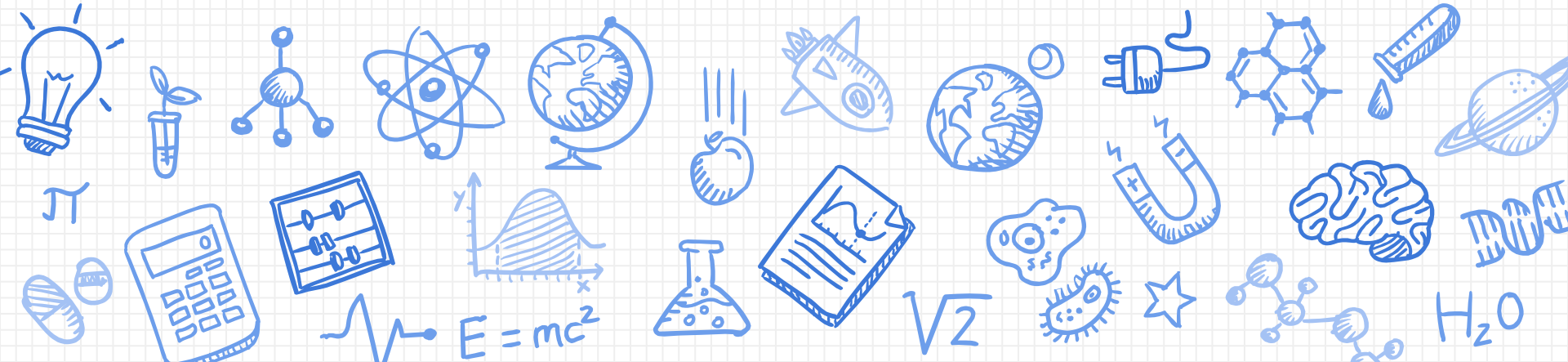
texas civic tech project

txctp.org

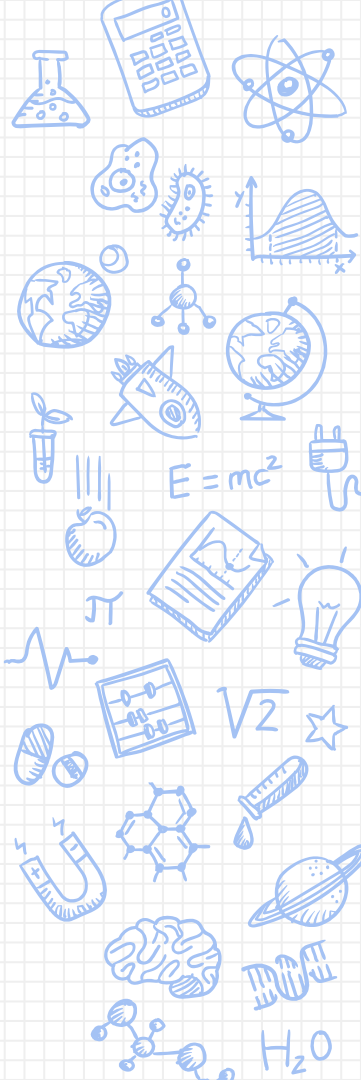
Welcome members of ISSS to CTP!!



CFAA

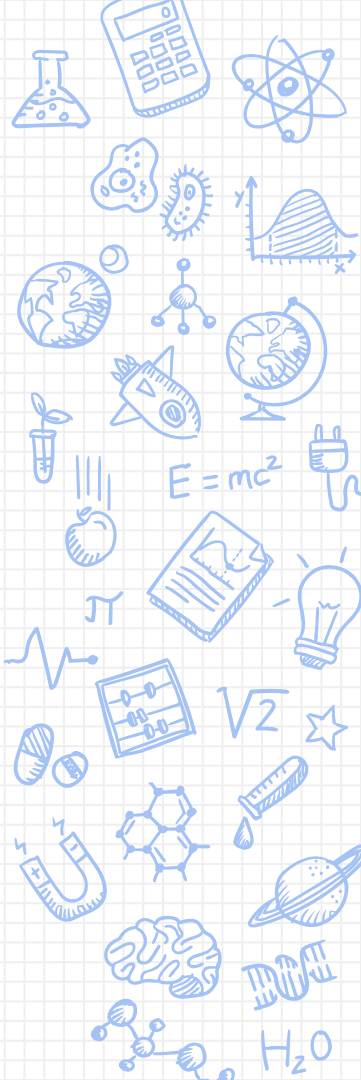
Computer Fraud and Abuse Act

- Passed in 1986 as a response to hacking panic
  - WarGames
  - 2000 computers in the US when passed
- Cyber security law
- Criminalizes “computer trespassing,” which is meant to cover hacking overall
  - law makes it illegal to intentionally access a computer without authorization or in excess of authorization
  - Definitions are very loose
- Has been used to prosecute everything from hacking to intellectual property violations



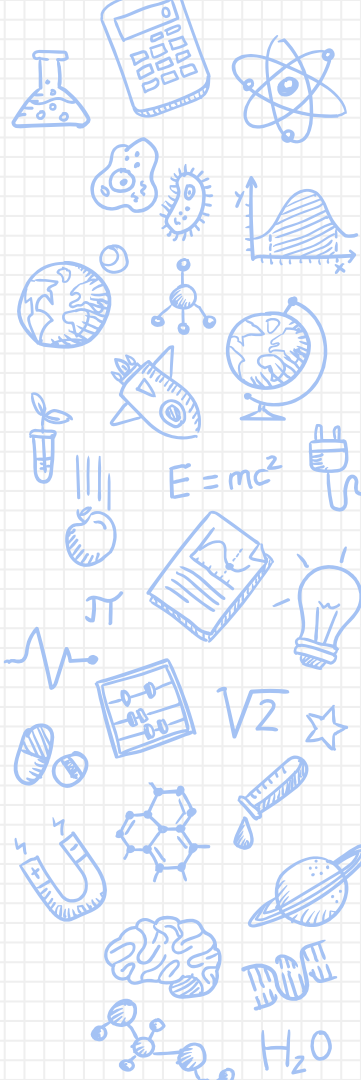
CFAA Issues

1. Overly broad
    a. “Authorization” can mean many things
    b. You could be jailed over ToS violations
2. Poorly written
    a. Redundancies => individuals can be tried for the same crime more than once under different provisions
3. Hurts Security Research
    a. Not all companies have robust bug finding programs
    b. Fear of being prosecuted



Aaron Swartz

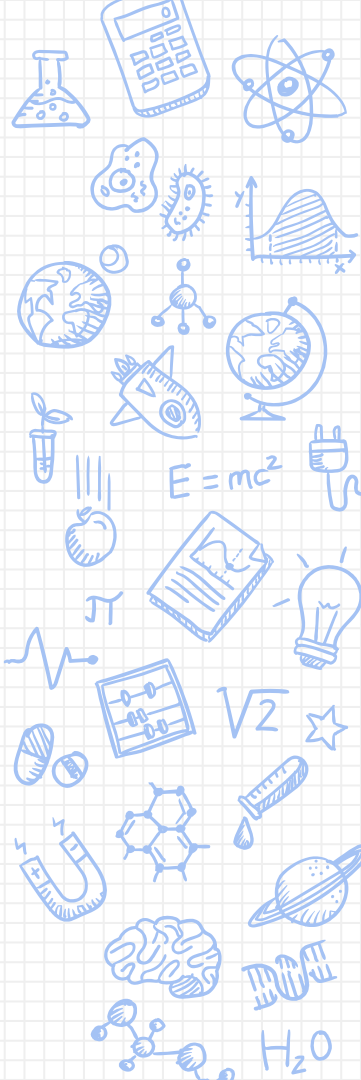
- Co-founder of reddit
- Believed in a freer internet
  - Left an unattended computer in MIT's closet to download MIT journals from JSTOR
- Was prosecuted under the CFAA
  - 11 conts
  - 35+ years jail time
- Committed suicide
- Led many to believe that the CFAA was flawed, too big a hammer



Aaron's Law

Amendments to CFAA by Ron Wyden #og

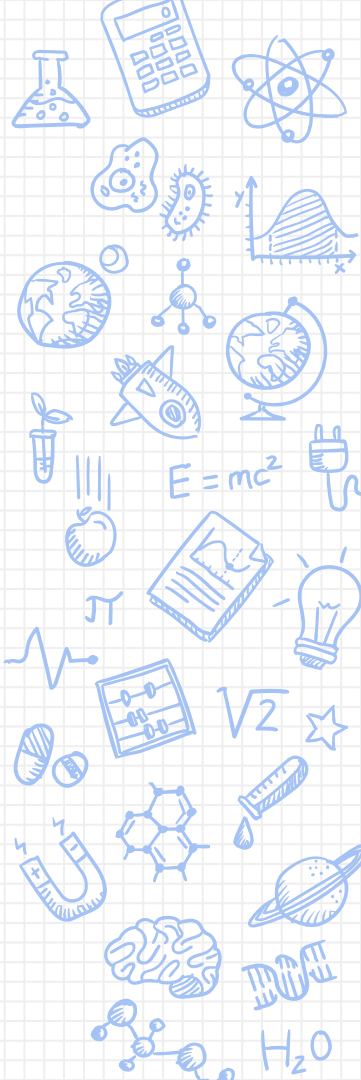
- Proposed in 2013
  - Tries to fix the overly broad aspect of CFAA by removing terms of service
  - Never passed
- Proposed again in 2015 with both (D) and (R) cosponsors
  - Again, stalled



Other CFAA Issues

More efforts to make it worse than better

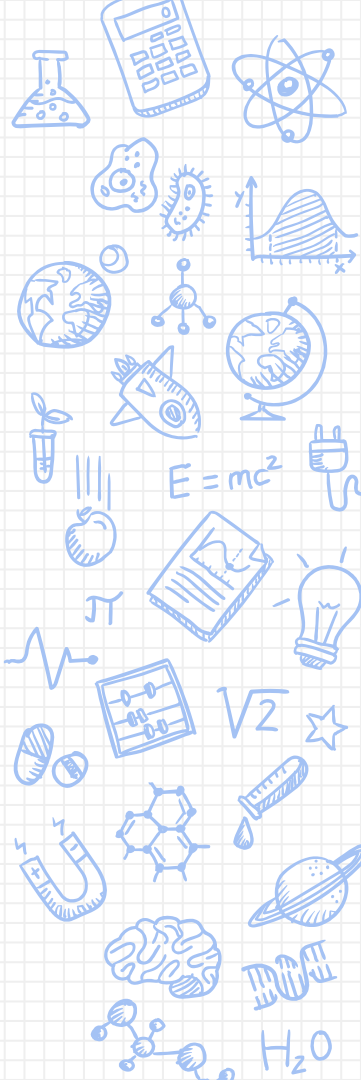
- 2001: Patriot Act further expanded the CFAA
  - increasing both its penalties and its effectiveness as a prosecution tool
- 2008: Identity Theft Enforcement and Restitution Act
  - Cybercrime, defined “loss”
- 2015: Obama wanted to expand it to make cybercrime harder (again)



Supreme Court / Scraping

Van Buren v. United States (2020)

- Nathan Van Buren = > accused of taking money in exchange in a sting operation for looking up a license plate in a police database
- Convicted under CFAA
  - He is arguing that he should not be prosecuted under a hacking law, not that he did not commit a crime
- Has not voted yet



Supreme Court / Scraping

Scraping

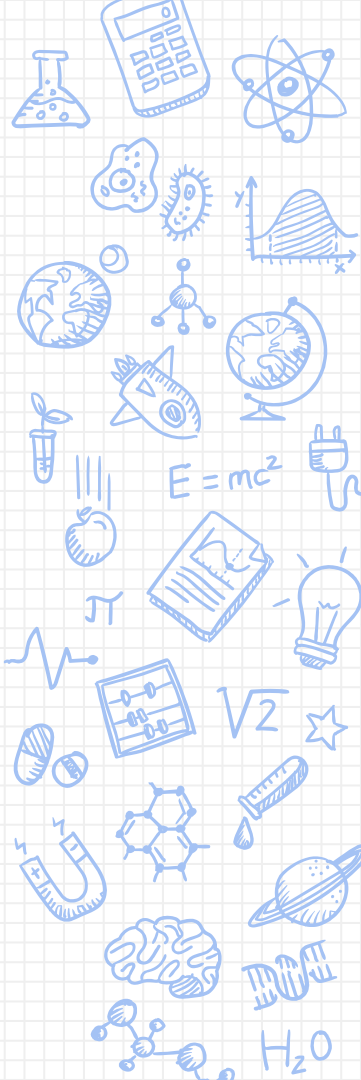
- Justice Dept has tried to prosecute scraping under CFAA before
- Sites try to stop it, put it in their ToS
- Can you prosecute someone for visiting an obscure URL?

City of Fullerton

- http://cityoffullerton.com/outbox

Parler

- @donk_eby scraped thousands of videos which were used in the impeachment hearings and trials

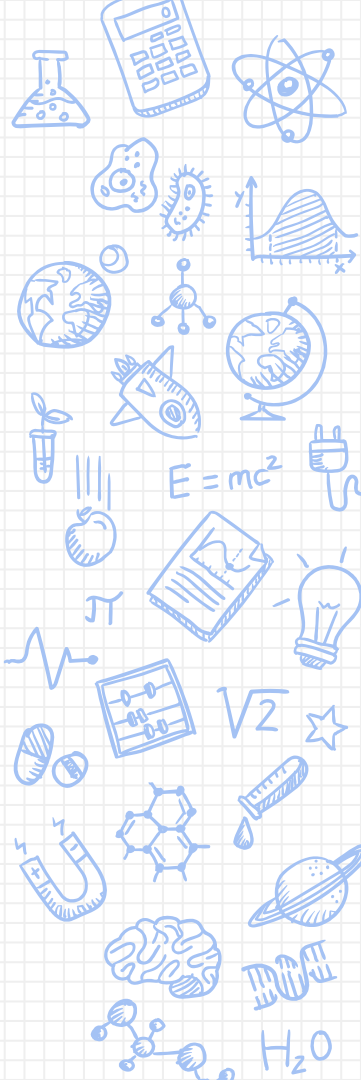


LinkedIn vs. hiQ Labs

hiQ scraped LinkedIn profiles and offered analytics to employers

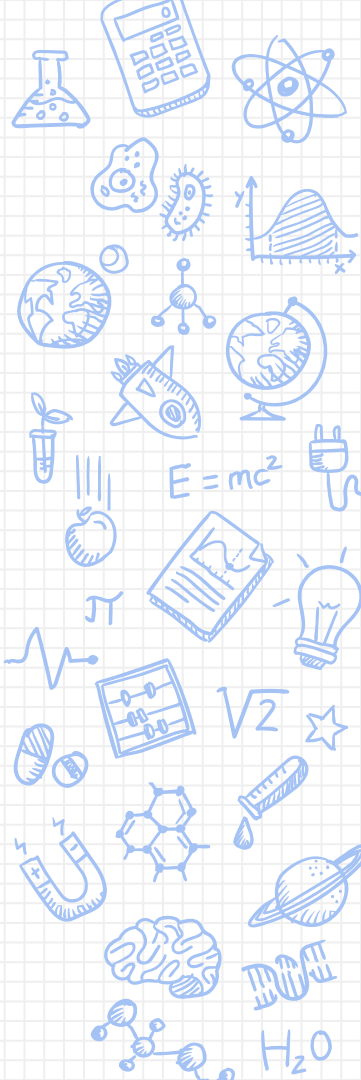
- Accesses public information and does not login as anybody (see. FB vs. Power Ventures)
- LinkedIn sent a cease and desist
- Ninth Circuit ruled that it was fine because the info was public

Conflicting: 1st Circuit have ruled against scraping (EF Cultural Travel BV v. Explorica, Inc.)



The US Government Hacking Others

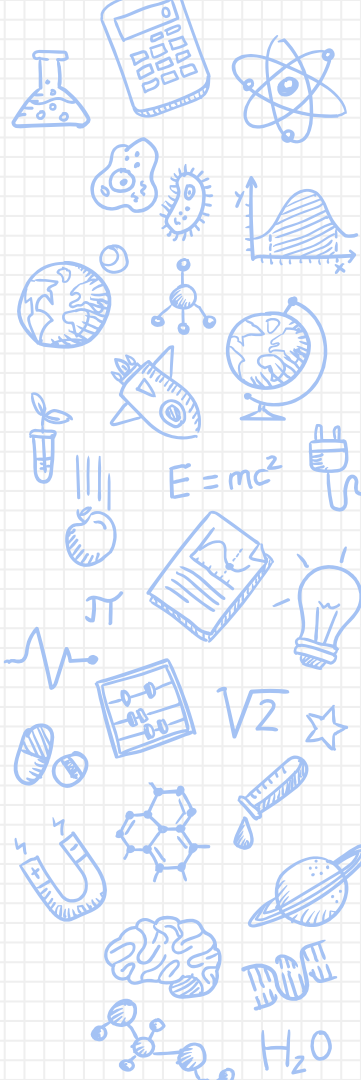
- Intelligence Gathering and Surveillance
- Snowden Leaks
  - PRISM
  - FiveEyes
    - Australia, Canada, New Zealand, the United Kingdom, and the United States alliance
    - Spying on each other's citizens and sharing surveillance info
    - Led to 14 eyes



The US Government Hacking Others

Snowden Leaks

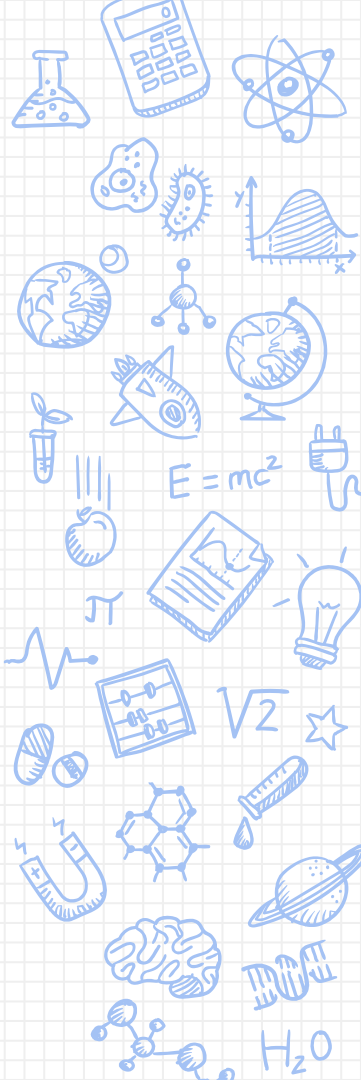
- U.S. spied on Brazil, France, Mexico, Britain, China, Germany, and Spain, as well as 35 world leaders
- Goal was to create a global network of information



The US Government Hacking Others

Mostly all of this is done through **covert action**

- US is allowed to undertake intelligence activities that seeks to influence the decision making of an adversary
  - propaganda, political action, or paramilitary activities
- Not acknowledged by the country or service that does it
- Expanded to cyber in 2018, but probably was happening before that



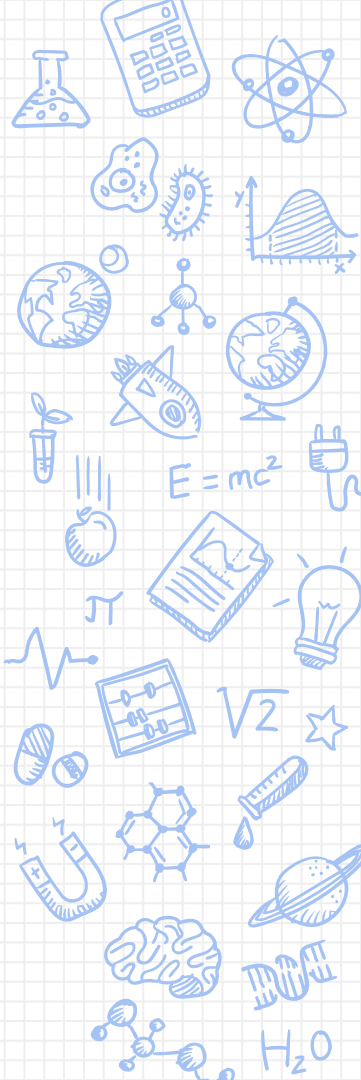
From EO 12,333: "Covert action means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but **does not include**:

a. Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
b. Traditional diplomatic or military activities or routine support to such activities;
c. Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
d. Activities to provide routine support to the overt activities (other than activities described in paragraph (a), (b), or (c)) of other United States Government agencies abroad."

The US Government Hacking Others

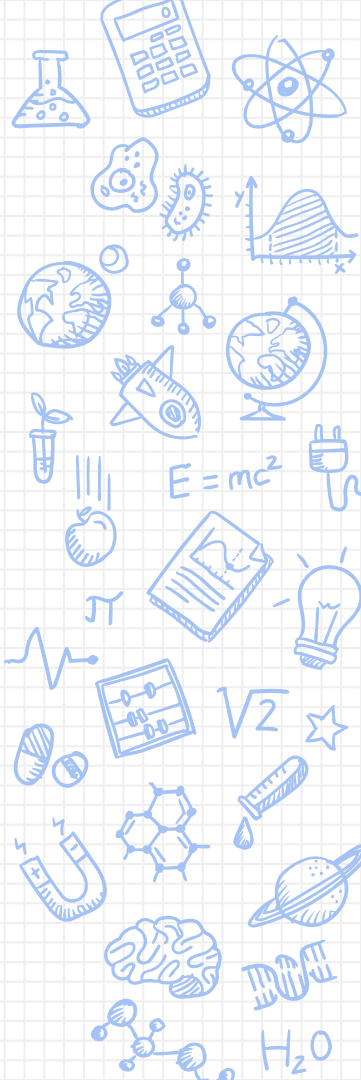
Covert operations

- Stuxnet (2010)
  - Iran Nuclear program hack
  - *maybe* led by US and Israel intelligence agencies
  - Bug that caused 1000 Iranian centrifuges that enriched uranium to spin too fast and break
  - First cyber “weapon”



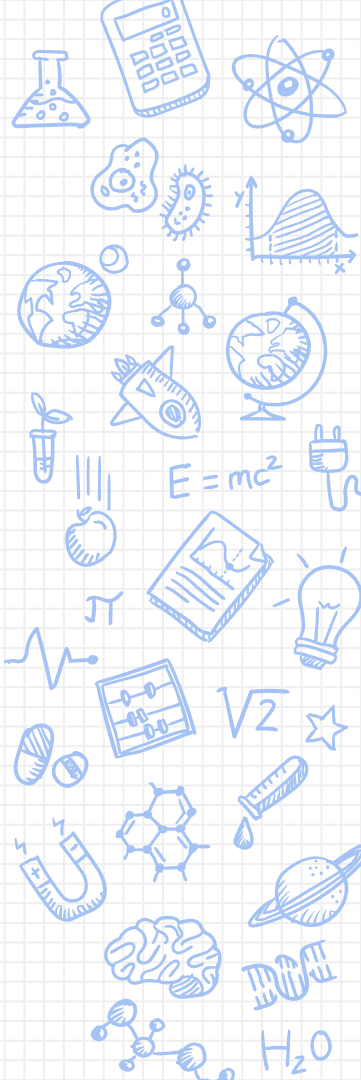
The US Government Hacking Others

- U.S Cyber Command founded in 2009
- 2011: White House published an "International Strategy for Cyberspace"
  - that reserved the right to use military force in response to a cyberattack
- CYBERCOM was intended to serve as a defensive branch



The US Government Hacking Others

- “persistent engagement”
  - Continuously engage in cyberwarfare, deterring attacks on the U.S
- Gunboat diplomacy
- Aggressive action against hacking groups, and troll farms during the election cycle



The US Government Hacking Others

U.S. Escalates Online Attacks on Russia's Power Grid

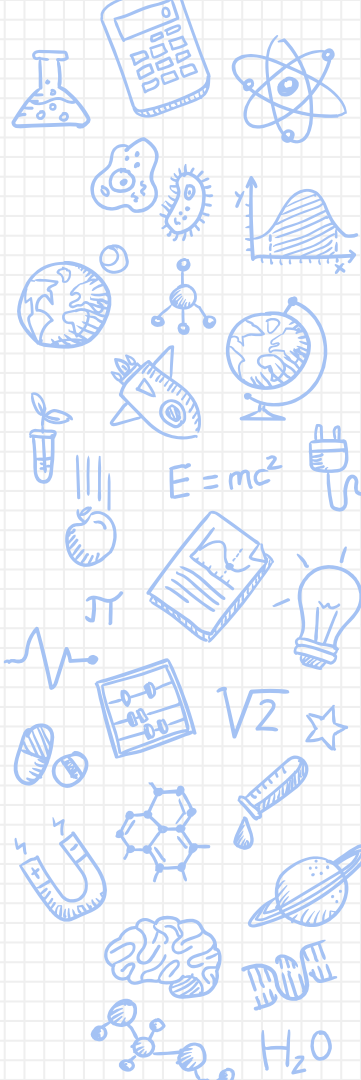
The US Government getting pwn3d

OPM hack

Solarwinds

Microsoft Exchange

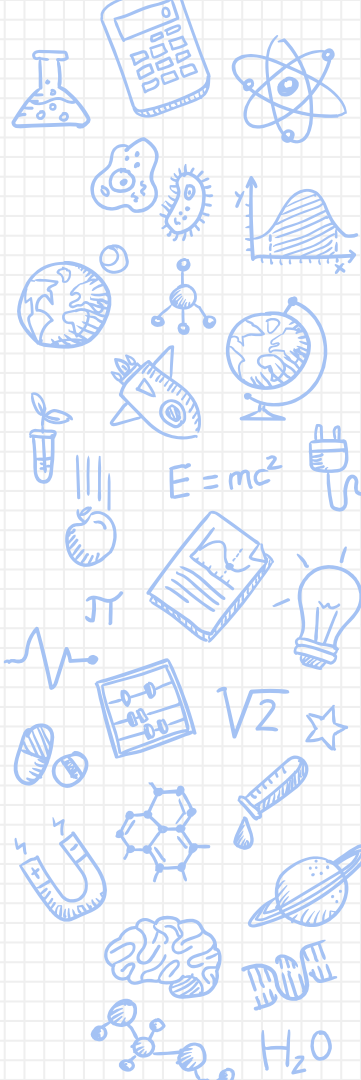
Infrastructure



The US Government getting pwn3d

OPM (Office of Personnel Management) hack

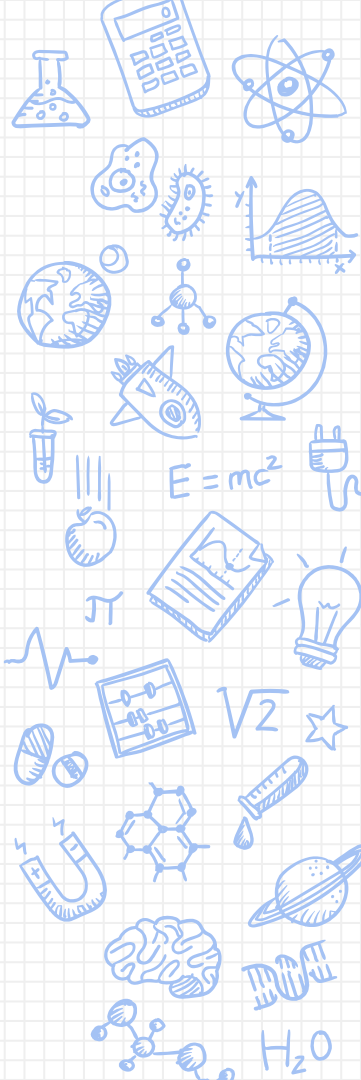
- Started off with a hack into the background check providers
  - OPM decided to “gather intelligence” and wipe the system a few months later
- Hackers installed a backdoor and keylogger
  - Wiping the system did not delete the backdoor
- **OPM did not have 2FA**
  - Took a year before realizing that the attackers were still present
- Gained private information



The US Government getting pwn3d

SolarWinds

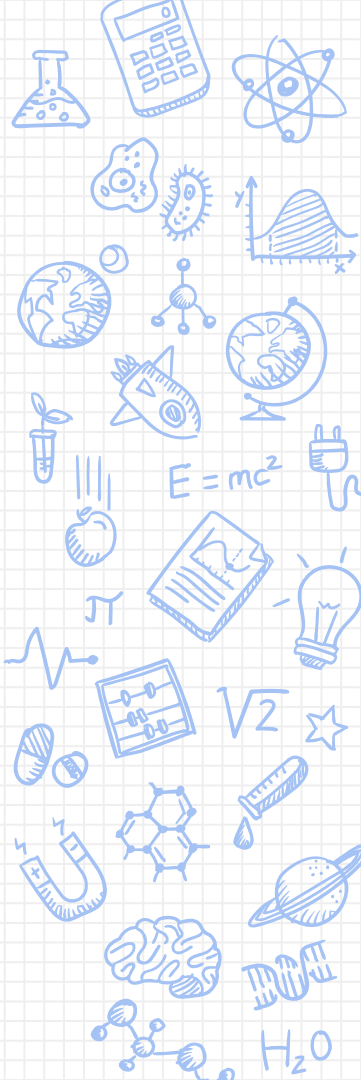
- Network management software
- Hackers obtained access to updating platform and sent malicious updates
- 18,000+ organizations affected including DOJ, Microsoft
- Solarwinds said **bad intern password**
- Procurement
- Attacked and gain control of systems



The US Government getting pwn3d

Solarwinds

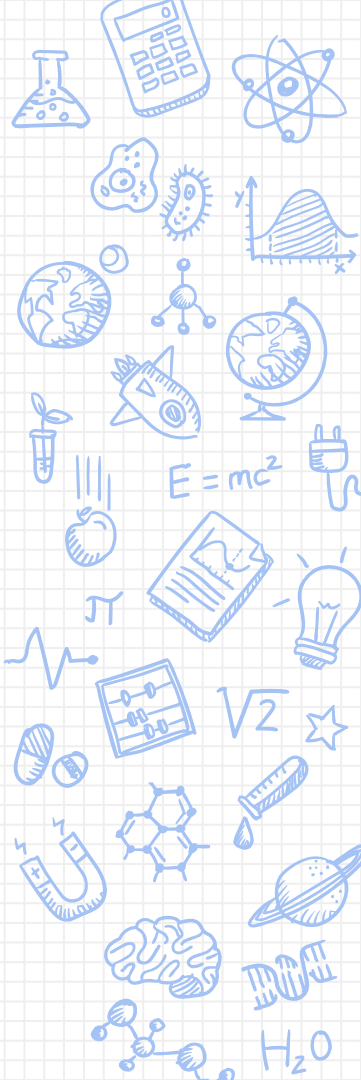
- First attacked in 2019
- “Early warning” sensors placed by Cyber Command and the National Security Agency deep inside foreign networks to detect brewing attacks clearly failed.
- FireEye (private security firm) found it



The US Government getting pwn3d

Microsoft Exchange

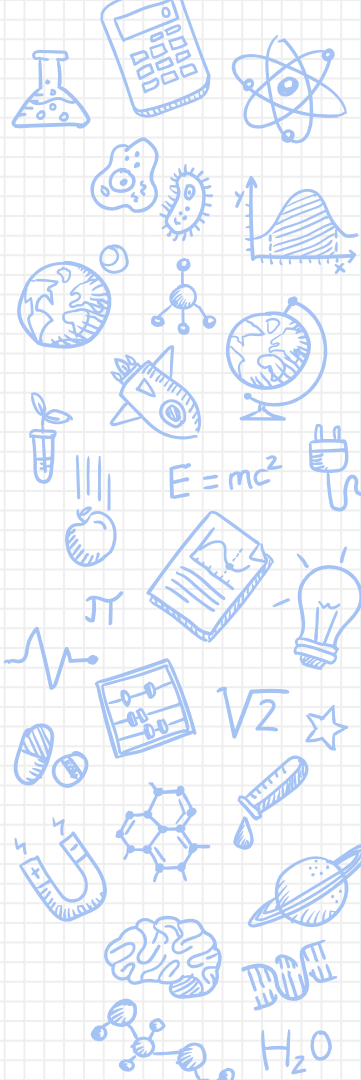
- January 2021
- Patched bugs from Exchange 2010 onward
- 30,000 organizations affected including local governments
- Incident response is extremely difficult



The US Hax YOU

Long history of government surveillance of citizens and activists around the world

- FBI's COINTELPRO
- Post 9/11 surveillance
- NSA programs

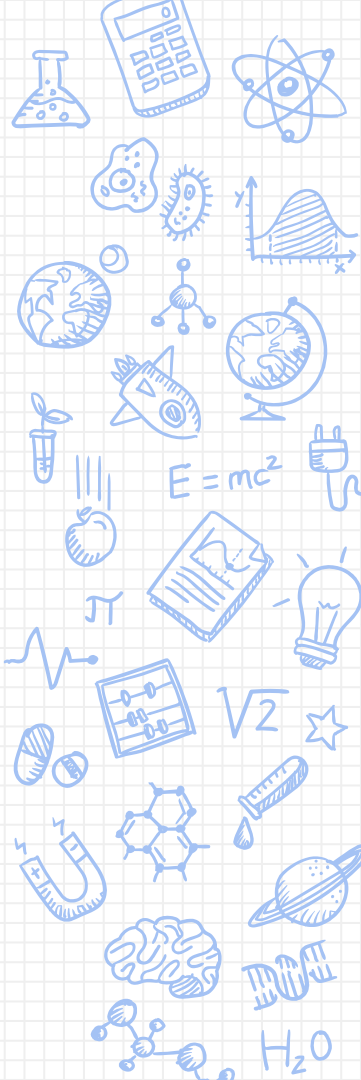


National Security and Foreign Intelligence

Foundations of surveillance

Foreign Intelligence Surveillance Act (1978)

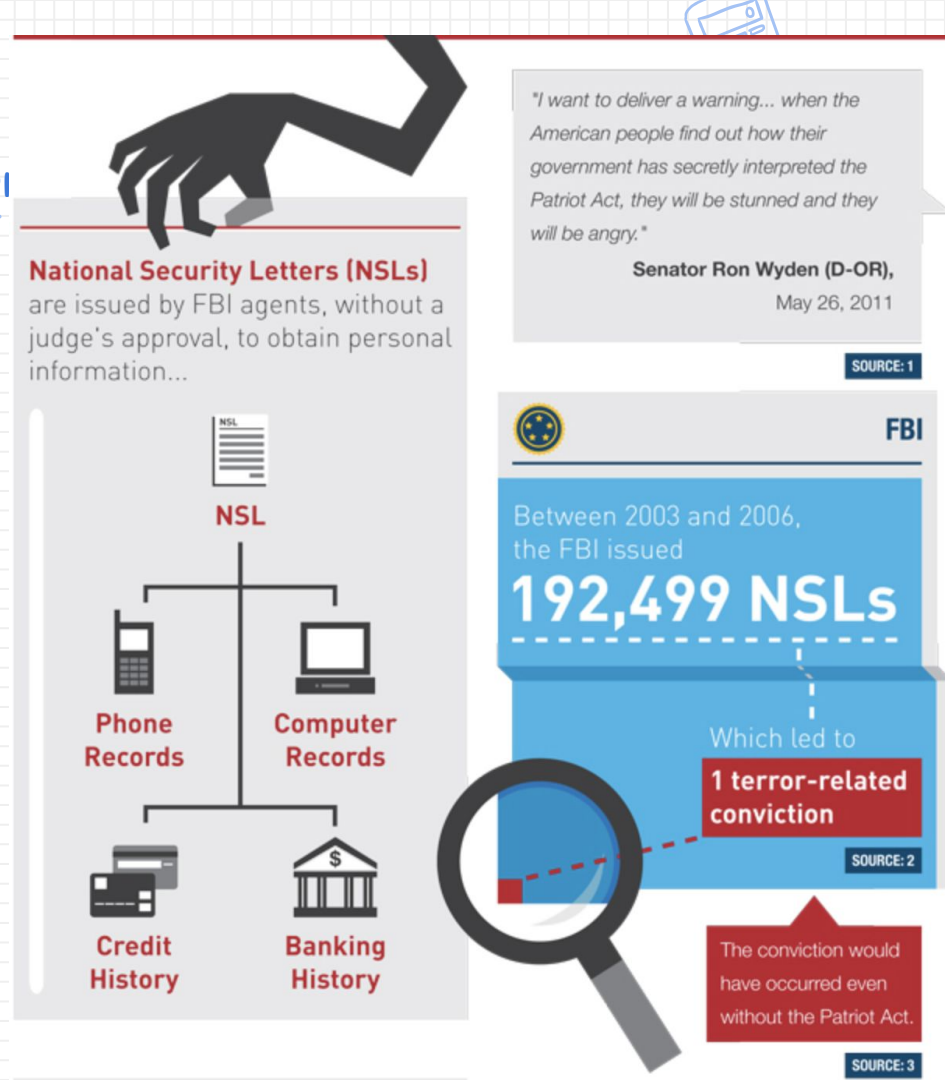
- Post Watergate
- Lets the government gather foreign intel
  - electronic surveillance, physical searches, devices that record or decode dialing, routing, etc.
- Created 2 specialized foreign intelligence courts to approve the use of FISA investigations
- Section 702 => counterterrorism tool
  - Broad, few rules, little accountability of abuse



National Security and Foreign Intelligen

PATRIOT Act

- Passed 45 days after 9/11
- Section 215: Provide “enhanced investigative tools” to assist in the prevention of future terrorist activities
- NSLs
- "Sneak & Peek" Searches
- Snowden: Section 215 lets US collect daily phone records of Americans (ended in 2015)



Policing & Data & Warrants

4th amendment

- Right to be free from “unreasonable searches and seizures.”

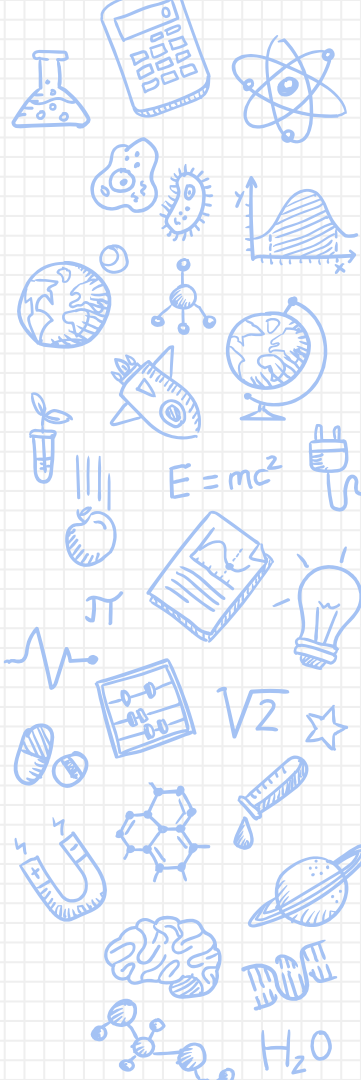
Carpenter v. United States

- Cell site location information subpoena
- Third party doctrine

New York tweets

- Can’t block

Because ad-tech vendors are private companies, cops can sidestep the Fourth Amendment hurdles because they’re buying records



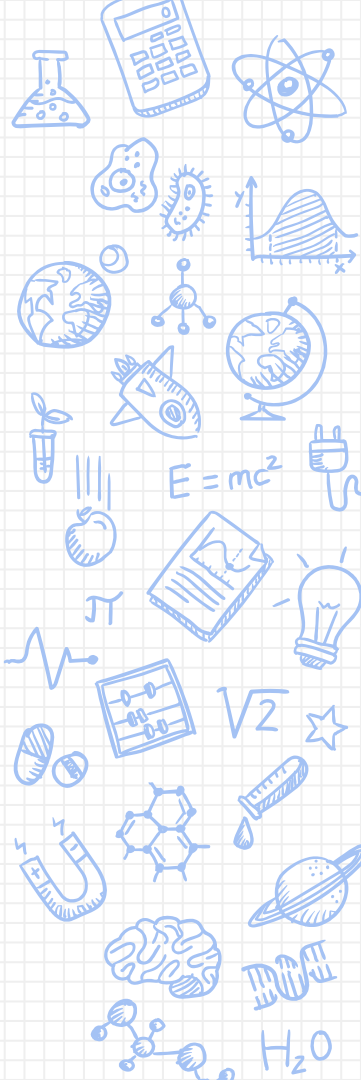
Tech = Police Goldmine

Liveramp, LexisNexis, Reuters

- All called data brokers
- Virginia
- Constantly building a digital folder on people, with pipelines to police

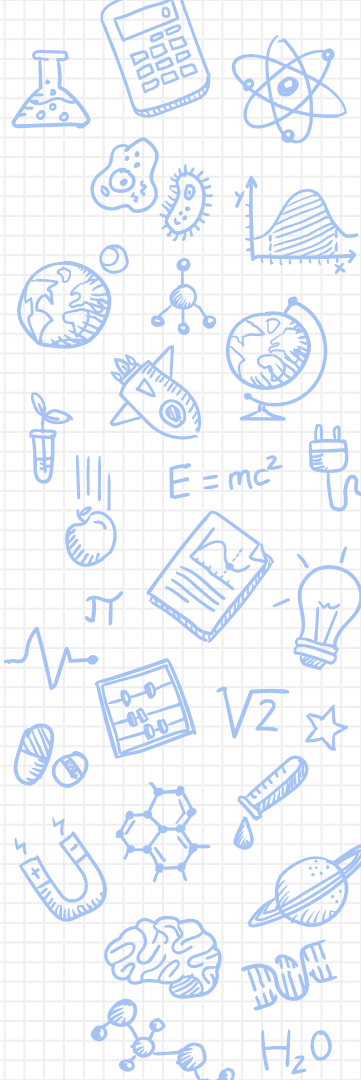
Cell-snooping tech

- Geofeedia (Baltimore)
- ICE agents
  - Cell phone activity in certain areas



The US Hax YOU

- Cellebrite
  - Tool to break into phones and retrieve data
  - Used by law enforcement



The US Hax YOU

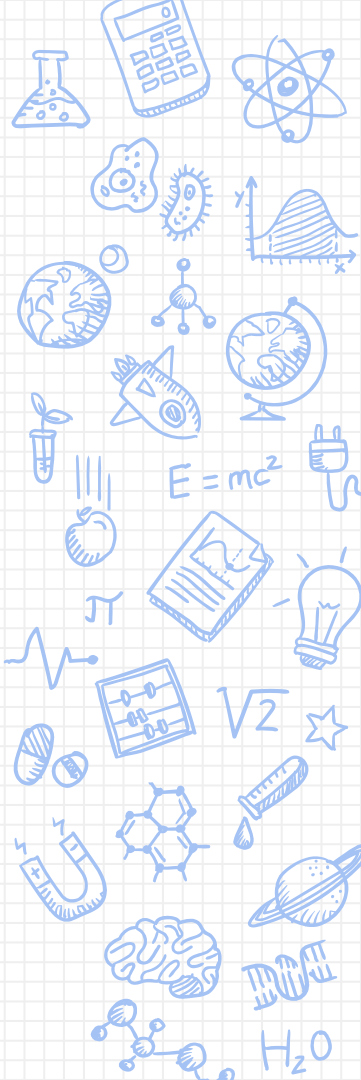
- Cellebrite
  - Tool to break into phones and retrieve data

Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective

moxie0 on 21 Apr 2021

The US Hax YOU

- Cellebrite
  - Tool to break into phones and retrieve data
  - Used by law enforcement
- Exploit showed how corrupted apps on a targeted phone could basically overwrite any data extracted by Cellebrite's tools
  - Outside party could write whatever data they want on confiscated devices.
- Brings into question the legitimacy of digital evidence



The US Hax YOU

- Cellebrite

PRIVACY AND SECURITY

Signal's Cellebrite Hack Is Already Causing Grief for the Law

Lucas Ropek
Tuesday 6:25PM

13 3

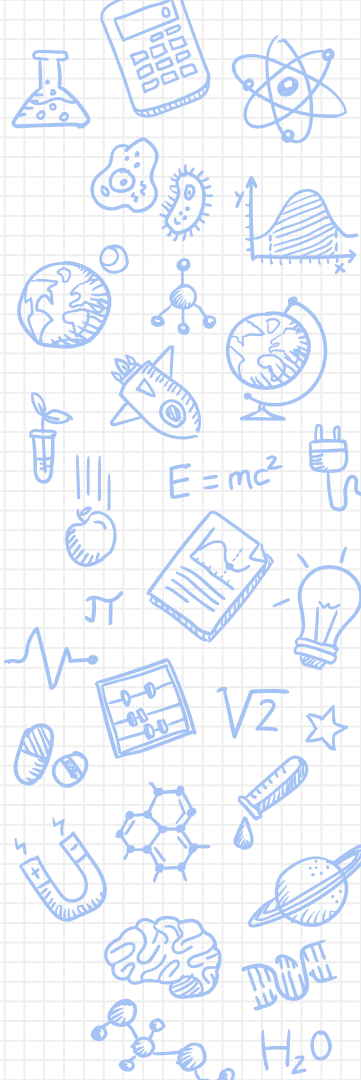
MORE FROM G/O MEDIA

READ ON GIZMODO

The US Government getting pwn3d

Classic, well known hacks

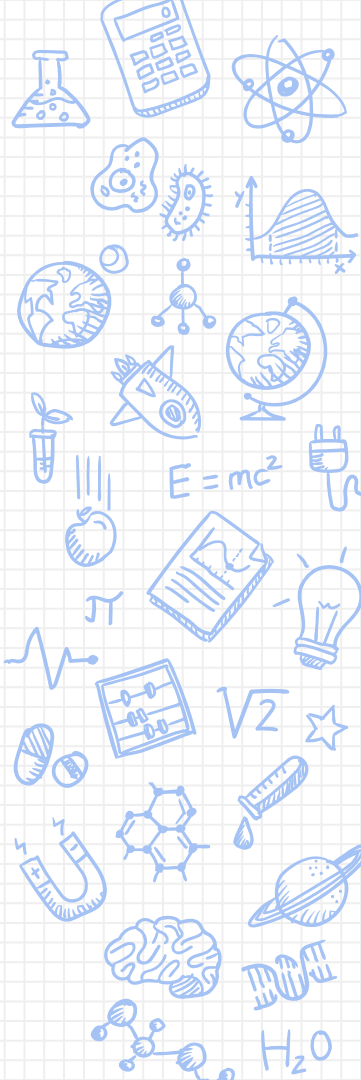
- Office of Personnel Management
  - Security clearances, noticed ssl pings to find hackers
- Stuxnet
  - Iran nuclear reactors
- Solarwinds (recent)



Governments getting pwn3d

NotPetya

- Ukraine targeted attack carried out by Russia
- Directly attacked infrastructure - $10 billion in damages
- Chernobyl radiation monitoring
- Shipping Infrastructure
- Ukraine is not as online as the U.S.



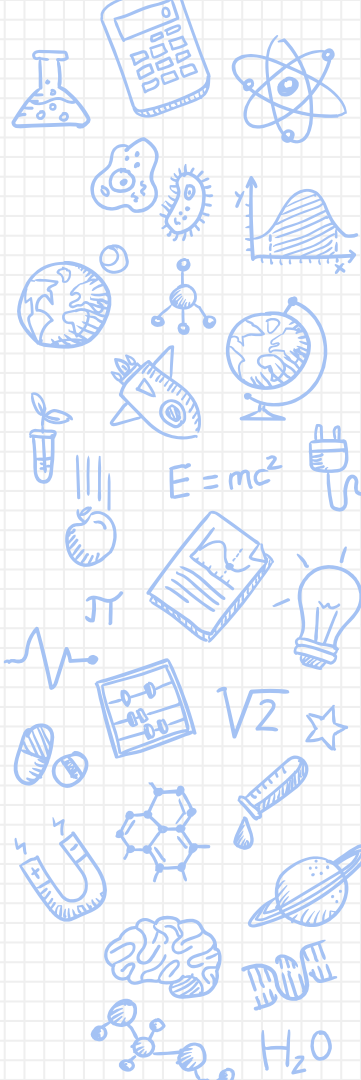
The US Government getting pwn3d

Digital works as critical infrastructure?

- Not so much of a reach anymore!

Infrastructure Hacks

- Stoplights, Water plants, Electricity Providers, Military Equipment



NEWS / **PINELLAS**

Someone tried to poison Oldsmar's water supply during hack, sheriff says

Pinellas Sheriff Bob Gualtieri said the attacker tried to raise levels of sodium hydroxide, also known as lye, by a factor of more than 100.

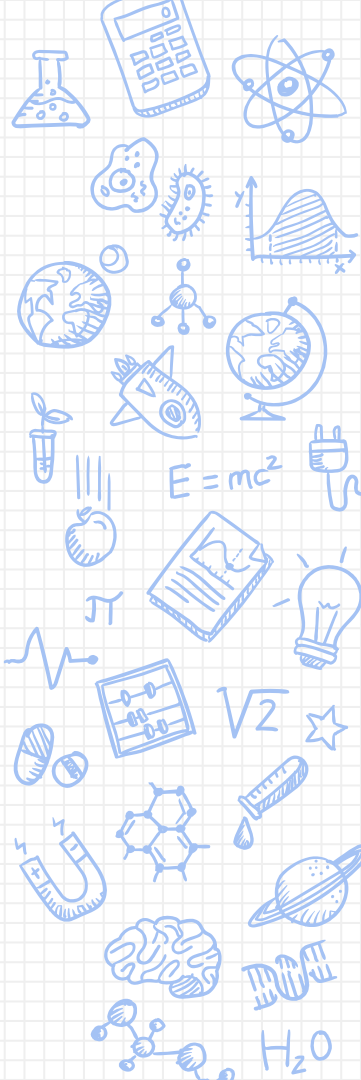
10 FEB 21

What's most interesting about the Florida water system hack? That we heard about it at all.

The US Government getting pwn3d

Infrastructure Hacks

- Stoplights, Water plants, Electricity Providers, Military Equipment
- 50k+ water facilities in the U.S
  - Many of these facilities are unattended, underfunded, and do not have someone watching the IT operations 24/7.



Discussion

- Do you think the CFAA is too broad? How do you distinguish behaviors online of white-hat and malicious hackers?