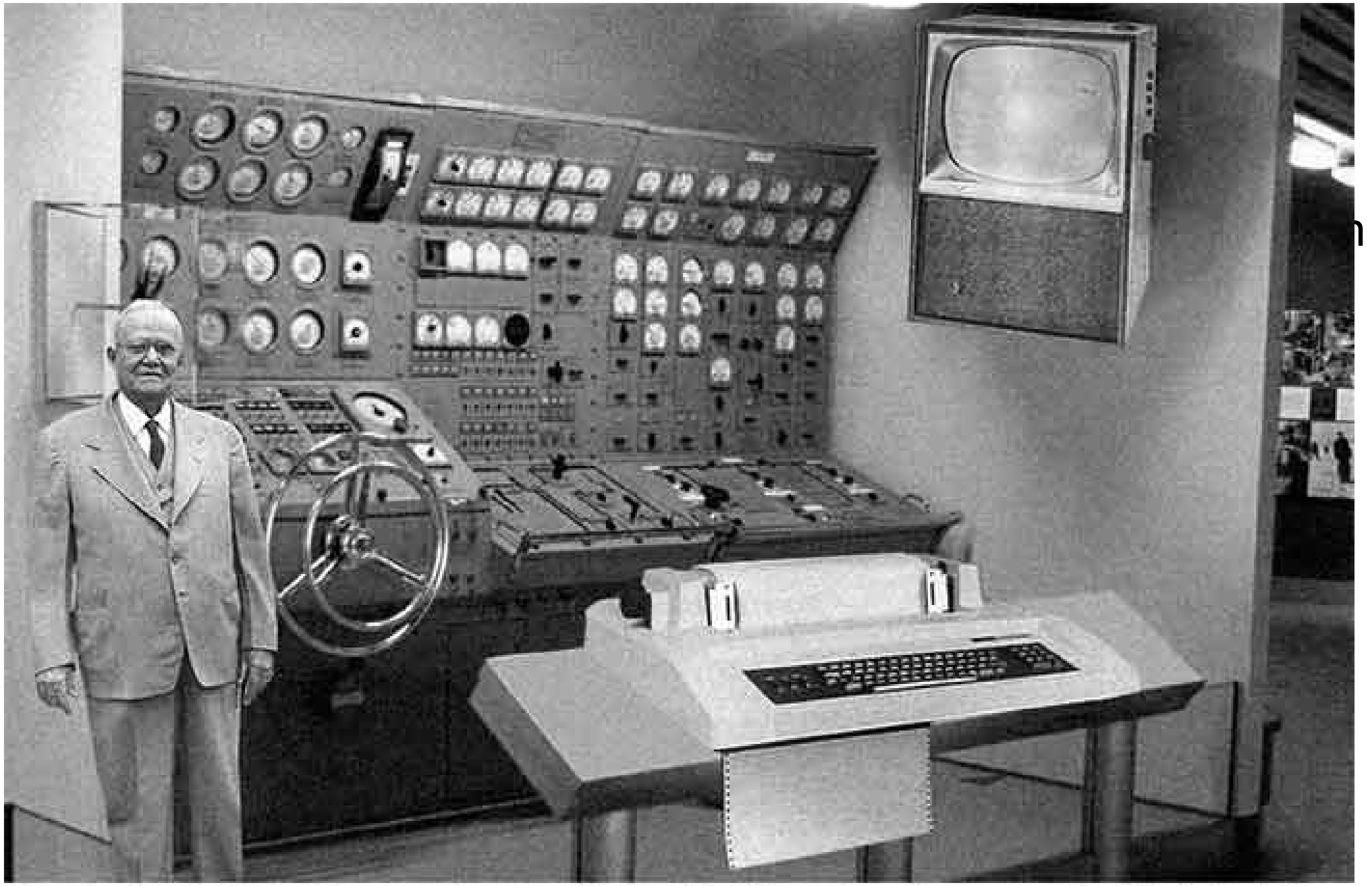
Policy for Cybersecurity in Critical Infrastructure: A Primer

Chris Bronk, Ph.D.
College of Technology
CISRE

The Home Computer!



here.

Scientists from the RAND Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 50 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use and only

Ukraine – 2015

A Brief History of Critical Infrastructure Hacks

2010 – Stuxnet (Iran nuclear program)

2011 – DDoS against US banks (attributed to Iran)

2013 – Rye Brook, NY Dam Attack (attributed to Iran)

2015 – SWIFT Banking system attacks (attributed to N. Korea)

2017 – WannaCry (UK NHS and others)

2017 – Petya/NotPetya (multiple targets: Maersk, DLA Piper, DHL)

2018 – Schneider/Triconex (Saudi petrochem target)

But What’s Critical Infrastructure Anyway?

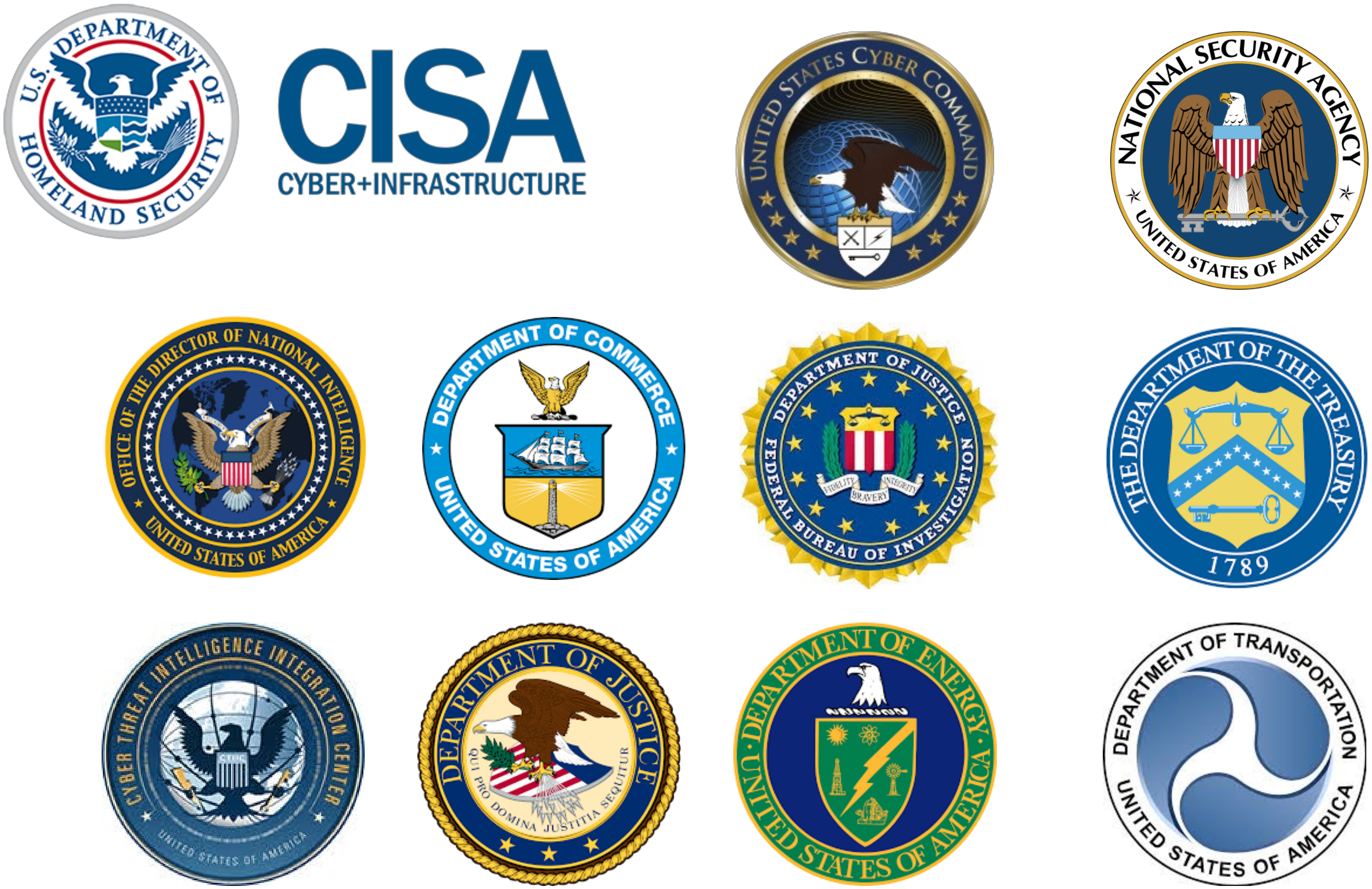
“The Nation's critical infrastructure provides the essential services that underpin American society.”

Presidential Policy Directive 21 (2013)

Sixteen Sectors identified by the Dept. of Homeland Security:

- Chemical
- Communications
- Dams
- Emergency Services
- Financial Services
- Government Facilities
- Information Technology
- Transportation Systems
- Commercial Facilities
- Critical Manufacturing
- Defense Industrial Base
- Energy
- Food & Agriculture
- Healthcare and Public Health
- Nuclear Reactors, Materials & Waste
- Water & Wastewater Systems

There’s a fix for all this, right?



Good thing the government runs the infrastructure…

Roughly 80-85 percent of what is considered critical infrastructure is not owned or operated by the federal government. So what are the priorities?

- Information sharing: indicators found by one organization should be shared among all those concerned.

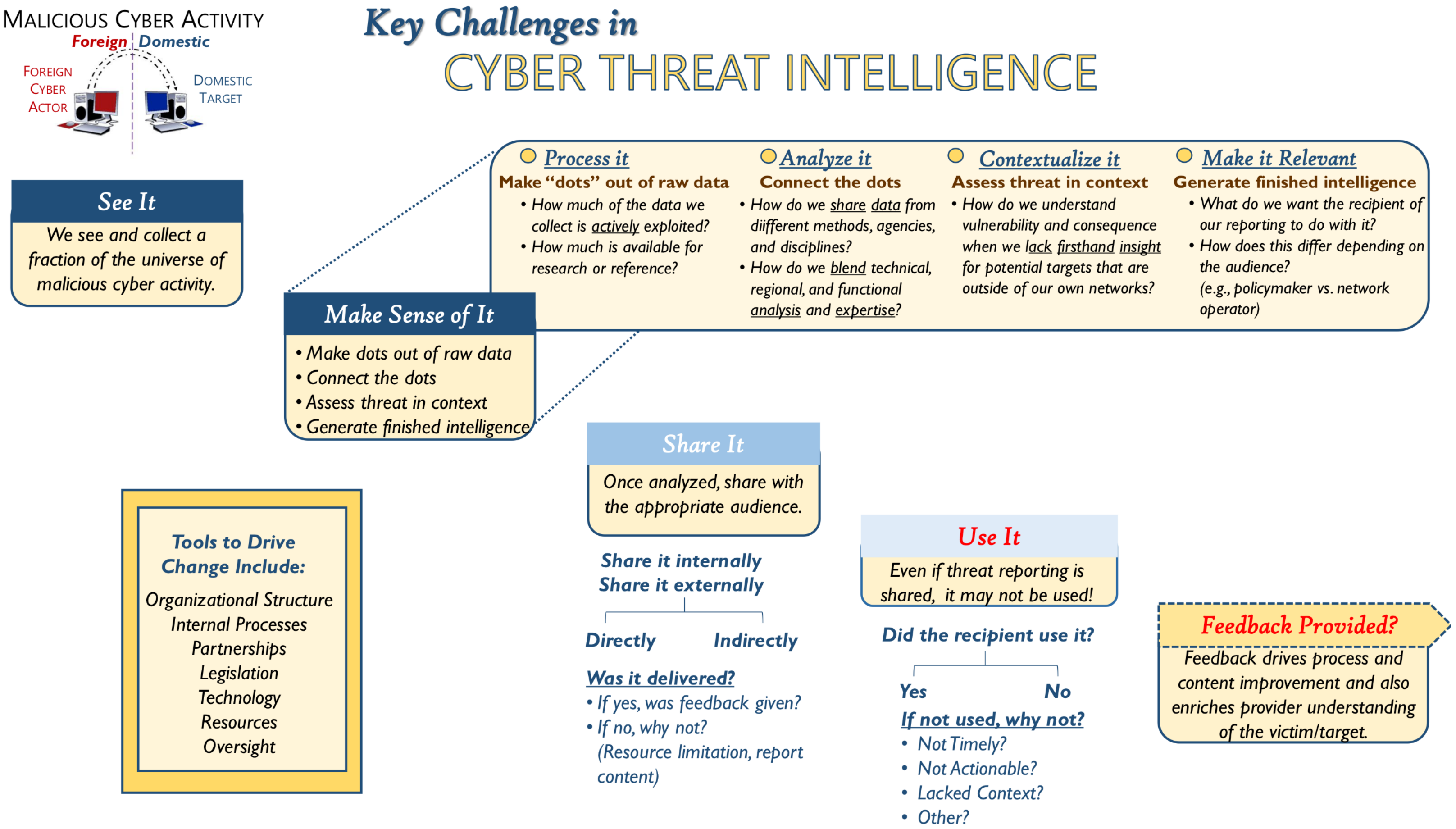
- Facilitating vulnerability assessments: establishing what issues are present for each provider of critical infrastructure.

- Deploying tools and resources: providing public resources to aid firms in mitigating their cybersecurity issues.

- Providing training: offer best possible educational and hands-on experience to security personnel.

- Fostering sector partnerships: aid the ISAC/ISAO functions in industry sectors.

Side Note: Sharing Intelligence Isn't Easy



MALICIOUS CYBER ACTIVITY

Foreign | Domestic

FOREIGN CYBER ACTOR

DOMESTIC TARGET

Key Challenges in CYBER THREAT INTELLIGENCE

See It

We see and collect a fraction of the universe of malicious cyber activity.

Make Sense of It

- Make dots out of raw data
- Connect the dots
- Assess threat in context
- Generate finished intelligence

○ Process it

Make "dots" out of raw data

- How much of the data we collect is actively exploited?
- How much is available for research or reference?

○ Analyze it

Connect the dots

- How do we share data from diifferent methods, agencies, and disciplines?
- How do we blend technical, regional, and functional analysis and expertise?

○ Contextualize it

Assess threat in context

- How do we understand vulnerability and consequence when we lack firsthand insight for potential targets that are outside of our own networks?

○ Make it Relevant

Generate finished intelligence

- What do we want the recipient of our reporting to do with it?
- How does this differ depending on the audience? (e.g., policymaker vs. network operator)

Share It

Once analyzed, share with the appropriate audience.

Share it internally
Share it externally

Directly **Indirectly**

Was it delivered?

- If yes, was feedback given?
- If no, why not? (Resource limitation, report content)

Use It

Even if threat reporting is shared, it may not be used!

Did the recipient use it?

Yes **No**

If not used, why not?

- Not Timely?
- Not Actionable?
- Lacked Context?
- Other?

Feedback Provided?

Feedback drives process and content improvement and also enriches provider understanding of the victim/target.

Tools to Drive Change Include:

Organizational Structure
Internal Processes
Partnerships
Legislation
Technology
Resources
Oversight

Source: Cyber Threat Intelligence Integration Center

Houston: Critical Infrastructure Central