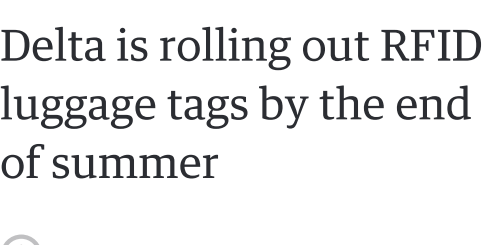


B@d P@sswOrd

Bad Password is a weekly hacking and security column examining infosec and our ever-eroding "privacy."

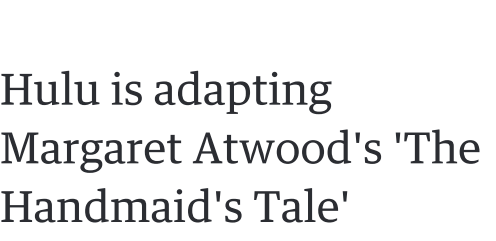
See all articles

Latest in Culture



Delta is rolling out RFID luggage tags by the end of summer

11h ago



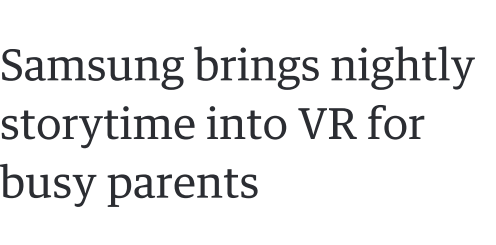
Hulu is adapting Margaret Atwood's 'The Handmaid's Tale'

14h ago



Who hacked Facebook?

17h ago



Samsung brings nightly storytime into VR for busy parents

19h ago

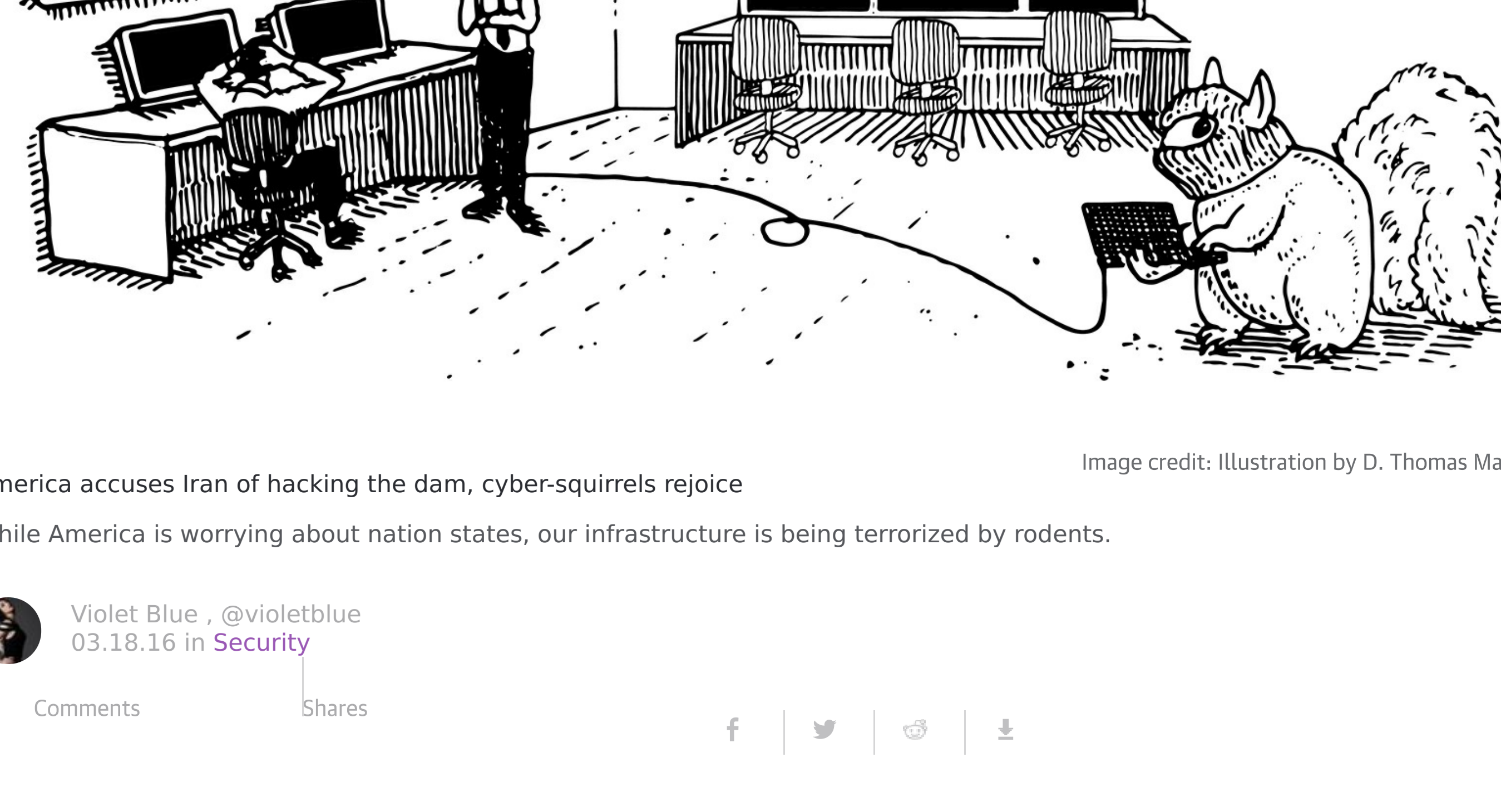


Image credit: Illustration by D. Thomas Magee

America accuses Iran of hacking the dam, cyber-squirrels rejoice

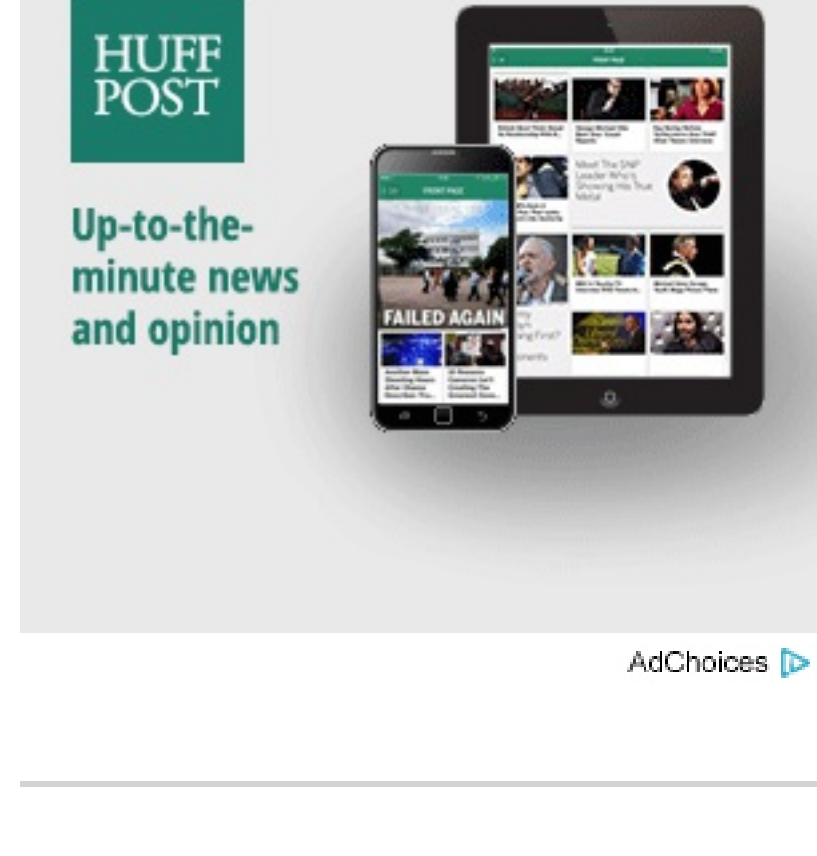
While America is worrying about nation states, our infrastructure is being terrorized by rodents.

Violet Blue . @violetblue
03.18.16 in Security

Comments Shares

f t e d

Illustration by D. Thomas Magee



Ad Choices

Sponsored Links by Taboola

Why High End Brands Are Now Company Cars

Christmas fairy lights may ruin your WiFi, warns Ofcom

10 Incredible Bicycle Concepts Of The Future

Facebook

As cyber-geddon stories go, Middle Eastern countries hacking into US dams or power grids and making stuff go haywire sounds like the plot for a not-so-subtly racist Hollywood scare flick. But that's the story we got when news outlets, citing unnamed sources, recently reported the Obama administration would be calling out Iranian hackers as the culprits behind a malicious 2013 breach at a New York dam.

Outlets reported at the time of the disclosure that hackers were "unable to get into the full dam system, but could take control of the flood gates."

The news drama here hinges on reports that hackers accessed the dam's floodgate controls. The Bowman Avenue Dam near Rye Brook, New York, whose only purpose is to mitigate flooding, does have a computer-operated sluice gate ... er, it does now, anyway.

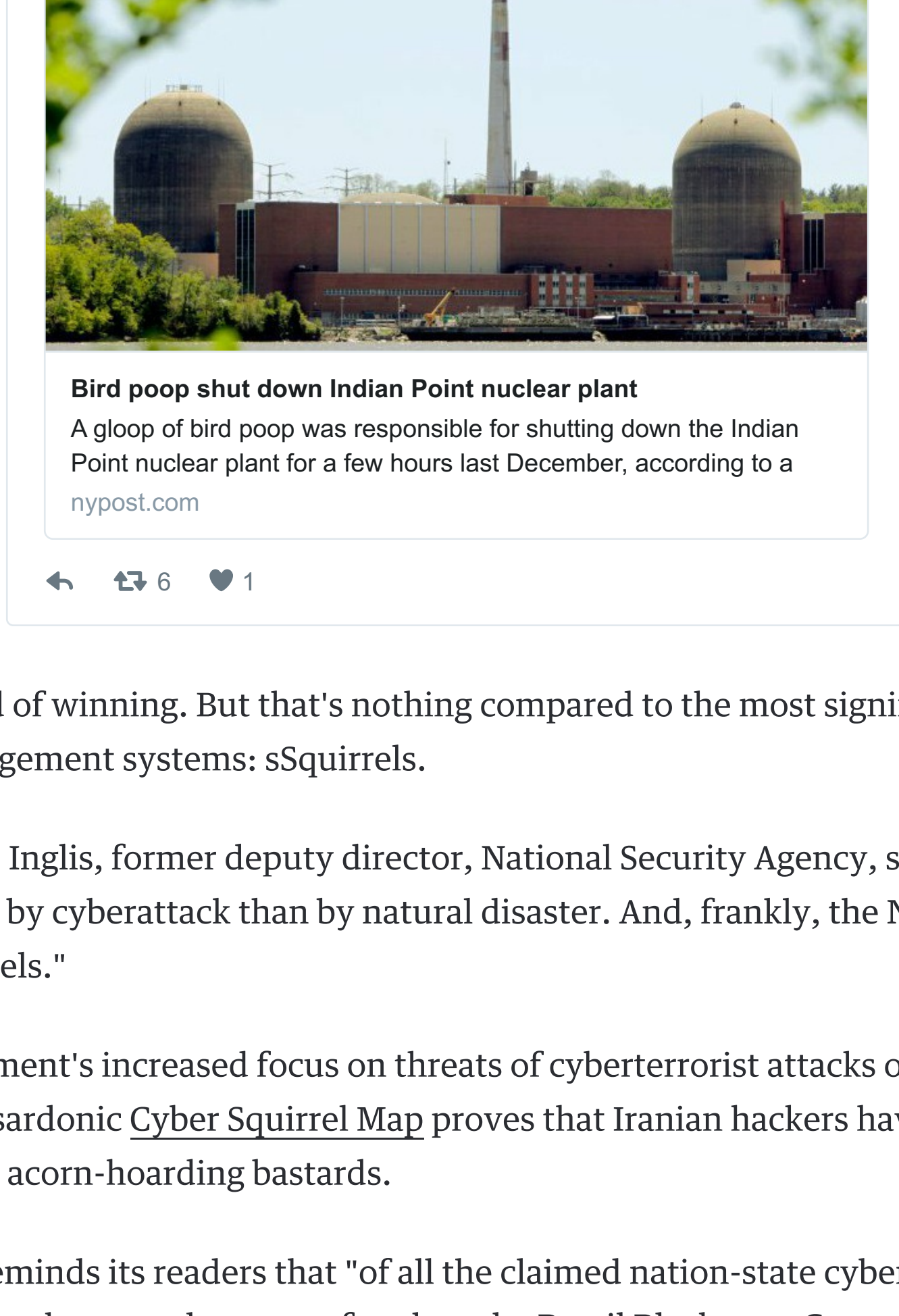
After the Department of Homeland Security approached the city of Rye about investigating the dam in 2013, Marcus Serrano, Rye city manager, told local press something that's not making it into this week's resurgence of stories about Iranian hackers. In local news outlet My Rye, Mr. Serrano said:

"In or about June 2013, a sluice gate was added to the Dam, in order to help control the flow of water and assist with flood mitigation during storm events. The gate was designed to be opened and closed via computer; however, despite a ribbon cutting ceremony, the gate was never fully operational, and remained non-functioning through the DHS investigation. In any event, based on information provided to us, at no time was the sluice gate ever manipulated by unauthorized users outside of the city.

Subsequent to and after taking certain security measures consistent with the DHS report, the City did implement the sluice gate for the first time during a storm event on or about April 30 to May 1, 2014."

So the damn dam, which in this case was really more like an artist's rendering of a dam, was operating at less than a minimum. The Iranian "cyberspies" who "had access to [the dam's] control system" had it only in theory.

It seems like someone's trying really hard to make Iranian hackers seem more dangerous than bird poop.



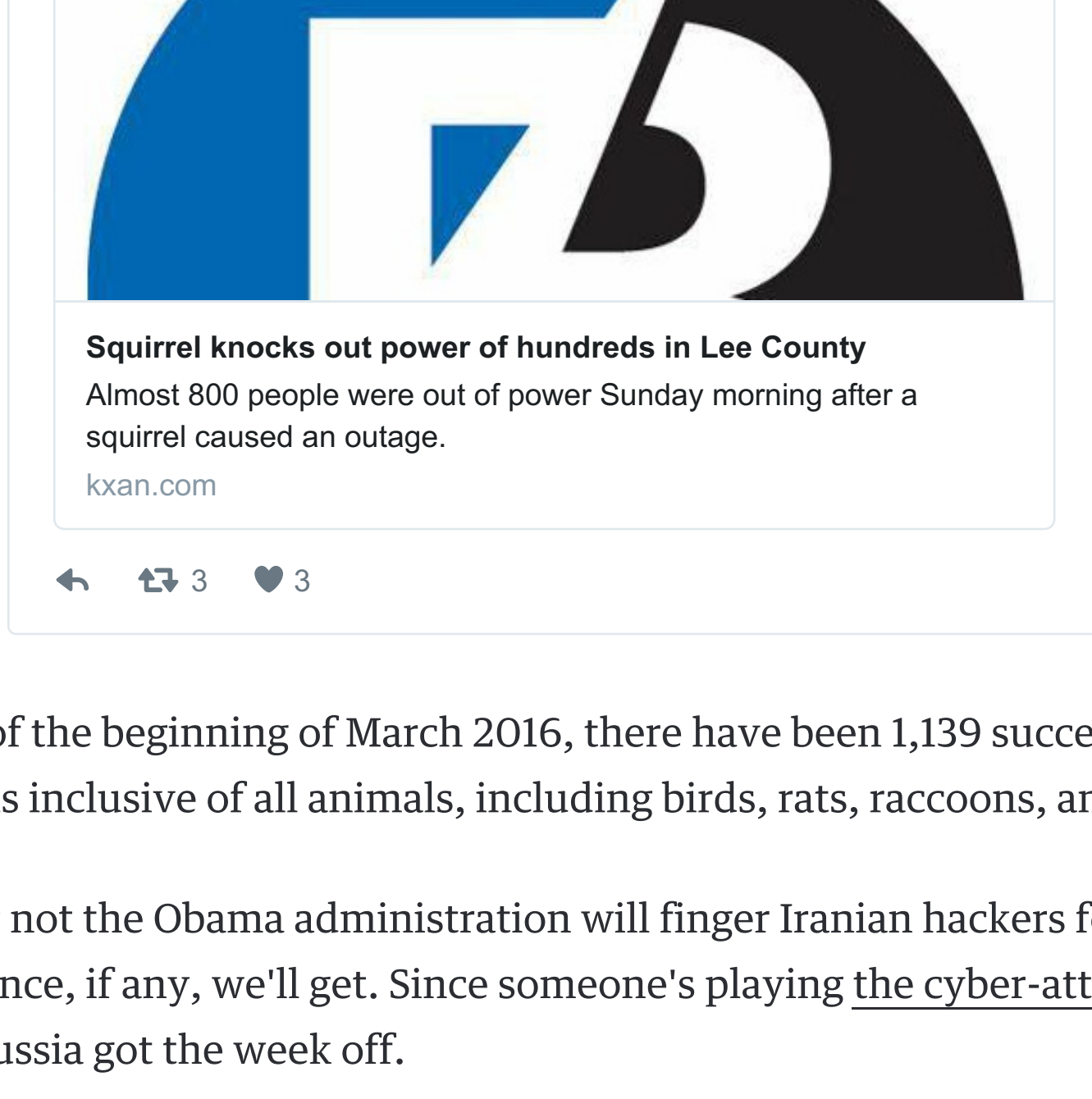
If it's a contest, bird poop is kind of winning. But that's nothing compared to the most significant and active threat to our nation's industrial control management systems: sSquirrels.

In a July 2015 comment, John C. Inglis, former deputy director, National Security Agency, said, "I don't think paralysis [of the electrical grid] is more likely by cyberattack than by natural disaster. And, frankly, the No. 1 threat experienced to date by the US electrical grid is squirrels."

And he's right. With our government's increased focus on threats of cyberterrorist attacks on industrial control systems (like power grids), the data from the sardonic [Cyber Squirrel Map](#) proves that Iranian hackers have nothing on the leet haxxor skillz of those bushy-tailed little acorn-hoarding bastards.

To this effect, [Cyber Squirrel 1](#) reminds its readers that "of all the claimed nation-state cyber attacks that have impacted critical infrastructure that we have been made aware of such as the Brazil Blackouts, German Steel Plant event, and the Ukrainian power outages only the US lead [Stuxnet operation](#) can be confirmed at this time. We are continuing to look into the December events in the Ukraine."

When it comes to executing successful infrastructure attack ops, squirrels have any and all government-sponsored hackers beat by a mile. Late last year, the hacker behind [Cyber Squirrel](#) began collecting "all unclassified Cyber Squirrel Operations that have been released to the public that we have been able to confirm."



According to Cyber Squirrel, as of the beginning of March 2016, there have been 1,139 successful "cyber squirrel" attacks -- though the running tally of ops is inclusive of all animals, including birds, rats, raccoons, and snakes.

It remains to be seen whether or not the Obama administration will finger Iranian hackers for the dam that wasn't really hacked -- and what sort of evidence, if any, we'll get. Since someone's playing [the cyber-attribution blame game](#) here, maybe it's just that China and Russia got the week off.

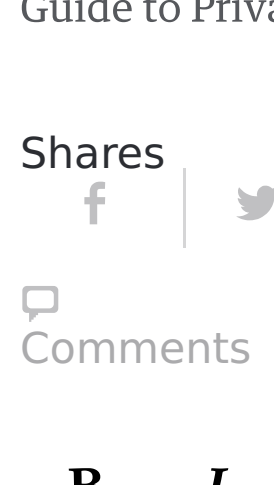
Perhaps it's part of the monster-of-the-week cybersecurity news roadshow, conveniently brought to us by a DHS that just might be desperately trying to look like it's really doing stuff. The madness around this dam -- the way it just doesn't add up but feels part of the general cybersecurity mood right now -- along with the Apple encryption mania, feels like a kind of hysteria in the air, one that news outlets seem to breathe in and catch.

Surely, this dam coming back into the news so circumspect with fact is a harbinger: The next Big Bad to be leveraged for scaring up both legislation and will be this sort of disclosure of industrial control systems (and switches).

But the beauty of Cyber Squirrel at a time like this is that it's all about perspective. That when it comes to domestic cybersecurity, authorities (and infosec) should be giving less attention to vague threats, and more to problems at home -- like getting our infrastructure systems properly patched.

In the meantime, for whatever the hell happened (or not) at the Bowman Avenue Dam, my money's on squirrels.

In this article: badpassword, culture, cybersecurity, cyberspies, cybersquirrel, DHS, electricalgrid, hackers, indianpoint, internet, security, stuxnet



By Violet Blue
@violetblue

Ms. Violet Blue (tinynibbles.com, @violetblue) is a freelance investigative reporter on hacking and cybercrime, as well as a noted columnist. She is an advisor to PeerLyst and Without My Consent, as well as a member of the Internet Press Guild. Ms. Blue has made regular appearances on CNN and The Oprah Winfrey Show and is regularly interviewed, quoted, and featured in a variety of outlets and publications that include CNN, BBC, Newsweek, and the Wall Street Journal. She has authored and edited award-winning, best selling books in eight translations and has been a sex columnist for the San Francisco Chronicle. Her talks at conferences include ETech, LeWeb, CCC, and the Forbes Brand Leadership Conference, in addition to two Google Tech Talks. The London Times named Blue one of "40 bloggers who really count." Ms. Blue is the author of The Smart Girl's Guide to Privacy.

Shares

Comments

Sign In

Rich text editor for comments with bold, italic, underline, and list options.

Submit

Show 7 Comments

3h ago in Space

Watch a 360-degree video of SpaceX's rocket landing at sea

It's like watching a show from the best seat in the house.

By M. Moon, 3h ago

8h ago in Robots

Puma's robotic running companion can keep pace with Usain Bolt

Too bad the BeatBot is so expensive it's only available to Puma's sponsored athletes, then.

By T. Seppala, 6h ago

8h ago in Wearables
Xiaomi's smartwatch for kids costs less than \$50



04.25.16
Double Play: How sports games reach deeper into gamers' pockets
The sci-fi network is the first entertainment channel to plug into Alexa.
By R. Starr, 04.25.16

Public Access



9h ago in Gadgetry
Ask Alexa what's playing on Syfy
The sci-fi network is the first entertainment channel to plug into Alexa.
By D. Lumb, 9h ago

More Stories

From around the web

- Why High End Brands Are Now Company Cars**
Financial Times
- Christmas fairy lights may ruin your WiFi, warns Ofcom**
The Inquirer
- 10 Incredible Bicycle Concepts Of The Future**
10amazing.com
- TOP 10 Best Paying Jobs in 2016**
buzzofun
- 12 Most Useful Apps Guys Must Have**
TopMensMag

Sponsored Links by Taboola

About

- About Engadget
- About Our Ads
- Advertise
- Brand Kit
- Contact Us
- RSS Feed

Sections

- Reviews
- Gear
- Culture
- Entertainment
- Gaming
- Science
- Public Access
- Video

Contribute

- Public Access
- Send us a tip!
- Support

International

- Español
- Deutschland
- UK

Apps

- Android
- iPhone
- iPad

Join Our Newsletter

Sign up for our newsletter

Subscribe

Follow Us

Aol Tech

© 2016 AOL Inc. All rights reserved.

[Reprints and Permissions](#) [Privacy Policy](#) [Terms of Use](#) [Trademarks](#) [Advertise](#)