SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

The Cyber Threat Intelligence Sharing Exchange Ecosystem Program

2015 Cybersecurity Innovation Forum

Information Sharing Track

Dr. Eric W. Burger

GEORGETOWN UNIVERSITY

Legal Disclaimers

- Funding Support
- The content of this presentation is my own and does not necessarily reflect the position of the National Science Foundation or the program sponsors

Everybody Wants It

Whatever It Is

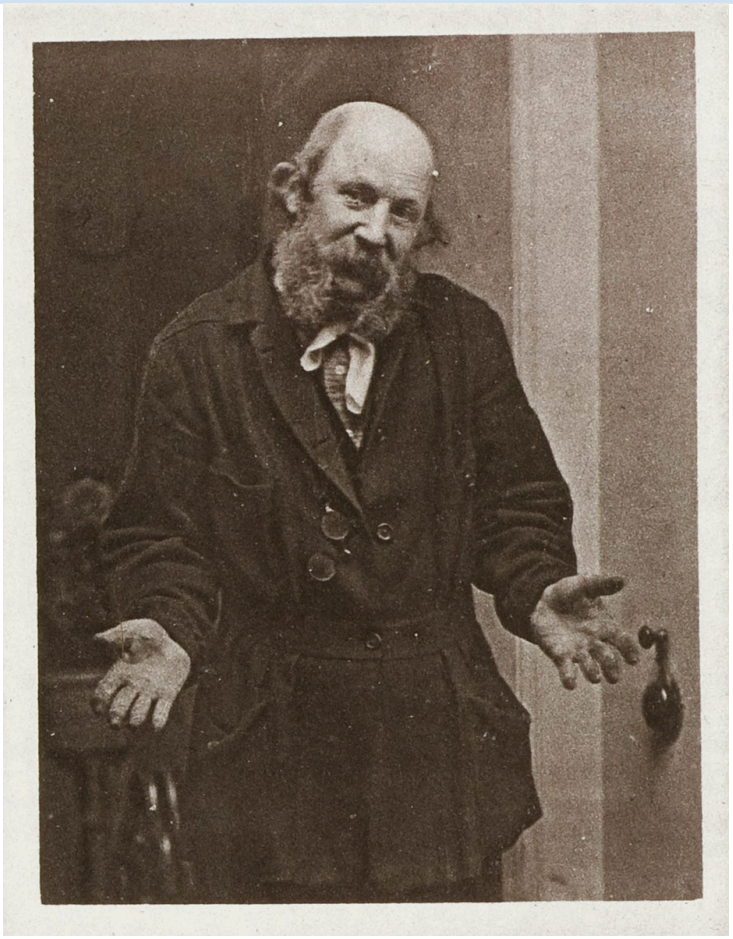
Photo: Shawn Rossi, https://commons.wikimedia.org/wiki/File:Children_at_candy_shop.jpg

Why Share?

Photo: http://kuaibozz.com/wp-content/uploads/2015/04/kids-sharing-food-good-design-2-on-inside-simple-home-design.jpg

SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

Why Is It Still a Pitch?



Credit: Wellcome Library, London. Wellcome Images images@wellcome.ac.uk http://wellcomeimagrs.org
Fold-out photographic plate by Mr Rejlander from Chapter Xl, Disdain, Contempt, Disgust, Guilt, Pride, etc. Helplessness, Patience, Affirmation and Negation. 1 and 2 show expressions of pride, 3 and 4 helplessness in the shrugging of the shoulders. 1872 The expression of the emotions in man and animals / Charles Darwin
Published: 1872

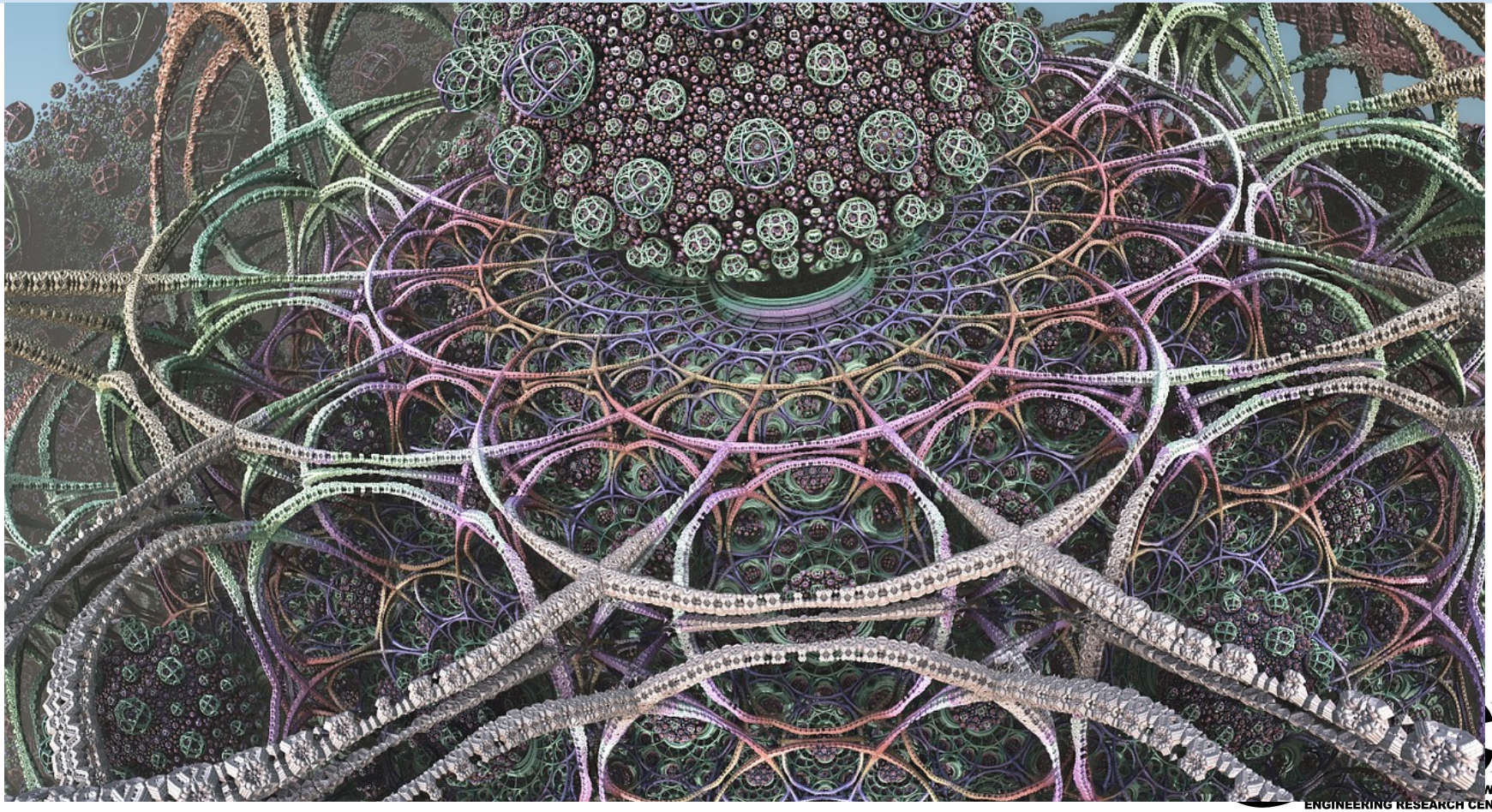
SERC
SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

Barriers to Exchange

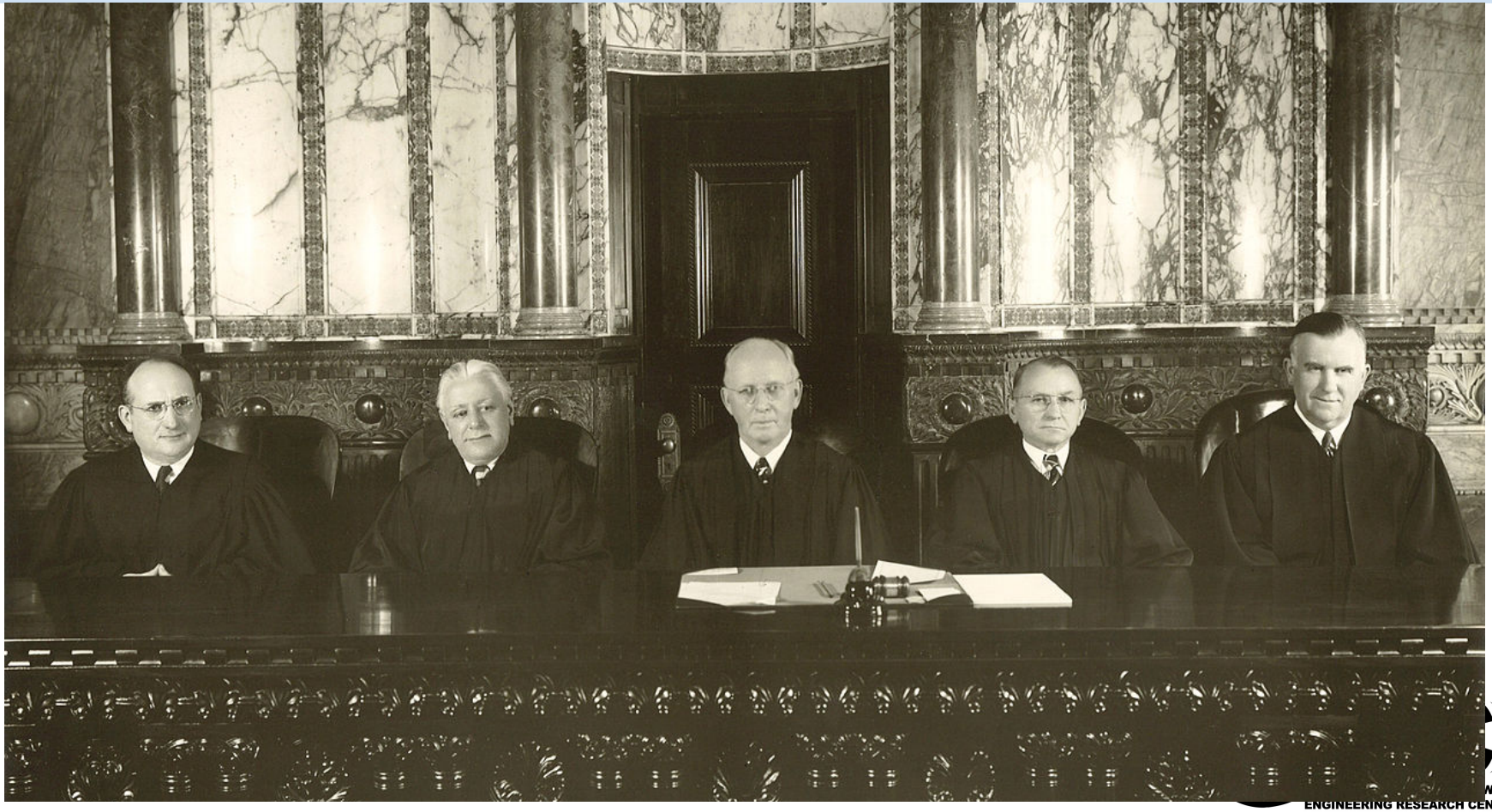
Photo: Daniel Case, https://commons.wikimedia.org/wiki/File:Tourists_outside_Royal_Observatory,_Greenwich.jpg

ENGINEERING RESEARCH CENTER

Technology?



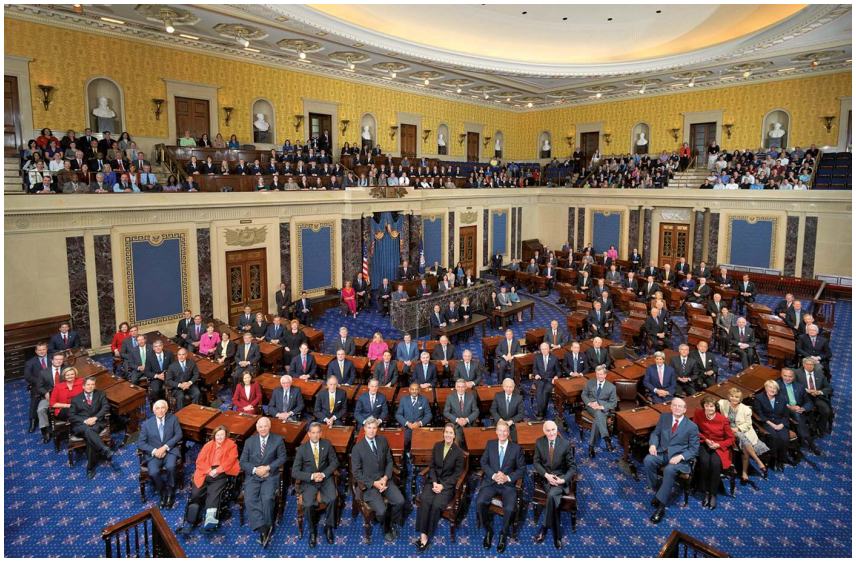
Law?



Economic?

SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

Policy?



SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

Cyber Threat Intelligence Information Exchange Ecosystem Program (CyberISE)

Photo: Raphaël Thiémard, https://www.flickr.com/photos/vivapictures/3403196193/in/photostream/

Who Is the Program For?

- Enterprises and end users
- Entities for operating secure networks
- Information sharing organizations
- Vendors of security products and services

- CyberISE is not an information sharing organization
  - Research, Education, Outreach
  - Not Operations

SERC
SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

CyberISE Accomplishments: Technology Taxonomy

Intelligence	• Action • Query • Target
5W's	• Who, What, When, Where, Why • How
Indicators	• Patterns • Behaviors • Permission on indicator
Session	• Authenticated Sender • Authenticated Receiver • Permissions on entire content
Transport	• Synchronous byte stream • Asynchronous atomic message • Raw byte stream

S2ERC SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

https://s2erc.georgetown.edu/projects/georgetown/results

CyberISE Accomplishments: Economic Analysis

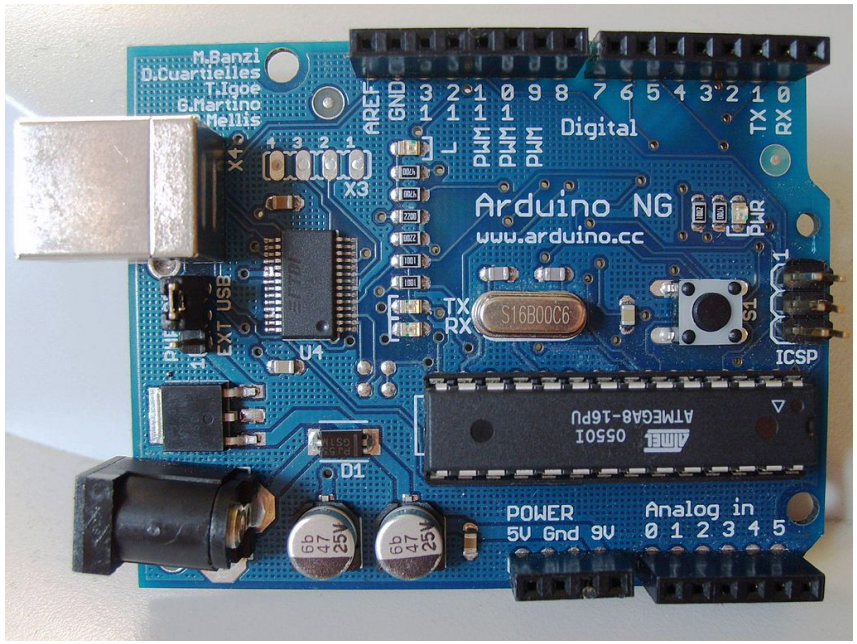
- *Cybersecurity and the Financial Sector*
- *An Analysis of US Government Proposed Cyber Incentives*
- *A Review of Return on Investment for Cybersecurity*

https://s2erc.georgetown.edu/projects/georgetown/results

CyberISE: People-to-People Interaction

SERC
SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

CyberISE Work Today



Technology

- Thesaurus Project
- Standards Development
- Secrecy Preserving Signatures Project

SERC
SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

GEORGETOWN UNIVERSITY

CyberISE Work Today

Policy

- Sensible legislation
- Relative importance G2B vs. B2B vs. G2G
- Help, not hurt, sharing, with privacy / without totalitarian tooling

https://commons.wikimedia.org/wiki/File:USCapitolbackside.JPG

SERC
SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

CyberISE Work Today

Law: International B2B Sharing Analysis

- Catalog & analyze conflicting laws & case laws touching information sharing
- Informs technology
- Focus on OECD First

SERC
SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

CyberISE Work Today

https://commons.wikimedia.org/wiki/Telescope#/media/File:Astronomer.svg

Reality on the Street

- Survey state of information sharing

SERC
SECURITY AND SOFTWARE ENGINEERING RESEARCH CENTER

How to Participate

- https://s2erc.georgetown.edu/projects/cyberISE
- Program under auspices of the Security and Software Engineering Research Center

- https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
- Where STIX, TAXII, CyBOX, etc. now live

Why Participate?

Photo: Valarie Zinger, https://www.flickr.com/photos/23389883@N04/3878472364/

GEORGETOWN UNIVERSITY