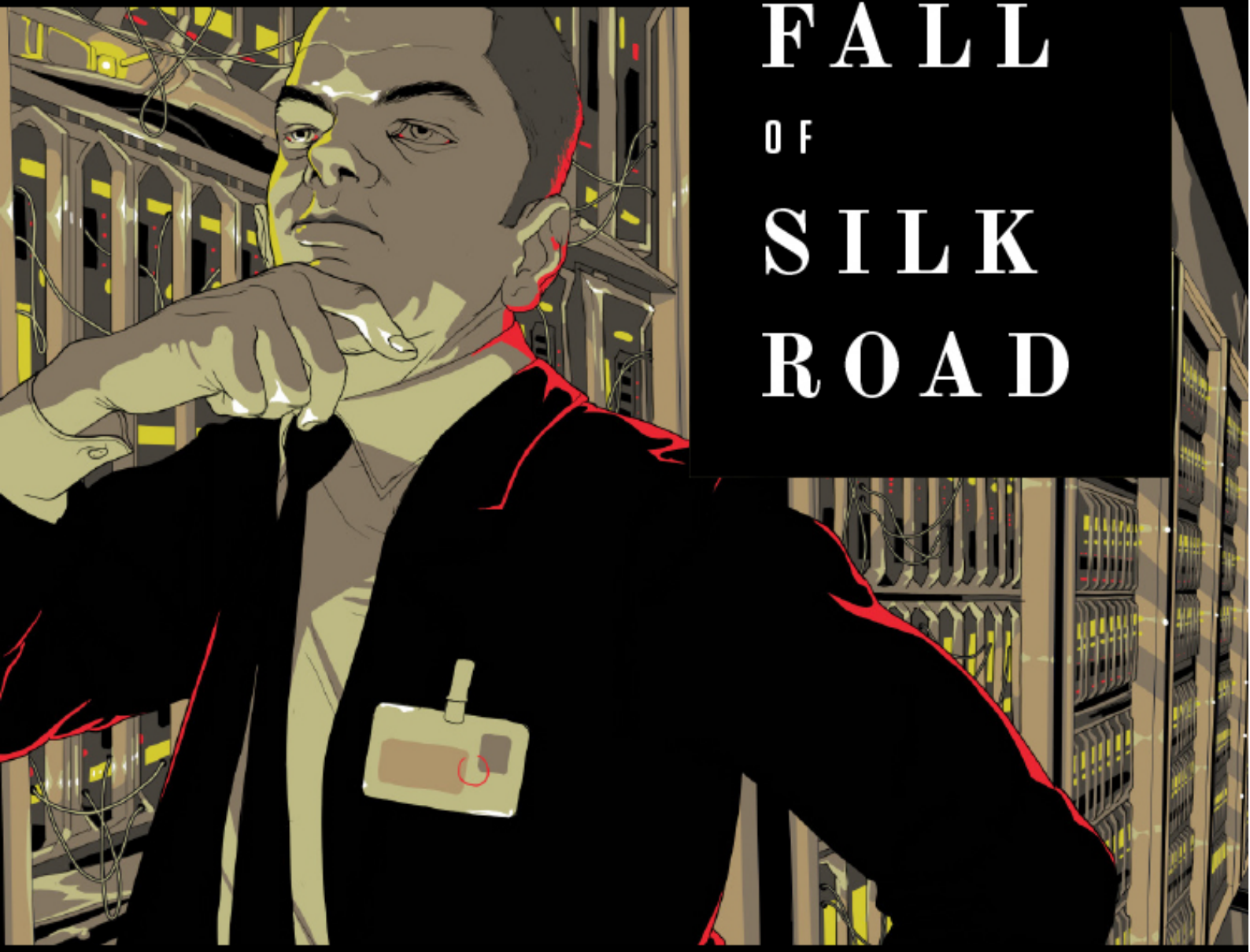
He does give some tantalizing hints: His team is exploring human and machine interaction as well as adaptation and learning. There will be a major reveal in April or May, he says.

“What I care about is using technology to create wonderful things,” he says. “We keep

making new discoveries. We adopt new technologies as they become available and integrate them into what we're creating. He adds: "Ideas are cheap. The hard part is to figure out which ones are worth pursuing, and executing."

Part II

THE RISE & FALL OF SILK ROAD



BY JOSHUAH BEARMAN

TOMER HANUKA

with additional reporting
by Joshua Davis and Steven Leckart

Read part I of this story here.

1

Thor

"I imagine that someday I may have a story written about my life and it would be good to have a detailed account of it." — home/frosty/documents/ journal/2012/q1/january/week1

THE DESCENT WAS stunning. Chris Tarbell, a special agent from the New York FBI office, was in a window seat, watching a green anomaly in a sea of blue as it resolved into Iceland's severe, beautiful landscape. On approach to Keflavík International Airport, he could now see the city of Reykjavik coming into view. And just beyond that, perched on the edge of a moss-covered lava field: the massive matte-white box that housed the Thor Data Center. That's why Tarbell and two US attorneys had come all this way. Thor was the home of a computer with a very important IP address, one that Tarbell and his FBI colleagues had discovered back in New York—the hidden server for a vast online criminal enterprise called

Silk Road.

They'd been working on this case for months, as had federal agents across the country, in a wide-ranging digital manhunt for Dread Pirate Roberts: the mysterious proprietor of Silk Road, a clandestine online marketplace that functioned like an anonymous Amazon for criminal goods and services. Silk Road investigations had been launched by Homeland Security, the Secret Service, and the DEA office in Baltimore, where an agent named Carl Force had been working an undercover identity as a Silk Road smuggler for more than a year.

Tarbell and his team—known as Cyber Squad 2 (or CY2 for short and "the Deuce" for fun)—were relative newcomers to the case. The other agencies had dismissed the FBI, partly because of interagency bluster and partly because the traditional agents who thought casework was all guns and grime and grit had no respect for the eggheads from cybercrime. But in the midst of this enormous law enforcement effort—mostly fruitless so far—Tarbell and CY2 had found the first promising lead in the case.

Cybercrime agents spend a lot of time at their desks, and it was exciting to be in the field. Down below they could see Iceland's fierce geology, all jutting rock built up from the water by volcanoes. Beneath the surrounding ocean are the massive cables that make the country an important location for web traffic; the island is nearly equidistant between North American and Europe, and its forbidding geography and climate reduce cooling costs and provide free geothermal power. One of the attorneys told Tarbell about Iceland's tectonic forces—the North American and Eurasian plates, slowly tearing open a growing chasm. *Really puts you in your place,* Tarbell thought.

Once on the ground in Reykjavik, Tarbell and the lawyers met with their counterparts and explained why they'd come. Silk Road had eluded law enforcement for almost three years because it ran on Tor, a kind of cryptographic camouflage that made it nearly impossible to see the site's users, vendors, or servers. Until Tarbell made a chance discovery.

His investigation had started entirely at his desk with virtual gumshoe

diligence, poking around Tor's IP publishing protocol and spending time on Silk Road looking for chatter about the site's security. His lucky break came from a thread on Reddit: A user posted a warning that Silk Road's IP address was "leaking"—visible to other computers. Dread Pirate Roberts (or DPR, as he was often called) had been alerted to the problem by a user but ignored the warning. Silk Road's success was making DPR arrogant. He had let down his guard, confidently telling colleagues that the site would never be found.

Tarbell threw data at Silk Road, hoping to see the leak. He entered usernames with bad passwords (and vice versa) and pasted data into input fields—all the while using regular old freeware to analyze network traffic and collect the IPs communicating with his machine. Then he tested those. On June 5, 2013, after staring at IP addresses for hours, Tarbell pasted one of them—193.107.86.49—into a browser and suddenly there it was: the Silk Road Captcha field. He showed it to fellow agent Ilhwan Yum and to Tom Kiernan, the civilian computer technician who formed the technical backbone of the cybersquad. This was what the team had been waiting for: a misconfiguration somewhere on the site that revealed the real IP address of Silk Road, which Tarbell proceeded to trace all the way to the state-of-the-art facility in Iceland.

Tarbell had been to the island nation once before and knew some of the officials at the meeting. There was an Icelandic prosecutor present—Tarbell was mildly distracted by how attractive she was, with her fitted skirt, secretary glasses, and hair in a bun—and an attaché from the US embassy. It's a delicate thing, making requests of another government—a US attorney had written up an official letters rogatory petition, requesting that Iceland honor the bureau's investigative requests—but the Icelandic authorities were accommodating, and the meeting was over in an hour. Not long thereafter, an Icelandic police detachment entered the immaculate foyer of the Thor Data Center.

What kind of data center has a foyer? The kind that also has a gleaming glass front and a spotless floor and houses the world's first zero-emission supercomputer. Cybercrime forensics often means untangling wires from machines stuck in some basement. Thor looked like the future. Past the foyer's key card entry was a former airplane hangar in which sat a double-high shipping container, bright blue with silver ducts, full of servers. Inside were three rows of blades lined up floor to ceiling, flashing with blue lights. There was a chill in the air and the thrum of a thousand fans, all powered by Vulcan forces from the rock below. The Icelandic authorities found the correct box and discovered that it had a mirror drive, a duplicate set of contents. They pulled the mirror, returned to Reykjavik, and handed the drive to Tarbell. And just like that, he was holding Silk Road in his hand.

Even on first glance the site's volume was surprising: On July 21, 2013, around the time Tarbell landed in Iceland, DPR's account received 3,237 transfers totaling $19,459, which would give DPR an annualized income of more than $7 million. The data center also kept system logs for six months; they could see all the other computers that had recently communicated with this machine. It was an investigative windfall.

After returning to New York, Tarbell started unspooling the electronic threads that led from the Iceland machine to computers around the world. They looked at traffic recorded for port 22—the encrypted connection where admins log in—and discovered several non-Tor IPs: a backup near Philadelphia, a hosting proxy server in France, a VPN in Romania.

On the wall of the CY2 computer lab, Tarbell mounted an 8-foot sheet of plotter paper and constructed the classic crime investigation visual, with a skein of lines mapping the complicated relationship of leads and evidence. But rather than the traditional godfather surrounded by his capos, this chart centered around a server in Iceland and a sprawling cryptographic computer network.

Tarbell was a visual thinker; he liked to see the connections. One of those connections was to an IP address that was the last known login to the Silk

Road VPN. Next to it Tarbell drew a question mark. A subpoena revealed the IP's physical location: Café Luna, Sacramento Street, San Francisco.

2

Joshua Terrey

WHEN HOMELAND SECURITY agents showed up at Ross Ulbricht's front door in San Francisco, his new roommates were surprised. They thought the quiet guy from Texas who'd just rented their extra room for a thousand bucks was named Joshua Terrey. The agents must have found that interesting, since Joshua Terrey wasn't one of the nine names they'd found in a stash of fake IDs at the Canadian border customs office, all directed to this address and featuring Ross Ulbricht's picture.

Ross had moved into this house after leaving Austin, where he'd grown up as a smart kid from a suburban family with an adventurous streak. Ross was handsome, charming, and always an overachiever, studying physics and engineering on scholarships. But he'd abandoned lab work to pursue an idea that brought together his technical smarts, entrepreneurial spirit, and newfound libertarian social philosophy: Silk Road. He'd come west, to the Mecca of startups, where he managed his powerful operation in secret.

Even though Ross had only recently moved into this sublet in West Portal, a neighborhood of single-family homes and strollers, he'd scored the master bedroom. His roommates thought that the guy named Josh, who had answered their Craigslist ad, was a currency trader. They did think it was weird that he had no cell phone, paid in cash, and was always on his

computer. Neither friends nor family had any idea that Ross had a secret alter ego: Online he was Dread Pirate Roberts. Nor did they suspect that the young man who ran what began as a politically motivated black market had become the leader of a criminal organization, a ruthless operator who had decided to kill one of his employees as retribution for theft (and as a sacrifice necessary to protect his political objectives).

If Ross was nervous about being discovered when the Homeland Security agents interviewed him, he didn't show it. He did not tell them he'd bought the colorful array of fake IDs so that he could covertly rent additional servers to deal with Silk Road's exploding scale and security challenges. The IDs were high-quality counterfeits, holographic features and all. But now they were in the hands of the Homeland Security agents at the front door. Ross was polite but knew he could refuse any questions.

Before the agents left, Ross did volunteer that "hypothetically" anyone could have shipped drugs or fake IDs to him via a website called Silk Road. A strange thing to mention—and duly noted by the agents—but they weren't there to talk about Silk Road, whatever that was. The agents left and took the fake IDs with them.

Ross was spooked by the visit. He moved again a short time later to another sublet, in the city's Glen Park neighborhood, but decided to use his real name. One of his new roommates, Alex, liked Ross right away because he was charismatic and easy to talk to.

RELATED STORIES

Want to See Domestic Spying's Future? Follow the Drug War
BY ANDY GREENBERG

New Dark-Web Market Is Selling Zero-Day Exploits to Hackers
BY ANDY GREENBERG

The Darkest Place on the Internet Isn't Just for Criminals
BY CLIVE THOMPSON

And, Alex observed, Ross' focus was impressive. He wasn't the type of guy to procrastinate watching cat videos on his Samsung 700z. He didn't smoke or drink much, although he sometimes played his djembe, a west African drum and one of his few possessions. He never brought friends over and seemed not to have a single memento. Nor did Ross get mail. "Sometimes," one roommate said to Alex, "I feel like Ross is hiding from someone."

Still, they couldn't have guessed that Ross, the new guy in their cheap share who liked giving hugs and hanging out shirtless, was sitting on their garage-sale furniture with that Samsung on his lap presiding over a criminal empire.

"MONEY IS POWERFUL," DPR wrote to the Silk Road faithful, "and it's going to take power to effect the changes I want to see." By that time, DPR was a millionaire many times over, but those resources, he told his followers, were for the revolution. Freedom, after all, needs financing.

DPR had founded Silk Road as a digital instantiation of the libertarian

3

Uneasy Lies the Head

ideal: a frictionless marketplace where everyone had freedom as long as it didn't impinge on someone else's freedom. For DPR and the community that grew around him, Silk Road was about more than contraband; it was a movement. As Silk Road quickly grew, DPR's pronouncements became more grandiose. He wrote that "every single transaction is a victory" in weakening the "thieving, murderous" state. What began as a belief in free choice came to sound like revolutionary dogma.

It made for ambitious business plans. DPR wanted to expand his liberty-fueled brand into an empire, with his own Silk Road–affiliated bitcoin exchange, credit union, and encrypted communication service. Buoyed by quick success, DPR shared the heady enthusiasm of the licit startup world. Whereas he'd once considered selling Silk Road for $1 billion, he told a reporter in a rare, encrypted chat interview that Silk Road was worth 10 figures, maybe 11.

But behind the scenes, Ross faced constant crises. There were technical problems, management issues, a quickly changing marketplace, and the volatility of bitcoin. There were scammers on the site. And even as Silk Road made more money, the cost to maintain it rose. Ross, feeling besieged from all sides, recorded his efforts in a log.

04/03/2013

Spam scams have been gaining traction. Limited namespace and locked current accounts.

Blackmail too was a problem. Hackers had figured out how to launch denial-of- service attacks on Silk Road, and DPR was forced to pay "protection" to the tune of $50,000 a week. In May 2013, hackers shut down the site for a week, and many users wondered if it was the work of a competitor. Atlantis, a new Tor-based illicit-goods bazaar, had just launched with a slick YouTube trailer and a group chat with reporters in which a spokesperson named Heisenberg offered the serious burn that Atlantis was the "Facebook to [Silk Road's] MySpace."

05/02/2013

Attack continues. No word from attacker. Site is open, but occasionally tor crashes and has to be restarted.

DPR's own staff was growing, although it was hard to find reliable subalterns. Batman73—a dealer named Peter Nash in Australia—was a cokehead. Inigo ran the site's book club, which DPR appreciated, but was the kind of guy who lived part-time on a boat, smoked a lot of weed, and was as organized as that lifestyle might suggest. DPR liked Libertas, though, and Smed was solid, offering rapid-response technical support.

05/03/2013

Helping smed fight off attacker. Site is mostly down. I'm sick.

The burden of leadership was getting to DPR, and his fluctuating moods played into the theory that the moniker was actually operated by multiple people. DPR encouraged this perception. In an interview with *Forbes*, he said that he was actually the successor to Silk Road's creator. It worked. On

Silk Road it became great speculative sport to decipher the many facets of DPR, with users believing they could even detect when the different DPRs took the reins.

“You are a busy guy. Actually I think you are going to kill yourself,” said a friendly message sent to DPR by a Silk Road vendor named Nob. “Take a vacation.” DPR believed that Nob was a Puerto Rican cartel middleman named Eladio Guzman, but he was in fact DEA agent Carl Force. Force had spent more than a year developing his undercover identity on Silk Road in an effort to get close to DPR. They’d become confidants, spending nights chatting at such length that DPR trusted Nob when he needed enforcement muscle.

It was Nob whom DPR hired to kill his employee, Curtis Green. Force then coerced Green into faking his own death as a ruse. Force was surprised to see DPR’s moral collapse up close, but then again, he’d seen this kind of thing before, during his younger DEA years in undercover. He too had experienced the temptations that came with a double identity. In fact, his secret life as a hard-partying operator had nearly destroyed his regular life. He’d left all that behind and recommitted himself to Christ. The Silk Road case was his first undercover role since those days, and it was a big one. Because of his tenure online as Nob, Force was able to carry out the supposed “hit” on Green, setting DPR up for a murder conspiracy indictment while at the same time cementing their relationship. Nob and DPR had become comrades-in-arms.

Now Nob wanted to capitalize on DPR’s apparent struggle. “You need a contingency plan,” Nob wrote. Force hoped that the mounting paranoia would eventually allow him to orchestrate what DPR would believe to be an escape—right into the arms of the DEA.

DPR confided his worries about “LE,” or law enforcement, not realizing

that he was talking to the DEA. That might have been a lapse in judgment in a realm that was full of speculation about narcs and informants. But DPR wanted to believe his friend Nob. Silk Road, after all, was built on DPR's confidence system. And besides, he was lonely. "I have no one to share my thoughts with," DPR posted to the wider Silk Road community at one point. "Security does not permit it, so thanks for listening."

05/26/2013

Tried moving forum to multi .onion config, but leaked ip twice.

DPR had also gotten lazy with his operational security. That diary he kept was a bad idea, for starters. Growing vanity had become a weakness. DPR's self-taught programming was catching up with him as well, leaving holes in Tor's invisibility cloak. And yet he would tell his admins there was nothing that could get traced back to them. When one user with a technical background private-messaged DPR to warn him that he should know the precise physical location of his servers, DPR brushed it aside. The tipster warned that the servers could be copied easily. Don't worry, DPR said. The servers are secure.

4

Lab1a

BACK IN NEW York, Kiernan was busy re-creating the entire Silk Road system in their lab. Once it was configured, Tarbell and his team could

access the system as superusers—seeing Silk Road as DPR—and learn the site's mechanics, communications, and structure. It was thrilling, of course, to fire it up for the first time. They wondered what they would see. Tarbell could immediately appreciate DPR's sense of industry, how hard he worked to expand and manage the site under incredible duress. Tarbell thought: *I guess he's really earning that commission*.

It was impressive. Especially because Tarbell could tell that DPR was not a professional programmer. The server was a "noisy box," clearly the work of an autodidact, a coding palimpsest that invited eventual discovery. The pseudo code was full of comments describing various technical experiments that were often run on the live server. Kiernan and Yum found the private messages, the forums, a bitcoin escrow account (from which DPR extracted his cut every Saturday night), and the main bitcoin server showing all vendor transactions.

They spent a lot of time in the lab, which they dubbed the War Room. It felt like college finals week in there, every day. The group would churn through Silk Road material, bringing lunch in from the deli downstairs and getting loopy by the afternoon, when Tarbell would call for a seltzer break and dance around with the bottle, singing the mellow gold classic "Afternoon Delight." Over time the jokes got weirder, like when Yum put up a sign in the War Room that said: Lab1a. To the delight of the cybersquad, no one in the computer-illiterate realm of the FBI noticed that this was also leetspeak for some sensitive lady parts.

While Yum and Kiernan worked on the machines, Tarbell combed through 1,400 pages of DPR's chat logs so as to really understand him. DPR was different things to different people, sometimes solicitous and businesslike, other times volatile and narcissistic. Eventually, he embraced murder as a necessary business practice.

Reading through DPR's correspondence, Tarbell was surprised to find evidence of more hired assassinations, this time a response to blackmailers. It was a complicated scenario, but what Tarbell put together was that a user called FriendlyChemist was blackmailing DPR. Another

user called Redandwhite, claiming to be a member of the Hells Angels, agreed to kill the blackmailer and, soon, others. For a handsome fee, of course.

DREAD PIRATE ROBERTS 3/27/2013 23:38

In my eyes, FriendlyChemist is a liability and I wouldn't mind if he was executed ... I have the following info:
Blake Krokoff
Lives in an apartment near White Rock Beach
Age: 34
Province: British Columbia
Wife + 3 kids

Always the businessman, DPR first invited the Hells Angels to become vendors on Silk Road, suggesting that Redandwhite "read the wiki and forums." Then the two got back to the cost of murder. Hit men apparently get a commission, according to this Hells Angel, if the target owes money. And if you want it to look like an accident, rates go up. A "clean hit" would cost about $300,000 (travel expenses included). DPR had sticker shock. After all, he'd only paid $80,000 for the Curtis Green hit. They haggled.

DREAD PIRATE ROBERTS 3/31/2013 8:59

Don't want to be a pain here, but the price seems high. Not long ago, I had a clean hit done for $80k. Are the prices you quoted the best you can do?

REDANDWHITE 3/31/2013 11:16

I'm sorry, but we can't do anything for that price. Best I can do is 150 and even that is pushing it.

In the interest of a "business relationship to be" the Hells Angels agreed to $150,000, or 1,655 bitcoins at the time. "Good luck and be safe" was DPR's sign-off. The next day they debriefed.

REDANDWHITE 4/1/2013 22:06

Your problem has been taken care of … Rest easy though, because he won't be blackmailing anyone again. Ever.

DREAD PIRATE ROBERTS 4/2/2013 00:55

Excellent work.

Tarbell had never seen anything like it. Here was a date- and time-stamped record of an entire criminal conspiracy as it unfolded. Turned out, Redandwhite told DPR, the blackmailer they killed was working with another guy known on Silk Road as Tony76, an infamous scammer. DPR didn't hesitate to add him to the invoice. But Tony76 had housemates, and they were also involved. Maybe. Probably. Fine, DPR said. Get them too, and send photographic proof when the job is done. Meanwhile, DPR and Redandwhite spent some time troubleshooting the Hells Angels' new chat app and privacy plug-in ("Please upload some screenshots of the settings") while also planning and pricing ("no bulk discounts") the next set of executions.

DREAD PIRATE ROBERTS 4/8/2013 18:50

I see your problem, you need port 9150, not 9151 … hmm … $500k in btc (3,000 @ $166/btc) has been sent to: 1MwvS1idEevZ5gd428TjL3hB2kHaBH9WTL

A week later:

REDANDWHITE 4/15/2013 10:11

That problem was dealt with.

Tarbell had been reading DPR's correspondence in reverse order, and it was a strange thing, winding DPR's life backward, from willing executioner back into idealist concerned with individual happiness. Some libertarian utopia, Tarbell thought. Although he wasn't exactly surprised. All systems

are vulnerable to corruption. Like the Internet itself, Tarbell thought, which began as a wonderful free prairie until people took advantage of that freedom. That's why, he thought, it needed a sheriff. Up on Tarbell's chart was an IP address with a name next to it: Frosty. This was an ID they'd found on the Iceland box. But they didn't know what it meant until Yum and Kiernan cross-referenced it with some other evidence they'd collected. It turned out that the Silk Road servers had a login system that created one trusted computer for all the other machines, whose encryption keys all ended with frosty@frosty.

This meant that these computers shared one key friend, a single machine they could all talk to. Tarbell looked at his chart, festooned with a network topology. One of those nodes must be Frosty, and whoever sat at its keyboard was Dread Pirate Roberts.

As the case accelerated, Tarbell and his team started working long hours and weekends, jackets off, sleeves rolled up, long past the late dusks of summer. Tarbell actually loved that feeling on Friday at 5 pm when the air conditioner turned off automatically, the bullpen emptied and grew quiet, and he realized he'd been yelling all day but could now finally think.

Except that it was high summer. This being a federal building, the air-conditioning was on a timer. There'd be no circulation until Monday at 8:15 am. So by midday on Saturday, when the place was boiling, Tarbell would strip down to his underwear right at his desk.

The only room with constant air-conditioning was the lab, which had to be cooled because of the electronics. So one day, Tarbell and Yum made a desperate attempt to transport some of the chill to their desks using fans. It kind of worked. And there they sat in the middle of the FBI office, Tarbell sweating in his skivvies, with a football game on in the background and a series of fans stretching back to the well-cooled room where the ersatz Silk

Road server hummed along, still keeping one key secret.

5

Glen Park

ROSS AND ALEX had become friends at the new house. Some nights they'd watch *King of the Hill* together, which reminded Ross of home, as it was a satire of a suburban Texas family like his own. Eventually Alex met that family when they all visited for a weekend. Ross' parents seemed like nice folks who had raised a nice son. Settling into his room, Ross bought a few things to make life more comfortable: a lamp, a white leather couch from a garage sale, a standing desk for his Samsung. Online, however, things were less settled.

Across the country, Force, the DEA agent, was hoping to capitalize on DPR's difficulties. He told DPR about "Kevin," a supposed source of counter-intelligence on the growing Silk Road investigation. Nob explained that like all good cartel-affiliated players, he had "a guy on the inside," a dirty Department of Justice employee on his payroll. Kevin, of course, was Force himself, and he had a lot of valuable information for DPR. Force told his supervisors that this informant game would make Nob seem omniscient and therefore more trusted. Citing Kevin, Nob fed DPR intel and predicted busts of Silk Road users and vendors. Things were getting dicey out there, Nob said. He pressed DPR on the need for a "30 seconds flat" escape plan, suggesting various itineraries.

DREAD: Can you explain to me why you chose this route?

NOB: Algeria does not extradite to the US.

NOB: Second you don't want to take a plane out of your mother country.

Ross had in fact taken some preparatory steps. He flew to Dominica, a tiny tax haven island in the Caribbean, and started an application for "economic citizenship." He tried to cultivate successors in case flight became necessary. DPR had created a special forum called Staff Chat for his elite admins, including Batman73, Inigo, and a newcomer called Cirrus. DPR told his admins how the pressure was getting to him, how he wanted time away. Even amid the rising chaos swirling around Silk Road, DPR started taking days off, leaving daily operations to his lieutenants. Ross spent a weekend with his old flame Julia, a free-spirited and sensual young photographer he'd met at a drum circle in grad school.

RELATED STORIES

Silk Road Judge Denies Retrial Despite Agents' Alleged Corruption
BY ANDY GREENBERG

Silk Road Boss' First Murder-for-Hire Was His Mentor's Idea
BY ANDY GREENBERG

DEA Agent Charged With Acting as a Paid Mole for Silk Road
BY ANDY GREENBERG

She flew in from Austin, and it felt like old times for the two of them, but also different. Ross still lived frugally in the Glen Park house, wore a faded red sweater all the time, and cooked his paleo diet, but he seemed happier. They had lots of sex, went dancing, and roamed the city, ending up one day on the cliffs overlooking the Pacific. In the distance, the Golden Gate Bridge rose beneath the lifting fog, catching the sun. Julia looked gamely

over her shoulder at Ross and decided it was a good time to get topless. She rolled down her yellow sundress and Ross took photos. She didn't care when a couple of hikers stumbled onto their soft-core pictorial. Ross stopped shooting and they ran off together, giggling, back toward the city.

Ross started spending more time with his housemates. One day he went to a nearby park with the girl who lived across the hall and hung out on the grass with her and her two long-haired Chihuahuas.

Marring the greenery, Ross noticed, was a piece of blue plastic stuck in a tree. A dedicated anti-litterbug, Ross climbed up to retrieve it. Back at the house he discovered he'd gotten a bad case of poison oak and needed plenty of calamine lotion for the spreading rash. He moped for days, still shirtless, but now bright red, standing out like a squad car's flasher against his white leather couch.

THE WHEELS OF the federal government grind slowly but exceedingly fine. As Ross had written in his diary in 2011, when Silk Road came to the attention of the US Senate, he knew he had awakened "the biggest force-

6

($curl_error)

wielding organization on the planet." Two years later, Chris Tarbell was lying on his bed at home, with his wife, Sabrina, cooking in the other room and his kids tearing around the house so loudly he had to turn up his phone to hear the name: "Ross Ulbricht."

Tarbell was on a conference call with the US attorney assigned to the case and an agent from Homeland Security Investigations named Jared Der-Yeghiayan. Der-Yeghiayan was stationed at the customs office in Chicago's O'Hare International Airport and had been finding retail-size drug parcels in mail on foreign flights, all carefully wrapped, with customer service slips and return addresses to StudyAbroad.com. This, Der-Yeghiayan discovered, was a vendor on a thing called Silk Road.

Der-Yeghiayan familiarized himself with the site and learned Silk Road well enough to bust a low-level admin named Cirrus and persuade her to cooperate, allowing him to take over her account. Now Cirrus was rising through the ranks, becoming a trusted insider. Tarbell invited Der-Yeghiayan to New York to work with CY2.

Another new agent from the IRS, Gary Alford, had joined the conversation that day. As it happened, he'd been in Tarbell's War Room earlier—Alford and the US attorney were working on a separate bitcoin case—and he'd taken a quick look at the chart. "Oh, that's funny," Alford said. He had worked with a different agency on Silk Road for a bit. "I had a lead in San

Francisco," he told the team. "I'll look it up."

He did and then explained to everyone what he'd found. Some months earlier, Alford had figured that whoever had started Silk Road had tried to drum up interest on regular websites with like-minded audiences. He searched for Tor URLs around the time of the site's first appearance and found a mention in a Shroomery.org forum on January 27, 2011, days after the Silk Road launch. A user named Altoid talked up this exciting new "service that claims to allow you to buy and sell anything online anonymously."

Googling elsewhere for the username Altoid revealed a question about database programming posted on Stack Overflow, dated March 16, 2013, asking, "How do I connect to a Tor hidden service using curl in php?" The email listed was *rossulbricht@gmail.com*. A minute later, that user changed the alias to Frosty.

The IRS didn't know what any of this meant, so that's where it ended. The info sat in a case file until dumb luck put Alford in Tarbell's lab, whose wall was a map where all roads led to Frosty. Der-Yeghiayan ran the name Ross Ulbricht through the federal database and found the Homeland Security report on Ross' fake IDs. A quick search for his last known address showed that he had lived half a block away from Café Luna, the San Francisco node on his chart (the site where an administrator had logged in to the Silk Road VPN).

Tarbell was ecstatic. Finally, here was the missing piece, the end of the digital trail. Tarbell thought it was funny that these clues were sitting out in the open. In the end, one of the best law enforcement tools was Google. It seemed clear that Ross had no idea Silk Road would become such a success and was careless early on. And in the era of informational perpetuity, you only have to be careless once.

A quick tour through Ross' social media presence revealed a digital portrait with an incredible likeness to Dread Pirate Roberts'. His LinkedIn profile was full of the same libertarian rhetoric. On YouTube he'd favorited videos from the Mises Institute, the political touchstone beloved by DPR.

On Google+ (where his profile described him as “spunky, funky, not so chunky”) he asked, “Anyone know someone that works for UPS, FedEx, or DHL?” In the lab, Kiernan found code on the Silk Road server that matched lines posted by Ross on Stack Overflow.

“We found the guy,” Tarbell told his department supervisor the next day.

They put in a request to the surveillance team to send two agents to San Francisco, to get eyes on Ross. They watched him, in that house he shared with Alex, working late on encrypted wireless. Sometimes he headed out with his laptop, like practically everyone else in San Francisco, and occupied a café table to work with coffee at his side.

An electronic wiretap on Ross’ email would require a court order—but at that point there wasn’t probable cause to search the account. So they decided to use the physical surveillance to see if they could line up Ross’ Internet usage with DPR’s activity on Silk Road. The activity matched; DPR and Ross were in lockstep. Every time Ross turned on his computer, DPR logged on to Silk Road. When he closed it, DPR logged out. Over weeks, the pattern was consistent. At his house, in cafés, in the morning or late evening, Ross and DPR were electronically aligned. When DPR would say he was taking the afternoon off, physical surveillance would watch Ross going to the park with his housemate and her Chihuahuas, lying on the grass, and getting poison oak by climbing into a tree to pull some blue plastic from the branches.

Tarbell started planning. This would be a complicated operation, seizing the site’s bitcoins undetected, taking control of Silk Road, and placing FBI people abroad—at the machine in Iceland and at another in France. Tarbell was also worried they might accidentally tip off Ross. He even wondered why Ross hadn’t bolted already. Der-Yeghiayan, online as Cirrus, was in DPR’s inner circle and knew that he was feeling extreme pressure. Tarbell

thought Ross was clearly smart enough to get out while he could. In fact, Force, as Nob, was actively encouraging DPR to flee. Force had been sidelined, but his final play was to convince the digital kingpin to meet him at some airport, under the guise of providing safe passage, and take him into custody. To juice DPR's flight instinct, Force pointed out that were he to be caught, prison would not be a safe place.

NOB: You are like one of my family. But I have to tell you that i have had several people killed who were sent to jail. It is very easy and cheap.

But Ross wasn't going anywhere. His hubris had only grown, based on his belief in Tor and his own intellect. He thought he was invincible. Even as warning signs flashed all around him and the Feds loomed on the horizon, Ross told a potential employee that they would never get caught. "Realistically," he said, "the only way for them to prove anything would be for them to watch you log in and do your work."

On the evening of September 28, the FBI's surveillance team watched DPR log off as Ross stopped working, closed his computer, left the house with his housemates, and headed for the beach.

7

Stay Positive

IT LOOKED LIKE a brochure for San Francisco living, a group of kids

sitting around a campfire at Ocean Beach beneath a crescent moon, listening to their friend Ross play his djembe. This was the first weekend of Indian summer, that glorious time in San Francisco when everyone ventures outside and you can sit in the sand within sight of Golden Gate Park and listen to the dark waves crash on the shore. Alex opened champagne, and Ross drank Tecates and drummed along with a dude playing "Wonderwall" on a guitar in the distance.

Toward midnight, the soiree was interrupted by three cops who told them to kill their fire. No bonfires after 11, they said. The group brought the party back to their house in Glen Park, drinking on the balcony. The guys in the next house over were on their balcony too, sharing some sangria, and passed a glass to Ross. He picked up Clementine, one of his housemate's Chihuahuas, and cradled her in his scarf like a baby in a sling, toting her around while still drinking. Ross was blotto—the only time Alex saw him drunk—and smiling.

"Let's go inside and jam," Alex said. And jam they did, with Alex on the piano, Ross knocking his djembe again, and some other friends singing. The music settled into a hypnotically repeating melody, as late night jams do, until everyone drifted back to their rooms or out the door. "Ha," Ross said, hand on his drum. "I can't keep time."

Online, Ross' stewardship of Silk Road was also off-balance. He recorded his troubles in his log. Law enforcement was trying to infiltrate the forums. Some big vendors were getting busted. He was hemorrhaging money, starting with a government seizure of $2 million that May from Mt. Gox, the world's biggest bitcoin exchange, where some key Silk Road accounts were held. Unrelated, Redandwhite convinced Ross to give him $500,000 and then disappeared. Even his friend Nob was still making veiled threats about how easy he would be to kill in jail.

Amid the chaos, DPR did talk to Libertas, one of his most trusted admins, about taking over Silk Road in case of emergency, but he never gave him server access. As he tried to keep his fingers in the dike, DPR confided his worries to Cirrus, who by the end of September was briefing a massive FBI

team in San Francisco alongside Tarbell and Kiernan on the looming arrest of Ross Ulbricht.

If Ross knew the noose was tightening, he didn't show it. In the days after the Ocean Beach party, he worked at his standing desk and called Julia in Austin, telling her he was going to visit in November. She sent him sultry photos, naked and dancing, as a preview. That Monday night, Ross wrote in his diary: "Had revelation about the need to eat well, get good sleep, and meditate so I can stay positive and productive."

8

/Mastermind

THE DINING ROOM of the San Francisco Airport Marriott was nearly empty at 6 am on Tuesday, October 1, 2013, when Tarbell met Kiernan and Der-Yeghiayan for another mediocre breakfast. Tarbell hadn't slept much since arriving in San Francisco two days earlier. He and his New York team were edgy, having been in position waiting on the right moment. There was, as usual, a bureaucratic complication. Silk Road was Tarbell's case, but he and CY2 were visitors at the pleasure of the San Francisco FBI office, and it was their assistant special agent in charge who had, as cops say, "designed the arrest."

In classic form, the local FBI wanted to mount a dramatic raid on Ross' house. Tarbell didn't like this idea. He was worried about repeating the mistake made during his first big cybercrime case, when they arrested a hacktivist named Jeremy Hammond in Chicago. There, a SWAT team

charged into Hammond's apartment throwing flash grenades, immediately alerting Hammond in the back room, who shut the lid of his laptop, encrypting it forever.

This kind of operation didn't need SWAT, Tarbell thought. It required finesse. To prosecute a cybercrime you needed direct evidence, which centered around Ross' machine. Tarbell wanted to get Ross *in medias res*, with "fingers on the keys," as they say in the trade. Tarbell had read in DPR's chats about how secure his system was, how one keystroke would erase it all. There was no margin for error. They needed complete surprise.

Still, the assault strategy remained in place. "Thank you for your input," the local FBI supervisor had told Tarbell. "Now here is the plan." There would be three SWAT teams, one for each floor of the house. They would hit at dawn, gaining "fluid entry." They couldn't promise, but they would try to catch Ross while he was online.

"These are the fastest SWAT teams," the supervisor said.

"But it doesn't matter," Tarbell said. "No one is fast enough."

The arrest had been scheduled already, but Tarbell kept asking to delay so that they could catch Ross at one of his cafés. They'd seen him out working once but didn't have "assets in position." Tarbell was granted one delay, but that was it.

"Your equity is used up," the San Francisco chief said. "No more favors."

The SWAT assault was scheduled for 5 am on Thursday. The entire tactical force—dozens of agents—had gathered at an FBI cybercrime facility an hour south in San Jose, prepping their final review.

TARBELL DIDN'T MAKE it to San Jose. He and Der-Yeghiayan stopped by the San Francisco federal court building to amend the search warrant for Ross'

house. Kiernan and another officer were still in San Francisco as well, near Ross' house in Glen Park. They had stayed in position, hoping, praying that Ross would come walking out that door with his laptop bag over his shoulder.

Tarbell decided to meet his team at Bello Coffee & Tea, a place Ross frequented just next to the Glen Park Branch Library. It was 1 pm. Sitting on the bench outside the café, Der-Yeghiayan went on Silk Road as Cirrus and saw that DPR was also logged in. Physical surveillance said Ross was still at home. Tarbell worried that in this leafy patch of San Francisco, he and his completely cop-looking crew, sitting around one laptop, would stand out. The group scattered and tried to act casual. Der-Yeghiayan went to a nearby market but then noticed his computer was nearly out of juice. So he went back to Bello, only to find the place full, with no free outlets. Tarbell returned to the bench, getting a chance to do some more worrying.

Halfway across the Atlantic, Yum was with the Icelandic authorities, poised to enter the Thor Data Center and "escalate privilege" over the Silk Road marketplace and bitcoin servers. Then the team in France would take over Silk Road's redirect server. Tarbell barely noticed the pleasant afternoon, instead staring at his BlackBerry, monitoring the constant scroll of messages tethering this whole delicate operation together.

At 2:45 pm, Der-Yeghiayan saw DPR log off. A few minutes later, Tarbell heard from surveillance: They had eyes on Ross leaving his house. He was wearing jeans and his red sweater and walking east. And carrying his computer. "He's on the move," they said.

Holy fuck! Tarbell thought. *He's coming*. CY2 scattered again, this time in a giddy panic, zigzagging for cover like in a game of hide-and-seek. Tarbell left Der-Yeghiayan, still holding his laptop, to head down the street in the direction of Ross' house. He felt high from the adrenaline. He didn't realize Ross was on top of their position. Tarbell was rereading Ross' description from the surveillance team when he looked up and saw Ross heading directly toward him. It felt like slow motion, coming face-to-face with the man he'd been tracking for months, resolving him from digital obscurity

into a real live person walking up Diamond Street. Tarbell worried he'd get made. He was trying to act all Mister Undercover, but, Jesus, did he look like a cop. Ross walked right past him toward the café.

FROM ACROSS THE street, Der-Yeghiayan saw Ross duck into Bello. This seemed promising; they'd been hoping he'd sit down somewhere and log on to Silk Road, giving them an opportunity for a red-handed arrest. But Ross quickly left. It was probably the lack of outlets, Der-Yeghiayan imagined, looking at his own computer, which now had only 22 percent battery power left. A scary number, as he had to be connected online to verify DPR's presence. Ross walked into the library next door.

Oct 1, 2013 2:53 pm
From: Chris Tarbell
Subject: Re: Ross Ulbricht

By email, Tarbell alerted his team. That message cc'd the whole operational group, which was midbrief, preparing for their raid, when they learned that the little squad of out-of-towners had ventured off-piste and cornered their man in the Glen Park Library. "We got him," Tarbell said when his supervisor called from New York. "I'll call you back in 10 minutes."

With Der-Yeghiayan's dying laptop, they watched Ross log on as DPR, then navigate into the marketplace, then the forum, then the elite admin chat where Cirrus was waiting to say hello. Tarbell knew the chief down south had surely mobilized. Fifty tacked-out federal agents were racing up Highway 101.

The cavalry was coming, and Tarbell wanted to get Ross before sirens

showed up.

Kiernan and another agent had been in the library when Ross walked in. He went right by them and continued unaware past the periodicals and reference desk, beyond the romance novels, and settled in at a circular table near science fiction, on the second floor. The other agent assessed the tactical landscape up there, which was tough: Ross was sitting in a corner, with a view out the window and his back toward the wall. There was no obvious approach. It was Kiernan's job to get Ross' laptop, and it looked tricky. "Your sole job is to get the laptop," Tarbell had drilled Kiernan. "Get the laptop. That's why you're here. Get the laptop. And keep it alive."

TARBELL AND DER-YEGHIAYAN joined the action in the library, taking a spot on the stairs at a landing. Der-Yeghiayan was alarmed at how fast his battery was draining, but he kept communicating with DPR, making sure he logged in to the admin panel. Tarbell peered over the last step but couldn't see much. Somewhere in the stacks was the other agent, but Tarbell wasn't sure where. Everyone was communicating electronically, trying to coordinate, caught blind by the moment. Minutes ticked past. Der-Yeghiayan and DPR still chatted. His battery dropped further. Tarbell heard from the plainclothes surveillance team—they were in the library too. Tarbell didn't know where exactly, because he didn't know what they looked like. (Such is the very low profile kept by field surveillance.) A few miles away, the giant squad of SWAT teams was approaching San Francisco. All the local supervisors were in that armada, so technically Tarbell was in charge here on the ground. He took a deep breath and sent a message: "Let the guy run if you have to, but don't let that computer close." This was the moment. Tarbell didn't know it, but the surveillance agents had designed a new arrest on the spot. He had no idea what would happen when he took a deep breath and told everyone: Go.

What unfolded next was a piece of improvisational theater. At 3:14 pm, DPR was typing away, writing to Cirrus. Just then, a middle-aged woman and man came toward Ross, ambling along in the kind of semihomeless shuffle you might often see in a San Francisco library. “Fuck you!” the woman yelled when they were directly behind Ross’ chair. As if they were a deranged couple about to fight, the man grabbed the woman by the collar and raised his fist.

Ross turned around for just a second, during which a hand reached across the table and grasped Ross’ Samsung. The petite, unassuming young Asian woman sitting across from Ross this whole time was, to everyone’s surprise, also an FBI agent. Ross lunged for his machine, a hair too late, as she turned like a quarterback for a quick handoff to Kiernan, who appeared out of nowhere—as instructed—to get the laptop. It took less than 10 seconds. From afar, Tarbell was astonished by the elegant choreography of the whole thing. It looked like the police procedural version of a tight jazz quartet.

While Ross was cuffed, Kiernan immediately sat down with Ross’ PC. It was open. He could see everything. The machine ID was Frosty. Ross was logged in to Silk Road as an administrator under an account called /Mastermind.

Kiernan also saw that Ross was torrenting some television. Of all things, he was downloading a segment from the previous night’s *Colbert Report*—an interview with Vince Gilligan, creator of *Breaking Bad*. The series finale had just aired, and Gilligan talked about the central theme of the show, how ordinary people are capable of terrible things. It took just two years for Walter White to turn from good-natured science teacher to liar, murderer, and master of a drug empire. Had Ross not been arrested he would have watched Gilligan say that yes, of course, Walter was doomed from the start. And everyone knew it but him.

TARBELL STOOD WITH Ross for the first time, searched him, and put him into a surveillance van, where he read him his rights. Ross showed only a slight quiver in his lip and asked to see the charges. Tarbell presented him the warrant for Ross Ulbricht, aka Dread Pirate Roberts, aka DPR.

The rest of the force started arriving, black Suburbans and SWAT vehicles with lights blazing. Soon there were uniforms everywhere. Even though Tarbell's improvised bust was a complete success, cops are cops, and the local FBI was fuming at Tarbell's departure from protocol. He and his team, considered computer dorks back home in New York, had the strange satisfaction of being called "fuckin' cowboys" by a swarm of guys bristling with gear and guns. Tarbell took it as a compliment. Then he put Ross in an FBI cruiser bound for the local jail.

Tarbell called Yum in Iceland to set that phase in motion. Yum shut down communication between the machine in the Thor Data Center and all the others around the world and then simply "changed possession" of the bitcoins by redirecting the digital pointers—this is how ownership of the currency works—from Silk Road to an FBI account. And voilà: All your coins are belong to us.

In France they discovered a digital booby trap: To redirect the Silk Road site itself required a delicate data process that could shut the box down; if restarted, the server was programmed to delete its key, basically self-destructing. But the trap was discovered, and gingerly evaded, and the machine succumbed. Thereafter, the Silk Road welcome page read: THIS HIDDEN SITE HAS BEEN SEIZED BY THE FEDERAL BUREAU OF INVESTIGATION. Within minutes, Reddit erupted. “Is this a joke?” someone posted, along with plenty of WTFs.

The arrest was such a coup that the Justice Department wanted to publicize it. They’d planned on staging a press conference in Washington, with attorney general Eric Holder himself, to make a strong statement about the government’s ability to take on cybercrime. But, as it happened, Ross was arrested on day one of the dramatic government shutdown, when one of his heroes, Rand Paul, along with other senators, held the federal budget hostage over the debt ceiling and forced Washington to go dark. There would be no Holder, no press conference, no government at all to celebrate its defeat of this libertarian, lawless challenge. The only public notice of Ross’ arrest was the release of the FBI’s initial 39-page complaint signed by Tarbell, cementing his new public persona as DPR’s digital Van Helsing.

In the car, Tarbell and Ross found themselves alone in the backseat. Tarbell had read so much about him, it was kind of like seeing an old pal. Tarbell talked about Ross’ life in a way that made it clear how much he knew. Ross was talkative but cagey. He seemed relaxed, as if relieved. Not in being caught, but just being with someone who possessed his secret. In front of Tarbell, he could be both Ross and DPR. He admitted nothing to Tarbell, but after a natural pause in the conversation, Ross said, “I don’t suppose $20 million can get me out of this?” It might have been the most authentic moment in Ross’ life in more than two years.

“No,” Tarbell said. He couldn’t resist needling him. “Even if it could, what about this guy?” He pointed at the driver, another FBI agent. “Have to take care of him too, right? How much money do you have?”

Ross looked ahead as they weaved toward the jail.

IN A VAN that doubled as a mobile lab, Kiernan worked forensics on Ross' computer. He quickly found a mountain of evidence: a list of all the Silk Road servers and the names Ross had purchased them under, 144,000 bitcoins (more than enough to cover that $20 million bribe), a spreadsheet showing Silk Road accounting (including a capital-equipment entry for the purchase of that very laptop), and those diaries Ross kept, which detailed his hopes, fears, and foibles in operating a vast criminal conspiracy.

Kiernan also found a file called emergency .txt, with an unrealized escape procedure:

Destroy laptop hard drive and hide/dispose
Hide memory stick
Go to end of train
Find place to live on craigslist for cash Create new identity (name, backstory)

RELATED STORIES

Darpa Is Developing a Search Engine for the Dark Web
BY KIM ZETTER

A Dope Dealer On What It's Like Selling On Silk Road
BY ANDY GREENBERG

The VC Who Bought the Silk Road's $19M Bitcoin Cache
BY ROBERT MCMILLAN

At Ross' house, agents found a USB drive containing some Silk Road programming, but beyond that, little else. When Alex and the other roommates got home, they found the warrant on the coffee table.

Alex visited Ross in jail. He expected him to be shaken, but Ross was the same as always. He would soon be transferred to New York to face a seven-count indictment. It was hard for Alex to believe that the new guy in the extra room, his pal, was also the guy described in that warrant. The thought of Ross being guilty of even tripping someone, much less ordering a murder, seemed unlikely. He was always such a chill dude.

9

All Rise

ROSS WAS ARRAIGNED in federal court in New York a few months later, still seeming pretty chill. He pleaded not guilty. Like Alex, Ross' friends and family couldn't believe the charges. They were first shocked, then incensed. There emerged a familiar refrain: Ross was such a nice guy. There must be some mistake. Ross' lawyer, Joshua Dratel, a seasoned, high-profile defense attorney who took on tough cases, made the same argument. His letter asking for bail was a moving collection of testimonials on Ross' behalf: "good role model," "reputation for fulfilling his obligations," "fearless embrace of making the world a better place for

everyone." But the judge, citing flight risk, denied bail altogether.

Online, Ross became a cause célèbre. The libertarian and cypherpunk communities naturally felt that their champion had been martyred. The charges were ginned up, they thought, retribution for Ross having the temerity to challenge the government itself. Many a Reddit thread overflowed with outraged chatter and meticulous analysis of what the community insisted was overreach, flawed evidence, or a frame job. A solidarity site appeared: Freeross.org.

Ross and his attorney prepared a defense that basically amounted to "Wasn't me." They chose to occupy that narrative gap of uncertainty made possible by the ambiguity of identity online. Dread Pirate Roberts was just pixels, they said. Everyone knew there were many DPRs, they argued, returning to the lore of Silk Road and the symbolism of the alias.

It was a powerful idea. In the months leading up to the trial, the defense created a speculative froth about the very nature of identity, suggesting that Silk Road was an ongoing mystery. After all, everyone loves a whodunit. The case became like a crowdsourced mystery theater, with so many potential question marks hidden in the numbers and code.

Then the trial started. And the conspiratorial mindset was no match for clear, hard, overwhelming evidence. The courtroom was packed with Ross' family, supportive spectators, and press as the biggest cybercrime trial in years unfolded in the federal district court building in downtown Manhattan. But armed with hundreds of exhibits, the prosecutors for the US attorney's office presented an efficient, detailed case. They showed the diaries. Der-Yeghiayan explained how they caught Ross logged in as /Mastermind. They read aloud from DPR's chats, stored on Ross' computer, presenting the odd spectacle of gray-suited government lawyers addressing the court with choice narrations like "Squid gave me the support link, just let me know when I have access." Outside, a vigil of protesters held signs, some reading "FREE ROSS".

Ross, who declined to be interviewed for this story, was not charged with any murders. The case involving Green, which came out of Baltimore, was a

separate indictment. (It is still pending.) The New York case dropped the five other murders after further investigation revealed that the whole thing was likely an elaborate catfish-as-blackmail scheme that snookered Ross out of a lot of money. But in all cases, the prosecution argued, Ross believed he was executing people, even receiving photographic evidence faked to prove it. For dramatic effect, the prosecutors read aloud selections of Ross' conversations where he sounded like a heartless mafia boss.

It was a quick trial, 13 court days, faster than expected. Observers were surprised at the volume and detail of evidence, the kind you rarely see. To the end, Ross' lawyer, Dratel, claimed it was a case of mistaken identity. (Like most criminal defendants, Ross himself didn't testify.) Or rather, a qualified case of mistaken identity. Dratel caused quite a stir in his opening statements by admitting that Ross had indeed started Silk Road, but then quickly sold it off to some other unnamed figure. The attorney also claimed that Ross was later duped by this savvy character back into Silk Road to take the fall as the FBI closed in. To account for the vast sum of bitcoin wealth, Dratel explained that Ross was just a good currency trader. Then Yum took the stand to demonstrate precisely how Ross received all the bitcoin commissions from Silk Road during the entire tenure of Dread Pirate Roberts.

Ross' family was surprised to hear the admission that he'd created Silk Road. Reporters could see it on his mother's face. Lyn Ulbricht was a sympathetic figure, a caring mother leading a vigil for her son. She was smart and articulate and had become a vocal public figure in support of Ross. Throughout the trial she maintained that the jury would set Ross free.

This was more than a mother's love. Lyn, like many supporters, just believed Ross. Which was understandable, to some degree, as Ross' story was one of fluid identity. The prosecution said that Lyn's good-natured son had turned into someone else. Lyn said that this someone, if he or she even existed, had been projected onto her son. Ross said nothing and remained a willing cipher, allowing everyone to project an identity onto him: To

Alex, Ross was the cool new roommate; to Julia, a passionate lover and inspiration; to his family, the perpetual Eagle Scout; to Force, an unlikely friend in the night; to Tarbell, a smart kid defeated by his own arrogance. To the Southern District of New York US attorney's office, Ross was simply the criminal conspirator Dread Pirate Roberts.

The likeliest reality is that Ross was all of those things. The open-minded seeker who conscientiously tried to pluck trash from a tree was Ross. As was the feverish visionary creating a virtual empire at any cost. Neither truth invalidated the other. Ross and DPR can (and did) coexist.

Amid all the murder minutiae, it's possible to lose sight of the young idealist who sat down and coded his way into history. He was right about the war on drugs: It is a failure. And Silk Road was a perfectly natural response. There was a lot to like in the site's original idea of an economically mediated utilitarian society. It is still easy to appreciate that Ross, the one who believed in choice and happiness. "Our basic rules are to treat others as you would wish to be treated," Ross wrote as DPR on Silk Road.

But it didn't take long for Ross' programmed utopia to resort to programmatic violence. It's an age-old story, the bloom and wilt of revolution. After tearing down the establishment's walls, the new regime soon realizes the rubble would make a fine set of gallows. Just as Tarbell thought, all systems are the same. At the beginning of Silk Road, what Ross created was just a system. Then, at a certain point, it became *his* system—at which moment the system was doomed.

Silk Road offers a neat political parable for the rising libertarian tide in Washington and the smug pride of today's Silicon Valley, where self-appointed revolutionaries of all stripes believe their powers allow them to transcend traditional human boundaries, including their own mortality. In

a way, Silk Road is the dark mirror of *The Social Network*, a wild technological success story taken to its logically extreme conclusion.

Force watched from afar in Baltimore. Having lost his big career case, he acknowledged that the FBI "won fair and square," and he had left the DEA by the time the trial started. But Force had a lot of sympathy for the guy he'd spent so much time with in late-night chats. As a man who was saved from the temptations of undercover work, Force believed that everyone was a sinner. He also identified with Ross. "I'm no different than him," Force said. "It easily could've went the other way." No one is either perfectly good or perfectly evil. People occupy a space right on each side of the line. And sometimes, without knowing it, you switch sides.

Force's words rang truer than anyone knew. In an incredible twist, Force, along with a Secret Service agent on his team, was also indicted and arrested this past March for running an elaborate series of rackets and thefts on Silk Road. The 95-page indictment alleged that they stole bitcoins from Silk Road and other exchanges (the digital equivalent of keeping the suitcase full of cash after a dockside heroin bust); pocketed $50,000 from DPR for intel services from "Kevin"; laundered at least half a million of that (some of which made it to Panama); and served a false subpoena on a digital currency exchange when they questioned his transactions and froze his account. It was, in fact, when all this came to the attention of the Department of Justice that Force left the DEA. "In retrospect," Tarbell said when he heard about the investigation of Force, "it's as if you found out at the end of *Breaking Bad* that Hank was dirty the whole time."

In retrospect, a lot of Force's story takes on a different light. Ironically, he had warned DPR about the danger of double identity, but if this indictment is true he seems to have fallen prey to it himself. Force allegedly operated online not only as Nob but had also created several other identities and used them to blackmail DPR with law enforcement information for at least $100,000. Like Ross, Force must have believed in the secrecy of Tor. During the sting operation with Curtis Green, Force even told Green he thought the Silk Road servers would never be found. But they were, and after they documented Ross' misdeeds, they also revealed that it was Force and the

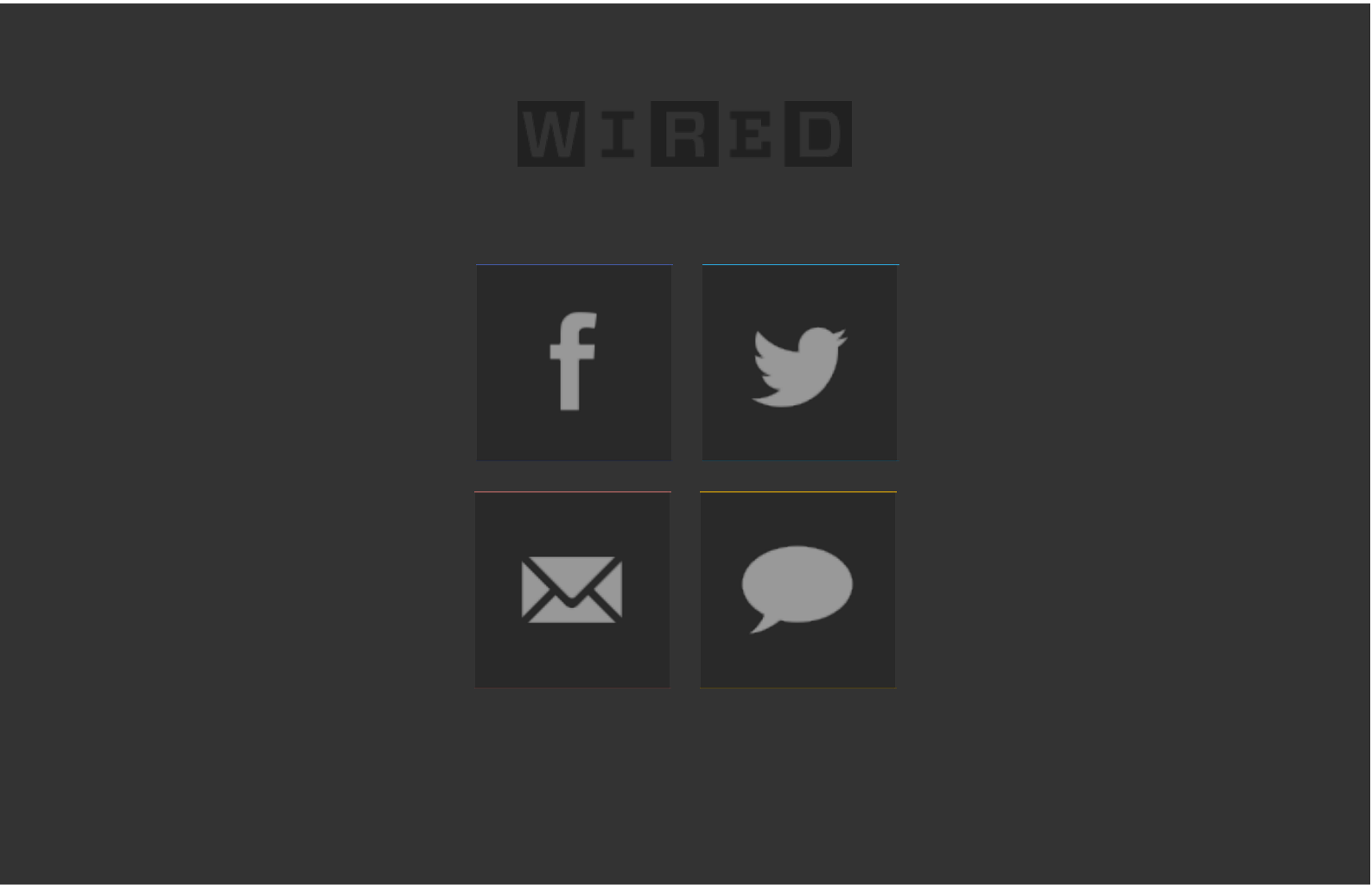
Secret Service agent who had stolen $350,000 in bitcoins from Silk Road—the theft that led Ross to put the hit on Curtis Green. None of this emerged during Ross' trial because Force's case was at odds with the FBI investigation and part of a different indictment. But if true, Force's fall mirrors the path of DPR. It was during the Green sting that Force took his first corrupt step, and DPR became a true criminal by ordering murder. Their simultaneous moral turns, so intertwined, reinforced the one theme that barely appeared during Ross' trial: how easy it is to forget the solidity and consequences of the real world when you live online.

The jury in *USA v. Ulbricht* was out for barely four hours. And that included lunch. They returned to the assembled courtroom and read the verdict: guilty on all seven counts. Ross' family looked stricken. A sympathizer stood up and yelled, "Ross is a hero!" Ross was led from the court. Outside, Dratel was set upon by reporters. He vowed an appeal. The press gaggle jockeyed for position and fired questions. Some were bloggers who sided with Silk Road. As news spread online, partisans continued the fight, arguing over the identity of Ross and Dread Pirate Roberts, echoing what Dratel said to the jury in his closing statement: The Internet is a place of confusion, where nothing is what it seems.

Ross returned to jail, where, his mother liked to explain, he had been teaching yoga to other prisoners and doing a lot of reading. Alex sent him a printout of the short story "Man of the Crowd" by Edgar Allen Poe. Alex thought it seemed fitting, as the story is about a man in detective mode following someone he calls a "genius of deep crime" through the streets. But there is confusion in the chase. And a hint that the pursuer realizes that the man he's after is, in fact, himself. Yet this other self remains beyond his grasp, "like a book that cannot be read." As night falls, the man finally gives up the pursuit and watches the unknowable shadow disappear into the crowd.

This article includes reporting by Nick Bilton, whose book on the Silk Road case will appear in 2016.

This story appears in the June 2015 issue of WIRED.



The White House Wants You to Build Tools to Improve Our Cities

A whole lot of valuable information is trapped in the antiquated databases and inaccessible filing systems of local governments across the country. Now, the Obama administration is hoping to unlock that treasure chest with the launch of The Opportunity Project, a new open data project spearheaded by the White House.

The goal of The Opportunity Project is to make local and federal datasets easily sortable and available online, so developers can combine them to build new civic tech tools to improve the relationship between cities and their citizens. The site, which launched today, features data on everything from crime to after-school programs to government job listings in nine major cities, including New York and San Francisco.

Chief US Data Scientist DJ Patil, who leads open data efforts at the White House, says President Obama is the one who initiated the idea. Throughout his tenure in office, Obama has worked to modernize the federal government, investing in technology that can streamline bureaucratic government processes without requiring Congressional approval. Later this week, at South by Southwest, the President will deliver a speech about the importance of technology in government.

'We should think of technology as neither radical nor revolutionary unless it impacts every single person.'

But while sophisticated data modeling is becoming routine at a federal level, Patil says, "the president has really been focused on the idea of how do you get the force of data to benefit everyday Americans? We should think of technology as neither radical nor revolutionary, unless it impacts every single person."

But in many cases, local governments don't have the resources to invest in data science. With The Opportunity Project, the White House is hoping to inspire developers to build tools that will make it easier for decision makers to access the information they need.

Civic Tech

The new platform showcases a dozen tools that have already been built using these datasets, from an app that helps families find housing near good public schools to the so-called National Equity Atlas, which uses data to showcase levels of inequity across the country.

The site also includes examples of everyday people who stand to benefit from the types of tools these datasets could yield, such as, for instance, a female survivor of domestic abuse looking to relocate. Today, there that woman might need to find shelter from one resource, childcare from another, and job training from another in

order to get back on her feet. But a tool that unifies information on these resources in cities across the country could simplify that already difficult process.

Of course, these aren't the types of issues that the tech world's most prominent companies typically invest in. Instead, Patil anticipates that most of these tools will be built by volunteers or a new generation of small business owners who are working on civic tech.

"We've shifted into a model where people are really empowered to take control of their communities," he says. "Fostering that community, where people can come together around hackathons and other things, is extremely powerful."

Think You Can Drive Fast Enough to Escape an Erupting Volcano?

Imagine being near a volcano when it unleashes a gigantic eruption. I'm not talking something fairly piddling like the 1980 eruption of Mount St. Helens or even the 1991 eruption of Pinatubo in the Philippines. I'm talking one of these eruptions that the tabloids and conspiracy websites say will destroy civilization, like Yellowstone or Toba. The common response is that everyone within hundreds of kilometers of the volcano would be killed almost instantly thanks to the fast moving pyroclastic flows that can rush outward from the caldera volcano for more than 150 kilometers (~100 miles). That idea is based on what we can see from these flows at smaller eruptions, where they race down the sides of the volcano at speeds over 500 kilometers per hour (300 mph). Cities like Pompeii and St. Pierre were wiped out mere moments after an eruption thanks to these avalanches of hot volcanic debris and ash.

However, we've never been able to examine first-hand the results of a really giant eruption that puts Vesuvius and Pelée to shame. So, we need to look at the deposits left by such gargantuan events to figure out how they might be similar or different than their smaller brethren. Do the pyroclastic flows race out at the same speeds and are these flows the same mix of hot gasses and ash? The answer to those questions can help us better prepare for such an eruption and interpret the deposits left by these monsters in the past.

A new study in *Nature Communications* by Olivier Roche (Université Blaise Pascal), D.C. Buesch (USGS) and Greg Valentine (University at Buffalo) has taken a stab at quantifying the speed of one of these massive eruptions and the results surprised me: Maybe we wouldn't be so doomed?

The Peach Springs Tuff (Arizona) sitting on top of a layer of the Cook Canyon Tuff in Arizona. *Calvin Miller (Vanderbilt University)*

Roche and others looked at the Peach Springs Tuff, a massive volcanic deposit that erupted from the Silver Creek Caldera in Arizona about 18.8 million years ago. Now, the Peach Springs Tuff dwarfs most eruptions in the past few thousand years, with at least 1,300 cubic kilometers (or enough to cover all of Manhattan with almost 22 kilometers —~13.6 miles!—of volcanic debris). Deposits of the Peach Springs Tuff can be found over 170 kilometers (~105 miles) from the caldera and in those places, the deposits are still 10 meters (~30 feet) thick! This was an enormous eruption in an area where we don't tend to imagine super-eruptions occurring.

A photograph shows dark rocks embedded in layers of ash. The rocks were picked up and moved across the landscape by pyroclastic flows when the Silver Creek caldera, a supervolcano, erupted 18.8 million years ago. *Greg A. Valentine*

The Peach Springs Tuff was big enough that the pyroclastic flows moved large pieces of rock (see above) that were lying on the ground before the eruption happened—kind of like how a stream picks up rocks and trees during a flood. By looking at the size and weight of these chunks of rocks, you can estimate the speed that the flow had to be moving if you make some assumptions about the flow itself.

If it is mostly made of hot gases and tiny ash particles, then it can't move big rocks without moving really fast. If it has a lot of heavier grains of volcanic debris, then it can move big rocks at slower speeds because it has more strength. Additionally, the longer you apply that force, the greater your ability to move the rock. You can picture it this way: Try moving a bowling ball with just a fan for a minute, then try with a firefighter's hose for 10 minutes. The added density of the water from the hose means you can move that bowling ball easier at slower velocity of flow, especially if you have more time.

So, Roche and others looked at the sizes of blocks picked up by and incorporated into the Peach Springs Tuff (see above). Now, they didn't move the full distance—that is, the 70 centimeter boulder found 150 kilometers from the caldera didn't move 150 kilometers. It might have only been moved 100 meters, but it was moved by the flow of volcanic material during the eruption.

Now, even at distances as far as 140 kilometers (~88 miles), the Peach Springs Tuff was happily moving rocks that are 70 to 90 centimeters across (a few feet). That is an

impressive feat! So, were they being moved by something thin and fast briefly or something thicker and slower for a longer duration?

By modeling the force needed, Roche and others found that the blocks that far away couldn't have been moved by something thin and fast because it would have required speeds over 720 to 2,340 kilometers per hour (447-1454 mph), which is wildly unrealistic based on any known volcanic process. Even some of the fastest known pyroclastic flows observed, such as the blast at Mount St. Helens, was moving around ~600 kilometers per hour (370 mph).

So, then what if the flow was dense instead? Roche and others ran experiments looking at miniature pyroclastic flows made of beads and sand to see how such flows could move larger particles. What they found is that such denser flows could move these large blocks at speeds closer to 18 to 72 kilometers per hour (11 to 44 mph). That is much slower than what we see at smaller eruptions, but for those smaller flows, we see what is happening within a few kilometers of the volcano. If the flow moves out 150+ kilometers, then maybe it can slow down but still have enough oomph to move block.

What that would require is a constant push from the eruption itself. If the Silver Creek Caldera erupted for 2.5 to 10 hours at a sustained rate of 38 to 150 million cubic meters per second, then these flows could move blocks even moving at only a few tens of kilometers per hour. Now, that eruption rate is huge, tens to hundreds of times more than Pinatubo, Tambora or Novarupta, some of the biggest eruptions of the last few centuries.

This means that the eruption of the Peach Springs Tuff was at least as large if not larger than the super-eruptions like Toba or Taupo. Yet, if you were 150 kilometers from the eruption, you might have upwards of 10 hours to get out of harm's way (well, at least out of the way of the massive pyroclastic flows—the resulting ash fall and climate cooling is a little trickier to handle).

What does this all mean? Well, it means that cities near(ish) to large volcanoes like Yellowstone or the Campei Flegrei might have a fighting chance** to survive in the face of such a catastrophic eruption. Rapid and organized evacuation of cities might allow for people to leave in time, much like people can evacuate before a hurricane. However, that should be seen as a last resort. It is really careful volcano monitoring that can save lives most effectively, letting people know when they need to leave before they have to worry about a pyroclastic flow barreling towards them … but it is nice to know that it might not be bearing down on you as fast as we thought.

****Addendum (4:00 PM EST March 7)**: I wanted to clarify a few things after an email

exchange with Dr. Valentine (from this study). First, it is clear that this study *does not* imply that evacuations can be effective in places like Naples near the Campei Flegrei after an eruption has started. Naples is far too close to have the finding of this study play any role. Remember, volcano monitoring and evacuation *before* the eruption is the best solution. Additionally, this study focussed on a single eruption from the Silver Creek caldera, so applying it to all very large eruptions is untested at this point.

Watch Us Epically Fail NASA's Astronaut Test

Always dreamed of going to space? Yeah, me too. With NASA now mid-hunt for their next class of astronauts, WIRED decided to take a trip to the Johnson Space Center in Houston, TX to get a sneak peak of what these future space explorers would go through if they're lucky enough to make the cut.

It turns out, however, that becoming an astronaut is harder than ever. NASA was accepting applications between December 14, 2015 and February 18 of this year, and in that time they received a whopping 18,300 submissions. That's more than 10,000 more than the previous record, which was set in 1978, and roughly three times as many as the last call a few years ago.

So how many of those wannabe astronauts have a real shot? While NASA doesn't yet know how many of the 18,300 current applications are viable, the agency told us that the last time around, about 4,800 applications met the basic requirements, about 79 percent. If that trend holds, roughly 14,400 people will make it to the next round of evaluations this year. (Some people, says Anne Roemer, NASA's manager of astronaut selection, apply just to get the rejection letter—and then they frame it. Wish I had thought of that.)

First, an applicant has to meet some minimum qualifications—a college degree in a STEM discipline, at least three years of field experience, basic height and weight restrictions. Every application cycle, Roemer says, NASA gets people who don't meet the education requirements but beg and plead to be considered anyway. Don't hold your breath: I tried, but apparently being a science and tech writer can't be substituted for actual course work.

After meeting those basic requirements, the panel—composed mostly of flown astronauts—reviews candidates for things like education quality, mission-applicable experience, and teamwork and leadership skills. "We're looking for folks who aren't just good at one thing," says Roemer. "We look at the full package: Not just what work experience do they have and what education, but what are their hobbies, adventures, and things of that nature." That winnows the group to about 500 candidates.

From there NASA does reference checks, and the astronaut selection board picks about 120 candidates for interviews. That's kind of your standard job interview, where they try to get to know you and rate you on astronaut-y skills. Fifty or 60 candidates will get a second interview—and a weeklong physical evaluation. Which is, shall we say, intense. A team of doctors from the Flight Medicine Clinic assesses candidates' general health, but also whether or not they could pass the Astronaut Long-Duration Spaceflight Physical. Of those 60, only eight to 14 will go on to become astronauts.

Those lucky ducks will go through at least two years of training in spacewalking, spacecraft systems, the Russian language, and more. If they manage to complete that training, they'll work some technical duties within the Astronaut Office at the Johnson Space Center. And finally, gloriously, NASA will assign them to a mission aboard either the ISS, the NASA's Orion spacecraft, Space X's Crew Dragon, or Boeing's CST-100 Starliner—assuming those last two are ready for primetime.

If you're not one of the spacefaring few, don't despair. "Being selected as an astronaut is a very competitive process," says Roemer. "So the number one piece of advice we always give to folks is we want them to pursue a career they're passionate about." Still, Roemer encourages everyone to apply. Just because they aren't looking for artists or writers on this mission, next time around, who knows? Maybe they'll be looking for the next voice of the space program; a storyteller to make the stars accessible to the people back on Earth and inspire the next generation of scientists.

But if that's the case, don't even bother applying. That job is mine, damn it.

WHILE YOU WERE OFFLINE: WELL, NOW WE'VE SEEN A MAN'S SOUL LEAVE HIS BODY ON LIVE TV

Oh, what a week it's been! Pornhub revealed the Fetish States of America (lesbians, congratulations on continuing your dominance of the straight male mind), the Republican presidential race literally turned into a discourse about penis size, and Kendrick Lamar dropped a new EP with no notice on Thursday night. But that's nowhere near all that happened over the last seven days. As we do this time each week, shall we take a trip together through the weird backwood swamp of this Internet we all call home?

Blink Twice If You Need Help, Chris Christie

What Happened: He might have withdrawn from the race, but nonetheless, Chris Christie won Super Tuesday thanks to a performance presenting Donald Trump that got everyone talking.

Where It Blew Up: Twitter, blogs, media think pieces

What *Really* Happened: You've doubtlessly already seen Donald Trump's victory speech from this Tuesday's election results, but if not it's above.

What caught everyone's attention wasn't what Trump was saying, but what was happening *behind* Trump. Chris Christie's performance, somewhere between panicked and confused, very quickly became a thing, with people either worried or amused by what they saw.

Twitter was, of course, ready to weigh in with instant commentary:

> Is Chris Christie about to have a stroke?
>
> — Official Wanda Sykes (@iamwandasykes) 3:56 AM - 2 Mar 2016

> In all seriousness, Chris Christie looks so strange. Like he's about to vomit.
>
> — emily nussbaum (@emilynussbaum) 3:53 AM - 2 Mar 2016

> Chris Christie looks like my dog when she realizes our car ride was to the vet
>
> — Matthew (@Matthops82) 3:56 AM - 2 Mar 2016

> What is going through Chris Christie's head right now?
>
> — Matt Viser (@mviser) 3:56 AM - 2 Mar 2016

> Chris Christie has been re-enacting Mike Myers' "Uh-oh, Kanye is veering off the script... What do I do?" Face for 15 solid minutes.
>
> — Bill Simmons (@BillSimmons) 3:59 AM - 2 Mar 2016

> "OH GOD WHAT HAVE I DONE?" --@ChrisChristie
>
> — Andrew Klavan (@andrewklavan) 7:29 AM - 2 Mar 2016

> It's Day 6 of the Christie Hostage Crisis. #ThoughtsAndPrayers #FreeChrisChristie http://www.usatoday.com/story/news/politics/onpolitics/2016/03/01/chris-christie-donald-trump-rally/81187404/ ...
>
> — Russell Thomas (@MrMeritology) 8:30 AM - 2 Mar 2016

> Y'all are mean to Chris Christie. What did he ever do except debase himself & betray any values he pretended to have in exchange for power?
>
> — Steve Hely (@helytimes) 5:56 PM - 2 Mar 2016

Things reached such fever pitch that Christie was forced to hold a press conference in which he *actually said*, "No, I wasn't being held hostage; no, I wasn't sitting up there saying, 'Oh, my God" ... I understand everybody had a lot of fun with it; it doesn't matter to me. I've had a lot of fun on the Internet with people at times, too." Sure, perhaps. But *this* much fun?

The Takeaway: Of course, that was earlier this week. Things have probably changed since th—

> UPDATE: Chris Christie just finished cutting up Mr. Trump's waffles just the way he likes them.
>
> — scott feschuk (@scottfeschuk) 1:10 PM - 2 Mar 2016

Imma Let You Finish Downloading, But This Twitter Beef Is the Weirdest of All Time

What Happened: Does Kanye West use Pirate Bay? After a picture he tweeted appeared to suggest the answer was yes, the Internet pounced (and Kanye parried).

Where It Blew Up: Twitter, media think pieces

What *Really* Happened: Ah, what would a week on the Internet be without Kanye doing something ridiculous? This week, however, it was seemingly by accident, as this tweet (below) ended up revealing more news than he probably intended. Namely, that

Kanye's browser tabs included The Pirate Bay, a fact that was not missed by many, likely to Ye's embarrassment.

> Day 3
>
> — KANYE WEST (@kanyewest) 4:39 AM - 2 Mar 2016

It got stranger, as Kanye was seemingly torrenting Serum, the sound-editing software from Xfer Records, created by Deadmau5, who just so happened to have co-founded Tidal with Kanye. He noticed.

> What the fuck @kanyewest ... Can't afford serum? Dick.
>
> — dead mow cinco (@deadmau5) 4:49 AM - 2 Mar 2016

> Let's start a Kickstarter to help @kanyewest afford a copy of Serum.
>
> — dead mow cinco (@deadmau5) 4:56 AM - 2 Mar 2016

> He needs a small loan of 200$ #prayforyeezy
>
> — dead mow cinco (@deadmau5) 4:57 AM - 2 Mar 2016

As should only be expected, this did not go down well with Mr. West.

> @Deadmau5 ... is this person's name pronounced dead-mow-five?
>
> — KANYE WEST (@kanyewest) 7:30 PM - 2 Mar 2016

> # ok very serious question...
>
> — KANYE WEST (@kanyewest) 7:32 PM - 2 Mar 2016

> # whose job is it to carry the head on the plane # hash tag # do you check the mickey mouse head or carry on # does it get hot?
>
> — KANYE WEST (@kanyewest) 7:33 PM - 2 Mar 2016

> # ok another super serious question ... is there a portable fan situation?
>
> — KANYE WEST (@kanyewest) 7:34 PM - 2 Mar 2016

> # hash tag you raised Tidal's subscriptions by a whopping
>
> 

downloads

— KANYE WEST (@kanyewest) 7:37 PM - 2 Mar 2016

I'm bored ### when you get married will your wife have a giant minnie mouse head? # This brightened up my day... thank you dead-mow-five

— KANYE WEST (@kanyewest) 7:37 PM - 2 Mar 2016

Do you do birthday parties?? My daughter loves Minnie mouse...

— KANYE WEST (@kanyewest) 7:38 PM - 2 Mar 2016

can you please bring the minnie mouse head ... not yours she specifically likes minnie mouse ...

— KANYE WEST (@kanyewest) 7:39 PM - 2 Mar 2016

I need you to perform at her party with specifically a minnie mouse dead-mow-five head... not a mickey mouse dead-mow-five head.

— KANYE WEST (@kanyewest) 7:40 PM - 2 Mar 2016

I'm very detailed oriented and I will know the difference so don't try to just throw a bow on the original head...

— KANYE WEST (@kanyewest) 7:41 PM - 2 Mar 2016

I want to stream you performing in a Minnie Mouse head on @TIDALHiFi

— KANYE WEST (@kanyewest) 9:31 PM - 2 Mar 2016

Imma let you finish.... But you should probably be saving the money for a 4th grade education. https://twitter.com/kanyewest/status/705128371903193088 ...

— dead mow cinco (@deadmau5) 12:15 AM - 3 Mar 2016

@kanyewest perform at your own daughters parties. You're a bigger fuckin clown than anyone I know.

> — dead mow cinco (@deadmau5) 12:57 AM - 3 Mar 2016

It was an unusually underwhelming Twitter beef considering those involved, which of course meant that plenty of people noticed. No news as yet if Deadmau5 has launched a LivingMinni3 spinoff inspired by the exchange, sadly.

The Takeaway: Perhaps the funniest part of the entire thing was the suggestion by Kanye West's publicity team that it clearly wasn't actually Kanye's own computer, but a screenshot of someone else's that he was using to illustrate piracy's dangers.

What Happened, Miss Simone?

What Happened: The first trailer for an upcoming biopic of musician/activist/all-round-badass Nina Simone dropped, reigniting an argument about whether or not Zoe Saldana was right for the lead role.

Where It Blew Up: Twitter, media think pieces

What *Really* Happened: Nina Simone was an amazing, and amazingly complicated, woman—one watch of the Netflix documentary *What Happened, Miss Simone?* makes that clear—which would make a biopic of her life an obvious choice. Less obvious, however, is the choice of actress to play Simone. Producers went for *Avatar* and *Star Trek*'s Zoe Saldana, and this week, audiences got their first look at her in the role.

If you're thinking, "*Wait*. Is Zoe Saldana wearing blackface in that movie?" then you're not alone. A lot of other people asked the same question.

> zoe saldana looks foolish at nina simone. foolish.
>
> — Tracy Clayton (@brokeymcpoverty) 7:14 PM - 1 Mar 2016

> Even though Zoe Saldana is a WOC, Nina Simone stuff is blackface. I'm not debating anyone. It just is.
>
> — ItsJustJayNow (@ChocnessMonsta) 7:30 PM - 1 Mar 2016

> They would rather put Zoe Saldana in brown face than to hire an actress with darker skin. Nina Simone deserves more.
>
> — Marty. (@Atwitisborn) 7:56 PM - 1 Mar 2016

> Zoe Saldana should have never been an option to play Nina Simone. They literally had to paint her face for that role. HOT MESS.
>
> — Awesomely Luvvie (@Luvvie) 8:19 PM - 1 Mar 2016

> This pics of Zoe Saldana as Nina Simone...listen, you'll never convince me a dark skinned Black woman couldn't have played that role better.
>
> — Mikki Kendall (@Karnythia) 9:41 PM - 1 Mar 2016

> That Zoe Saldana pic as Nina Simone looks like the blackface of a bad Halloween or frat party
>
> 
>
> — ProfB (@AntheaButler) 10:38 PM - 1 Mar 2016

> I feel like whoever did Zoe Saldana's make up for "Nina" saw "Tropic Thunder" and thought RDJ's look was a how to guide.
>
> — Lux Alptraum (@LuxAlptraum) 6:30 PM - 2 Mar 2016

The official Twitter account of Simone's estate was somewhat more direct.

> .@zoesaldana Cool story but please take Nina's name out your mouth. For the rest of your life.
>
> — Nina Simone (@NinaSimoneMusic) 2:26 AM - 3 Mar 2016

Unsurprisingly, that tweet grabbed much attention when posted, but at least one person is standing up for Saldana: Robert L. Johnson, founder of BET—which just happens to be distributing the movie. "The most important thing is that creativity or quality of performance should never be judged on the basis of color, or ethnicity, or physical likeness," he said in a statement. Which might explain the origin of this

hashtag:

> Future and Migos as the Beatles #BlackactorsinWhiteface
>
> — Angelica Pickles (@Itsprincesssyd_) 6:10 PM - 3 Mar 2016

> Michael Ealy as JFK #Blackactorsinwhiteface pic.twitter.com/9RSn6H4d4L
>
> — Angelica Pickles (@Itsprincesssyd_) 6:19 PM - 3 Mar 2016

> Brandy in the Queen Elizabeth Biopic #Blackactorsinwhiteface
>
> — Bare Witness (@TheQuietfreedom) 12:24 AM - 4 Mar 2016

> Future as Meryl Streep #BlackactorsinWhiteface
>
> — Fool's Gold (@Alexis_Mercury) 3:31 AM - 4 Mar 2016

The Takeaway: Yes, race is a complicated issue, and it's true to an extent that actors shouldn't be judged on their physical likeness to their (real world) roles. But, at the same time, didn't we just go through something like this?

> Zoe Saldana as Nina Simone needs to meet the same indifference from audiences, especially Black ones, as 'Gods Of Egypt'. Seriously.
>
> — Rusty Redenbacher (@rustymk2) 9:26 PM - 1 Mar 2016

That's Me in the Corner (Maybe)

What Happened: Lena Dunham got upset that a magazine had Photoshopped her appearance on its latest cover. Only problem is, it actually hadn't.

Where It Blew Up: Instagram, blogs, media think pieces

What *Really* Happened: Lena Dunham took to Instagram this week to complain about the fact that her photo on the cover of *El Pais*' *Tentaciones* magazine had been Photoshopped without her permission:

Her comments were picked up and widely shared, prompting new discussion about the use of Photoshop and retouching of women's photographs in popular culture.

There was just one problem, as the response from *El Pais* made clear. "Of course, we are aware that any media outlet needs to be responsible for what it publishes, but this photo was previously approved by the agency, the photographer and your publicist," the paper's open letter revealed. "We acquired the photo via the Corbis agency, and we used the original that they sent us without applying any kind of retouching." To

prove it, they shared the original image (and to make nice, they offered Dunham a subscription to the magazine).

Dunham replied, once again, via Instagram:

The Takeaway: Is this a case of the right hand not knowing what the left hand was doing, because the left hand had agreed to being retouched so that the right hand couldn't even recognize it?

Cancel the Oscars, We Already Have Our Best Actress For 2017

What Happened: We all love food, but you know what would make food better? America's greatest living actress, demonstrating her versatility once again.

Where It Blew Up: Instagram, media think pieces

What *Really* Happened: And talking about actresses and Photoshopping ... look, there's no way to properly introduce it, so we're just going to share some examples of the latest Instagram feed that people are going wild over.

Welcome to Taste of Streep, an Instagram account that really does just mash-up Meryl and food. It's a simple appeal, sure, but one that's won over a lot of people in the the last few days. It's easy to see why: Not only is it a gloriously stupid idea, but it's one that no one realized they needed until they saw it. We can only hope for high-quality rip-offs to debut any minute now: Vin Diesel morphed into the side of trucks, called "Van Diesel," perhaps.

The Takeaway: How could anyone hope to add anything to this?

Enjoy it while it lasts. It's only a matter of time before you've seen this kind of thing so often that you lose your appetite.

You'll Eat Bugs. These Investors Are Betting Millions on It

Greg Sewitz and Gabi Lewis are used to people laughing at them. Three years ago the two college roommates ordered two boxes of live crickets off the Internet, the sort you might feed your pet iguana. They promptly shoved the two shoebox-sized containers of insects into the freezer. Later, they ground the tiny frozen corpses in a blender and, using Lewis' own recipe, made a batch of protein bars that replaced whey powder with cricket dust.

They thought the bars tasted great, so they started selling them at gyms, health food stores, farmer's markets and their own online store. It was hard at first. Some people were excited at the thought of eating crickets. They do, after all, pack a lot of protein into a few calories. They even managed to get the bars on shelves in a few natural food stores in the northeast. But an awful lot of people just laughed nervously.

'Investors were always our biggest believers. They've seen crazier things.'

No matter. At least one deep-pocketed group is taking the pair quite seriously. Today Sewitz and Lewis' company, Exo, announced it has raised $4 million in a series A round of funding led by Accel Foods with participation by investors like Collaborative Fund[1], an early investor in tech companies like Kickstarter, TaskRabbit, and Lyft, as well as food companies like Hampton Creek. Exo has now raised a total of $5.6 million.

"Investors were always our biggest believers," Sewitz says. "They've seen crazier things."

Exo isn't the first to rake in dough from investors. Fellow cricket protein bar makers Chapul won a $50,000 investment from Mark Cuban on *Shark Tank* in 2014, and Tiny Farms, a company that develops technology for raising insects, announced an undisclosed amount of funding earlier this year from Arielle Zuckerberg (Mark Zuckerberg's sister), Investors Circle, and former Bain & Company consultant Drew Fink.

That may seem like a lot people betting a lot of money on a foodstuff historically considered taboo in Europe and North America. Sure, 2 billion people around the world already eat insects. Yes, the United Nations says insects could play a crucial role in feeding a growing global population without wrecking the environment. And yeah, several insect protein companies have run successful crowdfunding campaigns, proving that there's at least a niche market for edible insects. But will enough people be able to get over the stigma of eating insects to make these investments worthwhile?

Better Than Processed

The key, Sewitz believes, is in using insect protein in foods that people already eat, rather than encouraging people to eat whole insects. According to a *Consumer Reports* taste test, most insect bars don't have even a hint of "insect grossness." That's because the the powder doesn't have a strong taste, Sewitz says, which means you can use it to add protein to a wide variety of foods. "We don't view ourselves as a protein bar company, we view ourselves as an insect protein company," says Sewitz. "We'll use this as a replacement for whey powder, soy powder, and eventually beef and eggs."

Tiny Farms investor Fink agrees with this approach. "What I see going mainstream is the use of cricket flour as an additive in more and more consumer products, whether it's bread, pasta, crackers, etc.," he says.

Lauren Jupiter, managing partner at Accel Foods, an investor in Exo, agrees. "Portable protein is a $55 billion market across snack bars, protein powder and protein ingredients," she says. "This total global market expands to $371 billion when considering the applications for crickets and cricket ingredients in pet food, nutraceuticals, livestock feed, and other industrial uses."

On the human consumer side, Fink cites the enduring popularity of high-protein diets, concerns about the environmental costs of meat, and the growing aversion to highly processed foods as trends that work in favor of the high-insect diet. Plant-based meat alternatives, he points out, often are made with soy or wheat gluten—two ingredients many people are allergic to or have difficulty digesting. "[Most meat alternatives] are as processed as anything you can find," Fink says. "Insect protein gives that consumer an environmentally friendly alternative to animal protein with minimal modification from its natural state."

That's a big part of Exo's pitch. Whey protein bars often contain many additives, Sewitz says. He and Lewis made the first batch of Exo bars with about 10 common ingredients they bought at the local natural foods store. Lewis and Sewitz no longer make the bars at home—they outsource to a manufacturer now—but they are keeping the ingredient list slim.

The big bet, in other words, is that people would rather eat ground-up crickets than a bunch of exotic-sounding additives whose names they can't pronounce. That might not be such a funny idea after all.

[1] UPDATE 12:15 PM ET 03/7/16: An earlier version of this article incorrectly stated that Collaborative Fund was the lead investor in Exo's series A. It was actually Accel Foods.