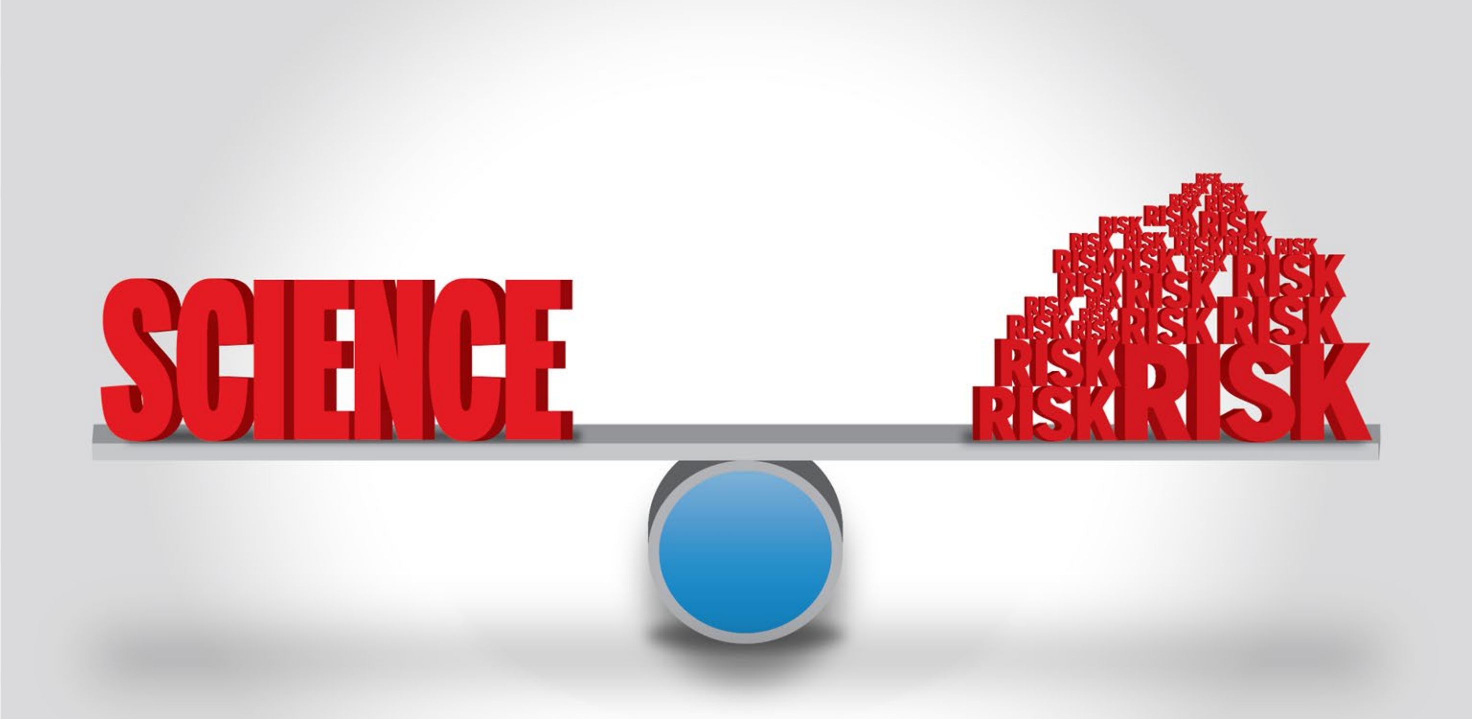
TRUSTED CI

THE NSF CYBERSECURITY CENTER OF EXCELLENCE

trustedci.org



Cybersecurity for Science: Why and How

Canada Foundation for Innovation
2021 Major Science Initiatives Workshop
March 18, 2021

Von Welch
Director, Trusted CI, the NSF Cybersecurity Center of Excellence

Cybersecurity and Open Science

A lot of research is regulated.

E.g. HIPAA, FISMA, NIST 800-171

I use "Open Science" loosely for science not guided by compliance

E.g. Astronomy, climate, physics, geology

AKA Fundamental Research

Gemini South on the summit of Cerro Pachón in Chile (left) and Gemini North on the summit of Maunakea in Hawai'i (right). Image credit: Gemini/NSF/AURA

My Talk

Why Cybersecurity for Open Science?

How to Implement Appropriate Cybersecurity for Open Science?

Myth:

Cybersecurity is about confidentiality hence, open science does not need cybersecurity.

Reality:

Open Science Needs <u>Appropriate</u> Cybersecurity

Appropriate cybersecurity supports organizational mission.

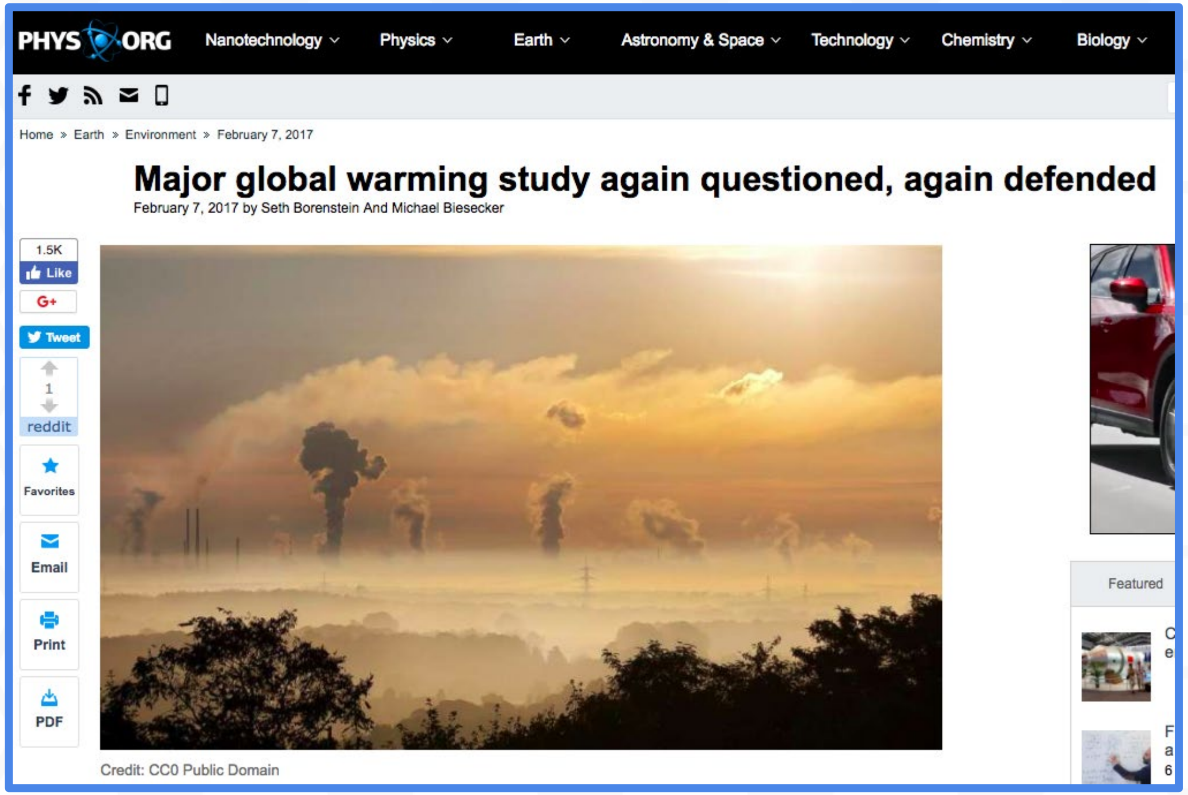
Adobe Stock

For Open Science, Cybersecurity supports:

- Trustworthiness
- Productivity
- Reproducibility

Trustworthy: Data Integrity

For Open Science, integrity of data is often most important aspect of cybersecurity.



Home » Earth » Environment » February 7, 2017

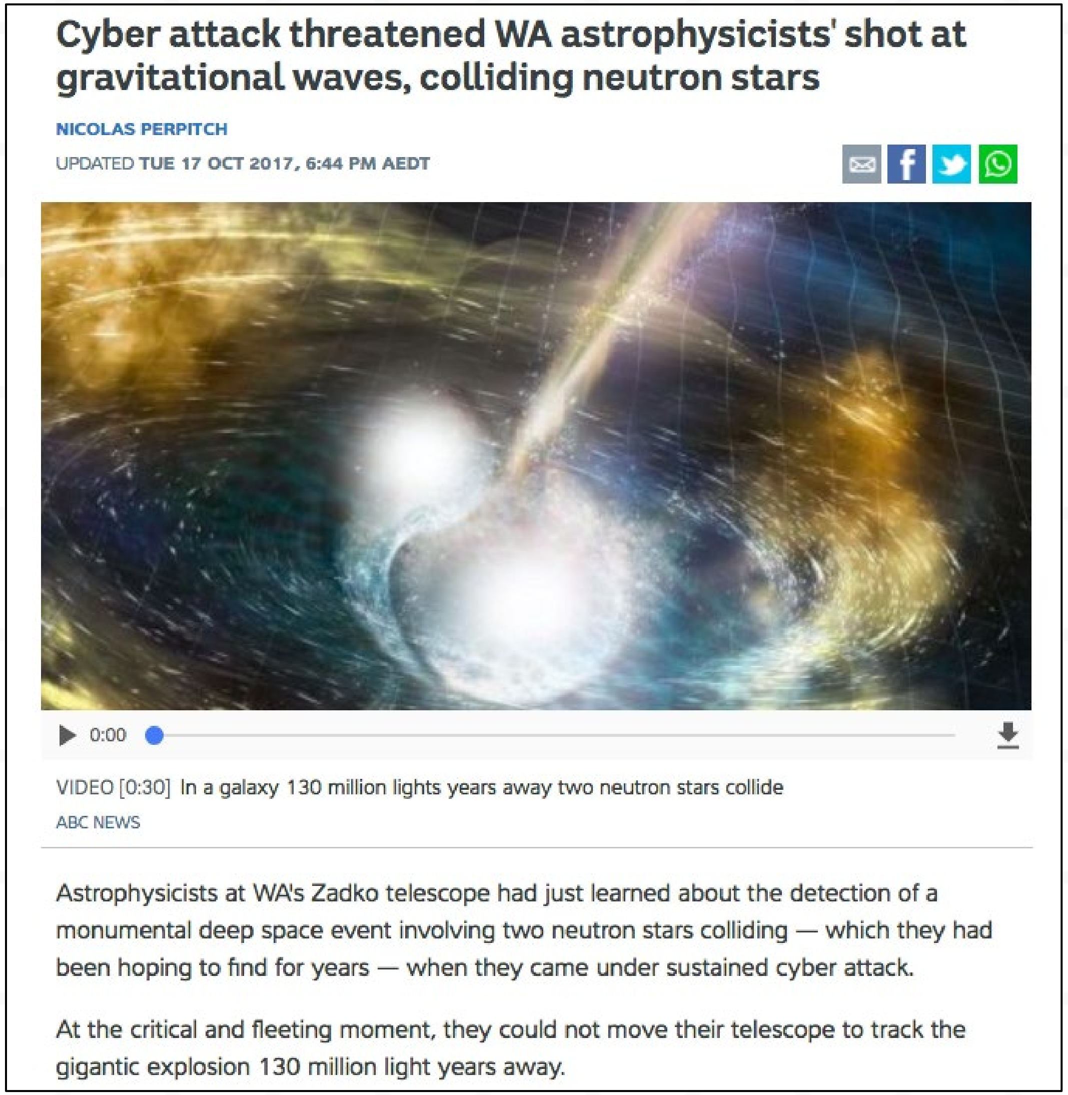
Major global warming study again questioned, again defended

February 7, 2017 by Seth Borenstein And Michael Biesecker

Credit: CC0 Public Domain

https://www.cbsnews.com/news/global-warming-climate-change-study-again-questioned-again-defended/

Productivity:
Threat of Unavailable Instruments



Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

NICOLAS PERPITCH

UPDATED TUE 17 OCT 2017, 6:44 PM AEDT

VIDEO [0:30] In a galaxy 130 million lights years away two neutron stars collide

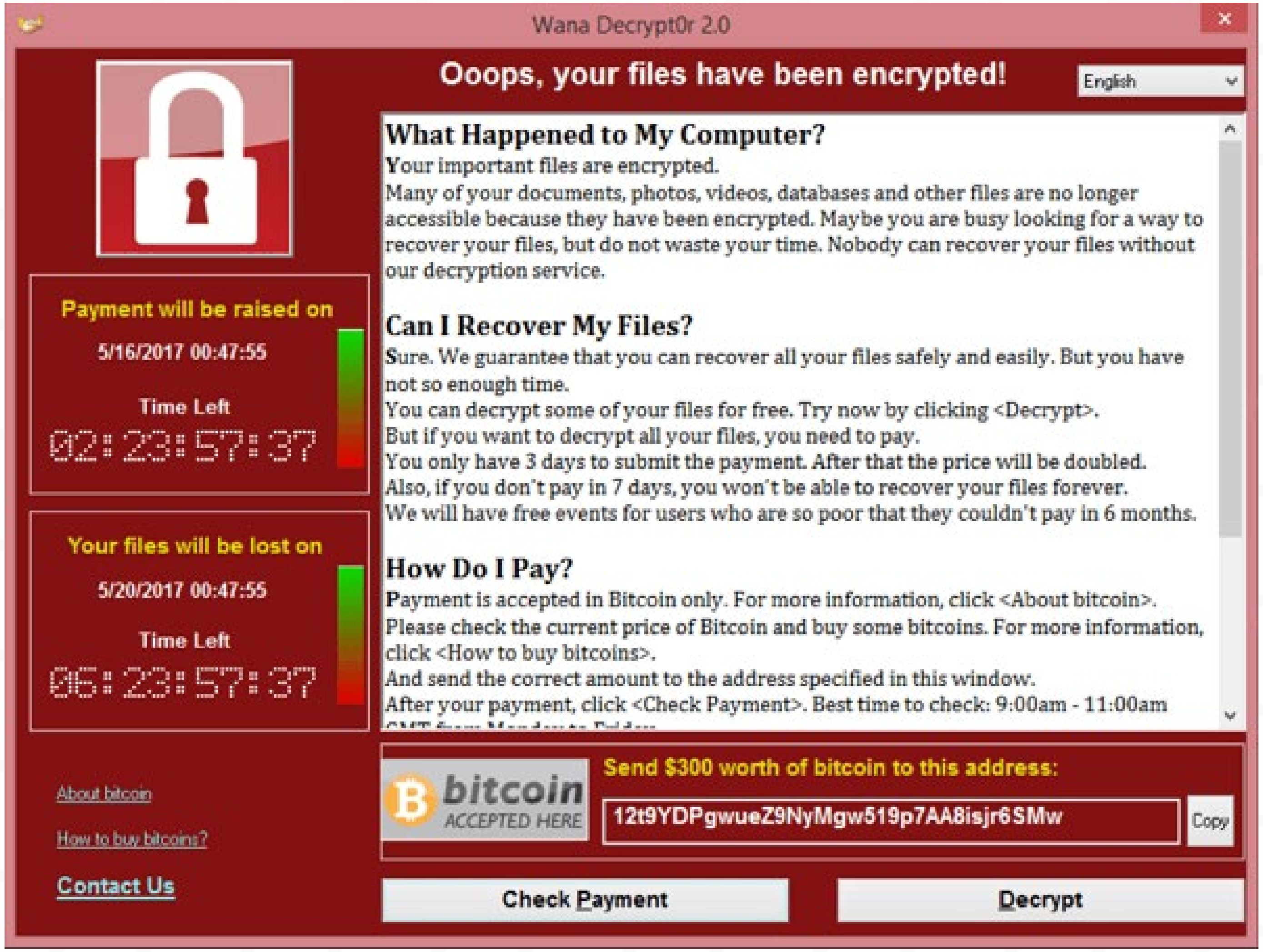
ABC NEWS

Astrophysicists at WA's Zadko telescope had just learned about the detection of a monumental deep space event involving two neutron stars colliding — which they had been hoping to find for years — when they came under sustained cyber attack.

At the critical and fleeting moment, they could not move their telescope to track the gigantic explosion 130 million light years away.

http://mobile.abc.net.au/news/2017-10-17/cyber-attack-almost-costs-team-look-at-colliding-neutron-stars/9055816?pfmredir=sm

Your Data Is Valuable to Criminals!



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

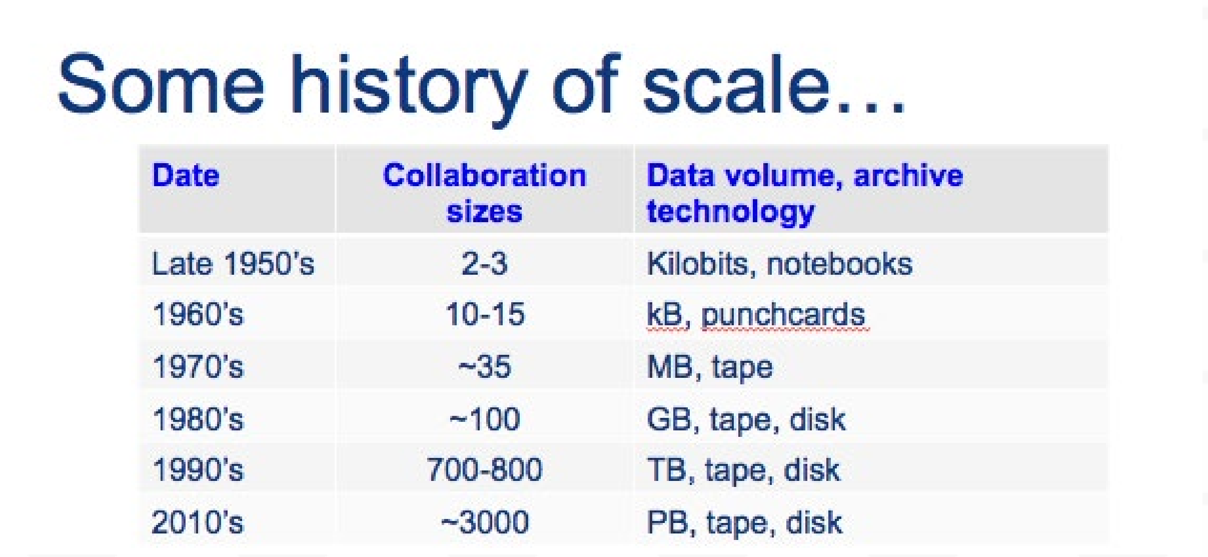
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Productivity: Rapid, Collaborative Projects

Research projects tend to be short-lived (3-5 years). They need to progress quickly.

It’s common for research collaborations to span universities and even countries.

Researchers want to define their teams, change those definitions and share access – all unrelated to institutional directories or human resources databases.



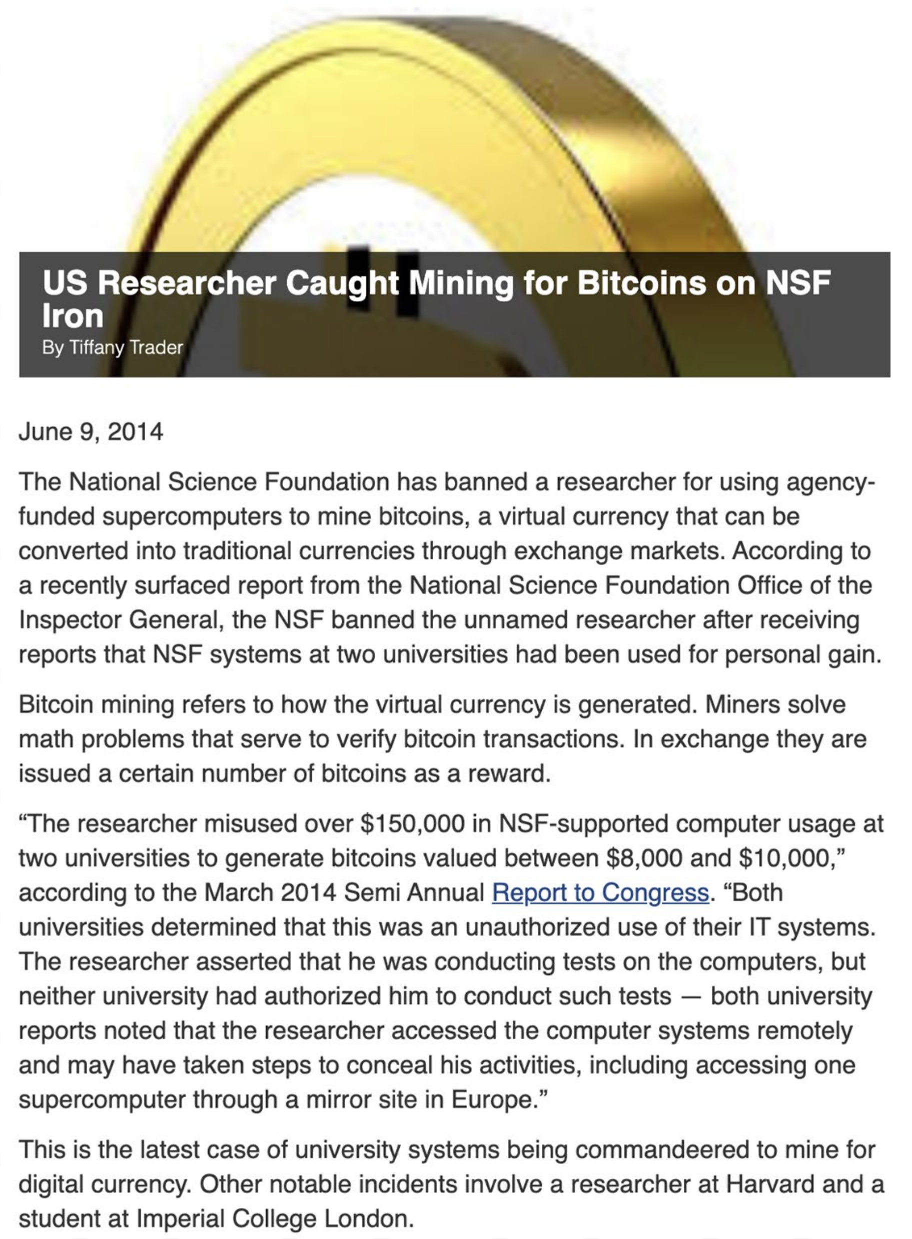
Some history of scale…

Date	Collaboration sizes	Data volume, archive technology
Late 1950’s	2-3	Kilobits, notebooks
1960’s	10-15	kB, punchcards
1970’s	~35	MB, tape
1980’s	~100	GB, tape, disk
1990’s	700-800	TB, tape, disk
2010’s	~3000	PB, tape, disk

Credit: Ian Bird

Reproducibility

Can we reproduce what we did on computers we didn't fully control?



US Researcher Caught Mining for Bitcoins on NSF Iron

By Tiffany Trader

June 9, 2014

The National Science Foundation has banned a researcher for using agency-funded supercomputers to mine bitcoins, a virtual currency that can be converted into traditional currencies through exchange markets. According to a recently surfaced report from the National Science Foundation Office of the Inspector General, the NSF banned the unnamed researcher after receiving reports that NSF systems at two universities had been used for personal gain.

Bitcoin mining refers to how the virtual currency is generated. Miners solve math problems that serve to verify bitcoin transactions. In exchange they are issued a certain number of bitcoins as a reward.

"The researcher misused over $150,000 in NSF-supported computer usage at two universities to generate bitcoins valued between $8,000 and $10,000," according to the March 2014 Semi Annual Report to Congress. "Both universities determined that this was an unauthorized use of their IT systems. The researcher asserted that he was conducting tests on the computers, but neither university had authorized him to conduct such tests — both university reports noted that the researcher accessed the computer systems remotely and may have taken steps to conceal his activities, including accessing one supercomputer through a mirror site in Europe."

This is the latest case of university systems being commandeered to mine for digital currency. Other notable incidents involve a researcher at Harvard and a student at Imperial College London.

https://www.hpcwire.com/2014/06/09/us-researcher-caught-mining-bitcoins-nsf-iron/

Open Science Cybersecurity Resources From Trusted CI

Trusted CI:
The NSF Cybersecurity Center of Excellence

Our mission: to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

INTERNET2®

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

PITTSBURGH SUPERCOMPUTING CENTER

BERKELEY LAB

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/

NSF Funds Research and Education across all Fields of Science and Engineering

Biological Sciences

Engineering

Mathematical & Physical Sciences

Computer & Information Science & Engineering

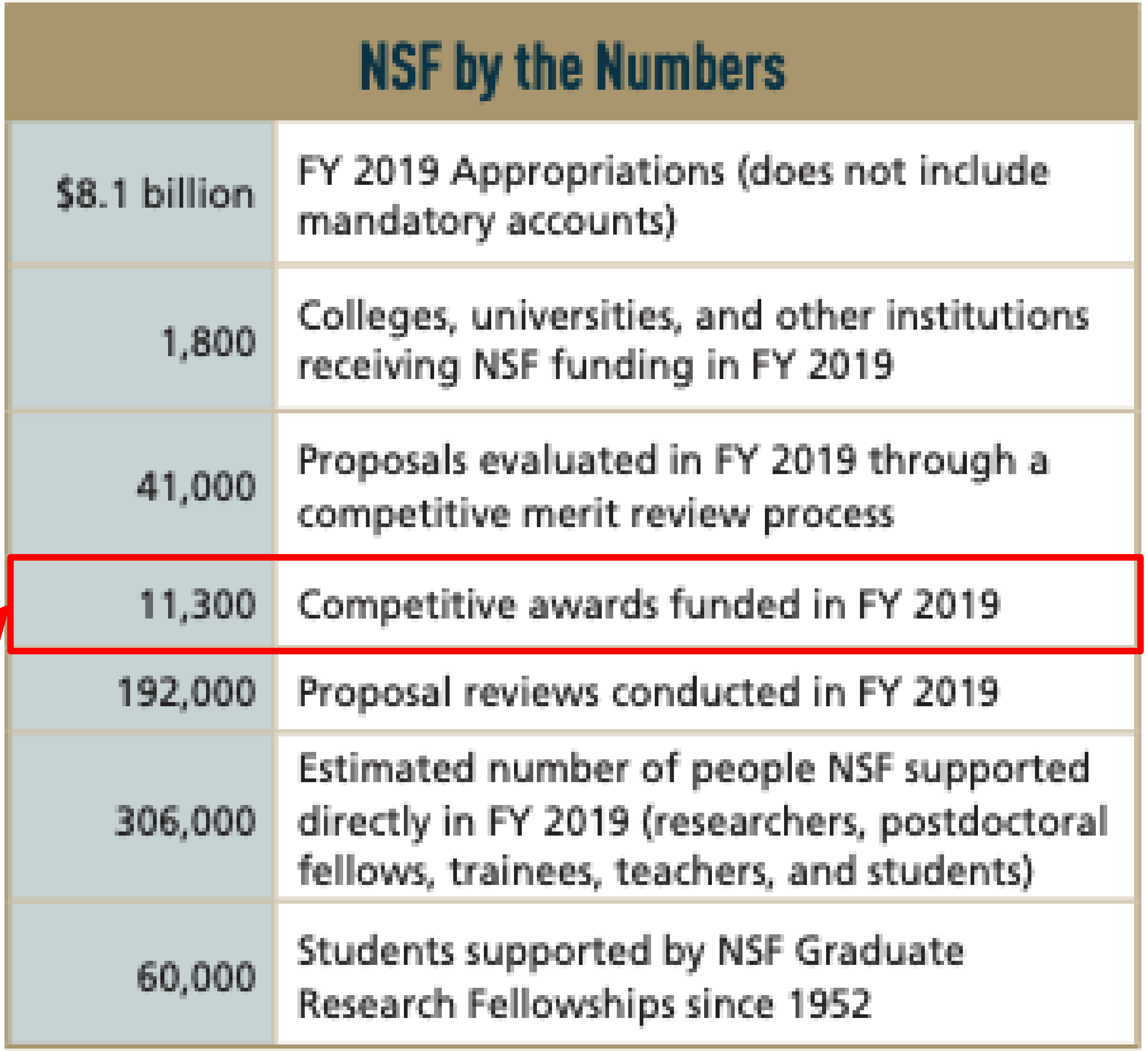
Geosciences (including Polar Programs)

Integrative Activities

Education & Human Resources

Social, Behavioral & Economic Sciences

International Science & Engineering



NSF by the Numbers

$8.1 billion	FY 2019 Appropriations (does not include mandatory accounts)
1,800	Colleges, universities, and other institutions receiving NSF funding in FY 2019
41,000	Proposals evaluated in FY 2019 through a competitive merit review process
11,300	Competitive awards funded in FY 2019
192,000	Proposal reviews conducted in FY 2019
306,000	Estimated number of people NSF supported directly in FY 2019 (researchers, postdoctoral fellows, trainees, teachers, and students)
60,000	Students supported by NSF Graduate Research Fellowships since 1952

Awards > $1m:
644 in FY20
4283 active in 3/2021

https://www.nsf.gov/pubs/2020/nsf20003/nsf20003.pdf
https://www.nsf.gov/news/speeches/cordova/17/fc170523_fy18budget.jsp

Trusted CI

...is a trusted partner, not an auditor, not selling a product.

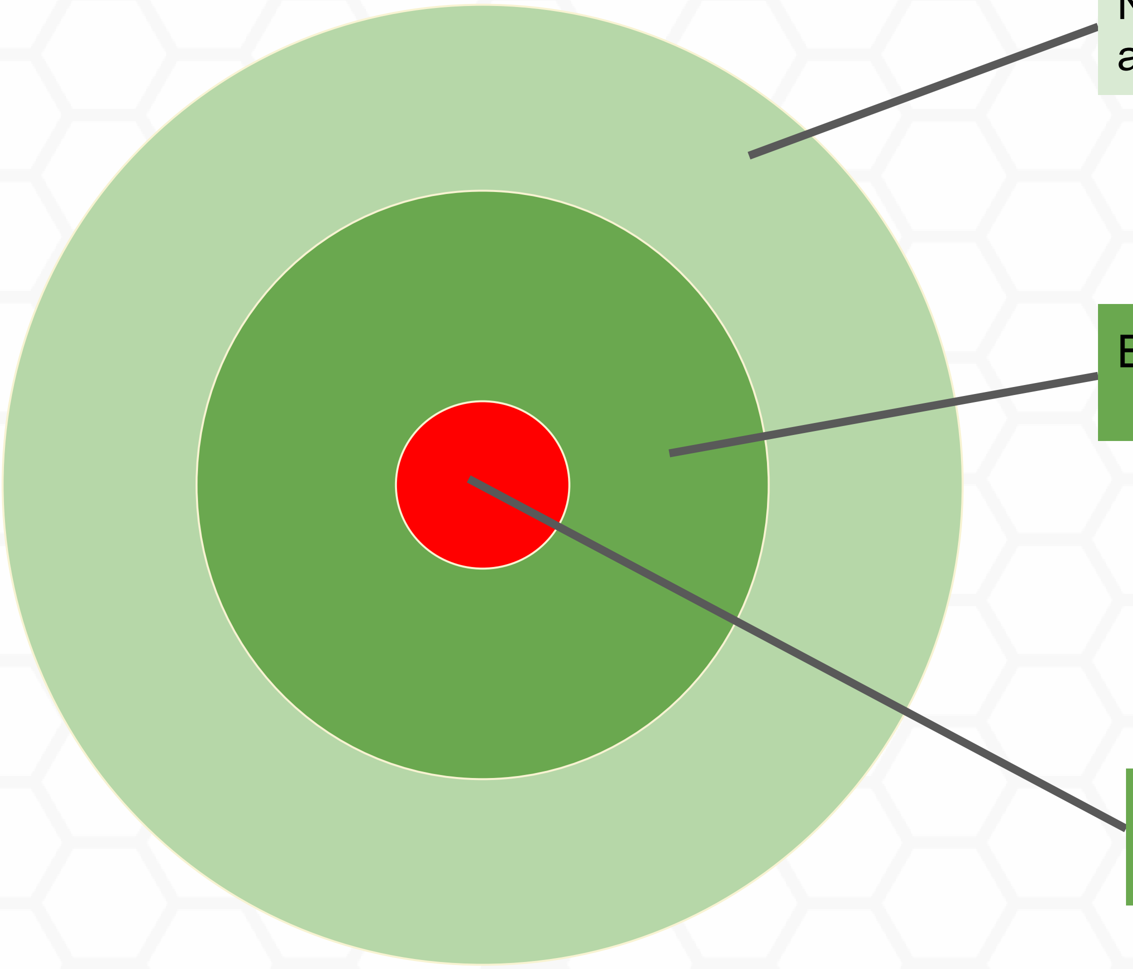
...helps projects tackle their cybersecurity challenges.

...builds community and serves.

...leads to advance state of practice.

...is applied research in community engagement.

Trusted CI: Scopes of Impact



National level: Leadership, community building, webinars, annual cybersecurity Summit, situational awareness.

Broad impact: Training, best practice guides, workshops.

Individual project: Consulting and Engagements.

Trusted CI: Impacts

Updated impact as of July 2020:

Trusted CI has positively impacted over 480 NSF projects since inception in 2012.

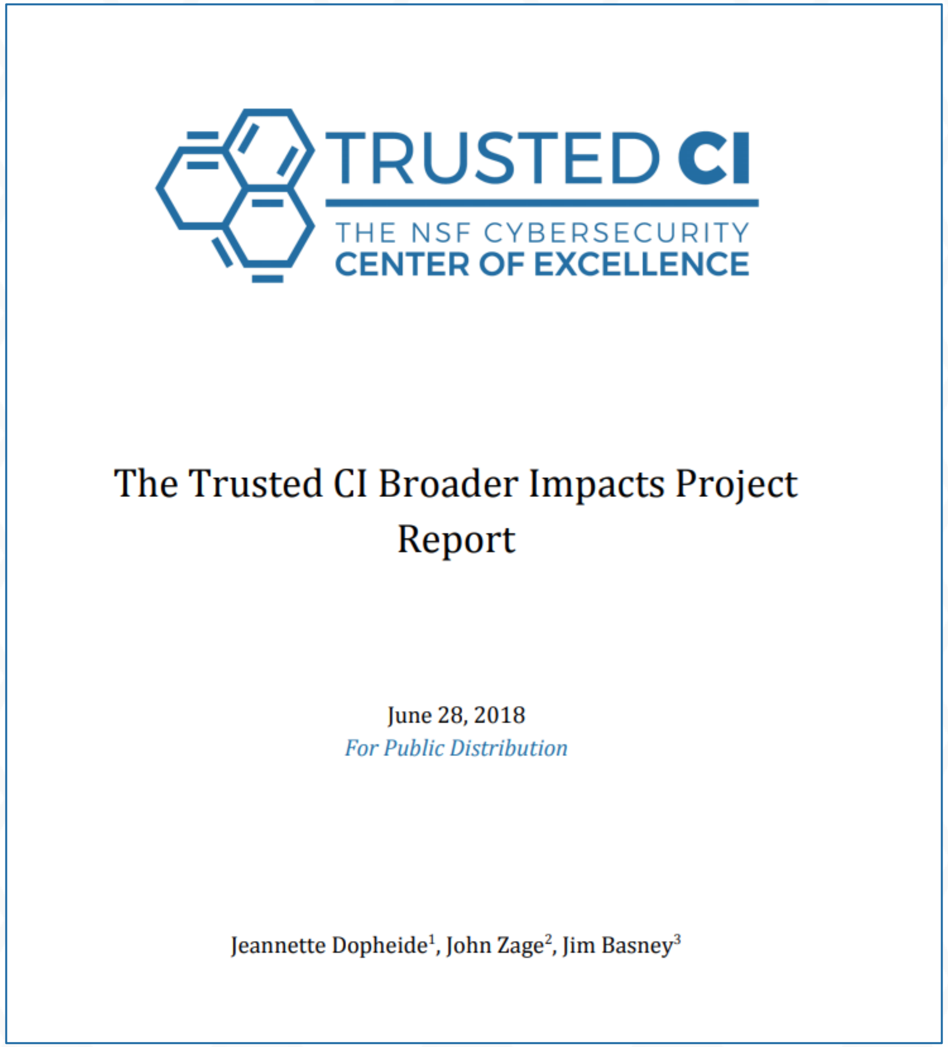
Members of more than 330 NSF projects have attended our NSF Cybersecurity Summit.

Members of more than 140 NSF projects have attended our monthly webinars.

We have provided more than 300 hours of training to the community.

We've had 52 engagements with NSF funded projects, including ten NSF Large Facilities.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Trusted CI Broader Impacts Project Report

June 28, 2018

For Public Distribution

Jeannette Dopheide[1], John Zage[2], Jim Basney[3]

https://hdl.handle.net/2022/22148

Best Practices

Security Best Practices for Academic Cloud Service Providers

- https://trustedci.org/cloud-service-provider-security-best-practices/

Identity Management Best Practices

- https://trustedci.org/iam

Science Gateways

- https://trustedci.org/sgci/

Software Assurance

- https://trustedci.org/software-assurance/

Software Engineering Guide

- https://sweguide.trustedci.org/

Agave Platform
Cornell University Center for Advanced Computing
CYVERSE
Jetstream
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Security Best Practices for Academic Cloud Service Providers

Version 1.0

http://hdl.handle.net/2022/22123

The Trusted CI Framework

4 Pillars, 16 Musts

The Trusted CI Framework helps leaders establish and refine cybersecurity programs that work.

Its straightforward structure focuses on foundational decisions about organizational **mission alignment**, **governance**, **resources**, and **controls**.

This is not yet another long list of technical requirements.

Framework Implementation Guide for Research Cyberinfrastructure Operators

Go to https://www.trustedci.org/framework and hit the **green button**. The guide gives research organizations a community-tailored head start on choosing among good paths and avoiding treacherous ones.

Includes:

- roadmaps for establishing mature cybersecurity programs
- tailored advice on overcoming common challenges
- pointers to resources

Built by Trusted CI's experienced multi-institutional team, and vetted by a Framework Advisory Board representing the diversity of our community.

Getting Started

Check out trustedci.org/framework/core. This briefly explains the **16 Musts**. For each, ask yourself, “Have we addressed this? If not, why not? If so, how’s it working out?”

Hit the green button to grab the guide, and share with your teams.

Staying Connected with Trusted CI

Trusted CI Webinars

4th Monday of month at 11am ET.

https://trustedci.org/webinars

Follow Us

https://trustedci.org

https://blog.trustedci.org

@TrustedCI

Monthly Office Hours

Announced on discuss email list

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Email Lists

Announce and Discuss

https://trustedci.org/trustedci-email-lists

Ask Us Anything

No question too big or too small.

info@trustedci.org

Cyberinfrastructure Vulnerabilities

Latest news on security vulnerabilities tailored for cyberinfrastructure community.

https://trustedci.org/vulnerabilities/

Acknowledgments

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, and 1920430. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

NSF

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI activities are made possible thanks to the contributions of a multi-institutional team:

https://trustedci.org/who-we-are/

Trusted CI License Statement

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Thanks!

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI is supported by the National Science Foundation under Grants 1547272, 1920430, and 1920430. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.