RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: AIR-W04

TAKING THE PULSE ON CYBER INTELLIGENCE

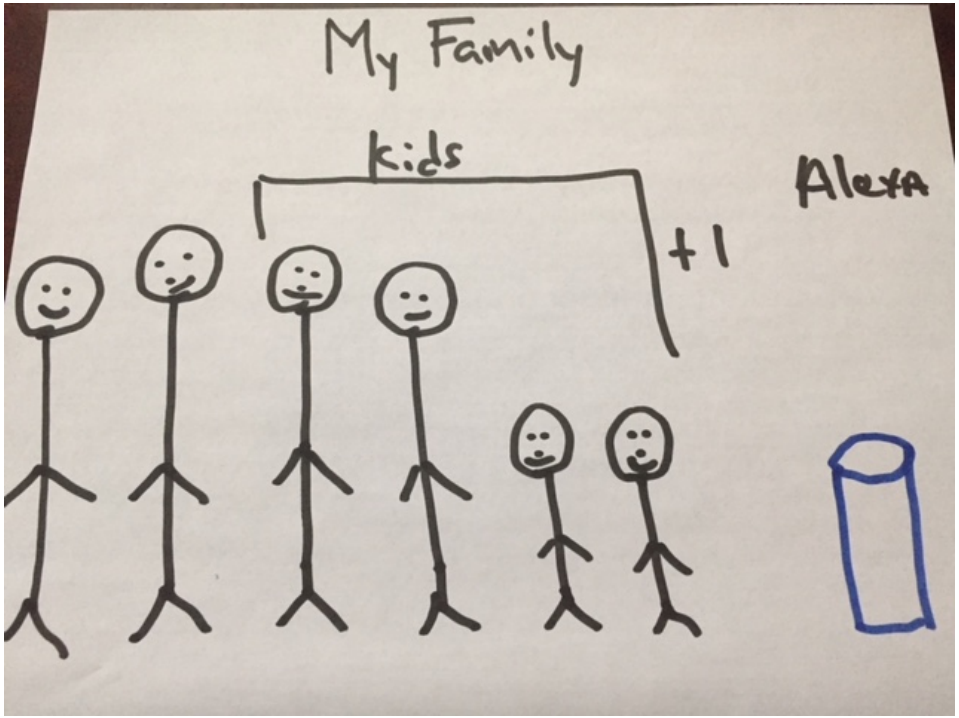
Jared Ettinger

Cyber Intelligence Researcher
Carnegie Mellon University, Software Engineering Institute, Emerging Technology Center

Legal

This material is based upon work funded and supported by the Independent Agency under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

My Family

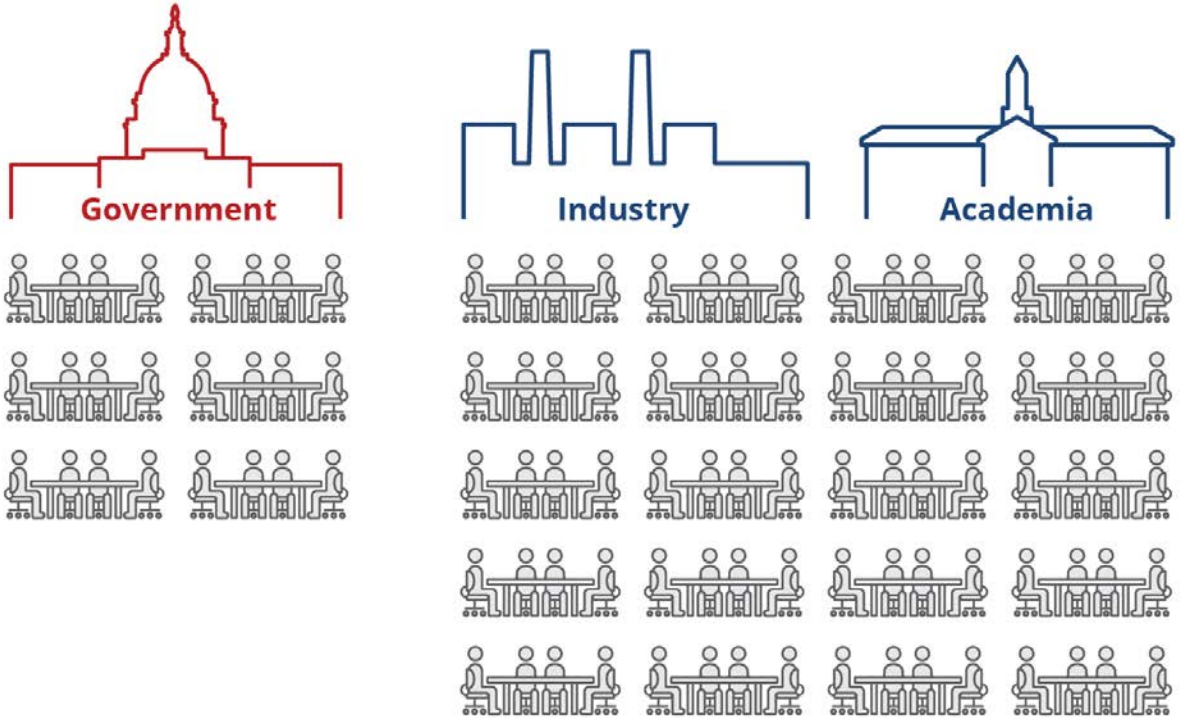


What is cyber intelligence?

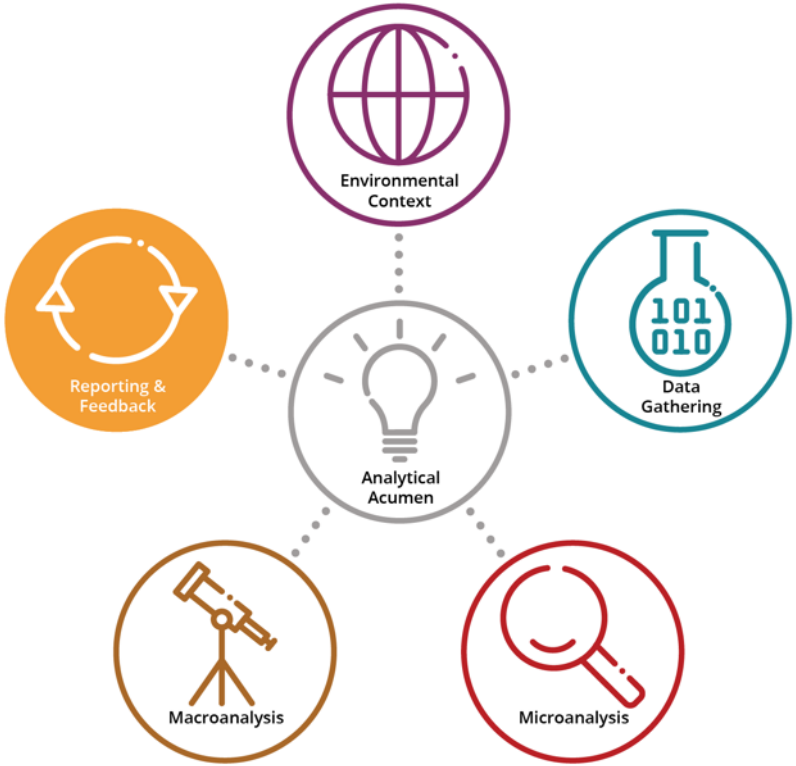
The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making.

Carnegie Mellon University
Software Engineering Institute
2013

Cyber Intelligence Tradecraft Project



Cyber Intelligence Analytical Framework



2013 Findings: What's going well?

- Aligning functional and strategic cyber intelligence resources
- Global situational awareness
- Knowing your intelligence gaps
- Knowing your enemy

2013 Findings: What needs improvement?

- Applying a strategic lens to cyber intelligence analysis
- Adopting a common cyber lexicon and tradecraft
- Communicating “cyber” to leadership
- Difficulty capturing return on investment

Good guys*

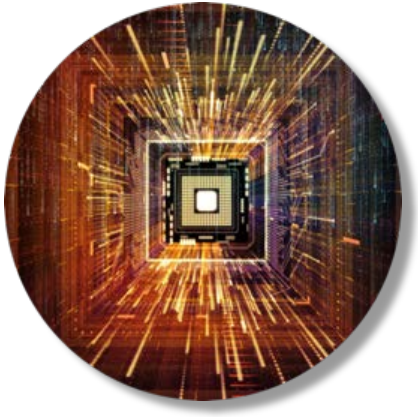
- $6 trillion/year, cyber crime damage
- >$1 trillion/year, cybersecurity spending

Bad guys*

- $200, remote access trojan
- $50, password stealer
- $200, sophisticated license for widespread attacks

source: CSO Online, Recorded Future

Advances in technology



Advanced Computing

Applied Artificial Intelligence and Machine Learning

Human-Machine Interaction

Will Alexa know the answer?

Reverse the asymmetric trend

- Cyber intelligence best practices
- Technological advancements

Goal: Advance organizations' cyber intel capabilities

What

- Highlight best practices and shared challenges
- Identify models, frameworks, and innovative technologies

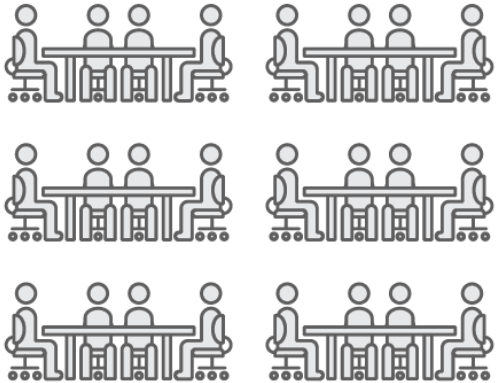
How

- Understand current state of cyber intelligence
- Describe changes in cyber intelligence since 2013
- Explore a future outlook of cyber intelligence
- Explore the utility of public cyber threat frameworks

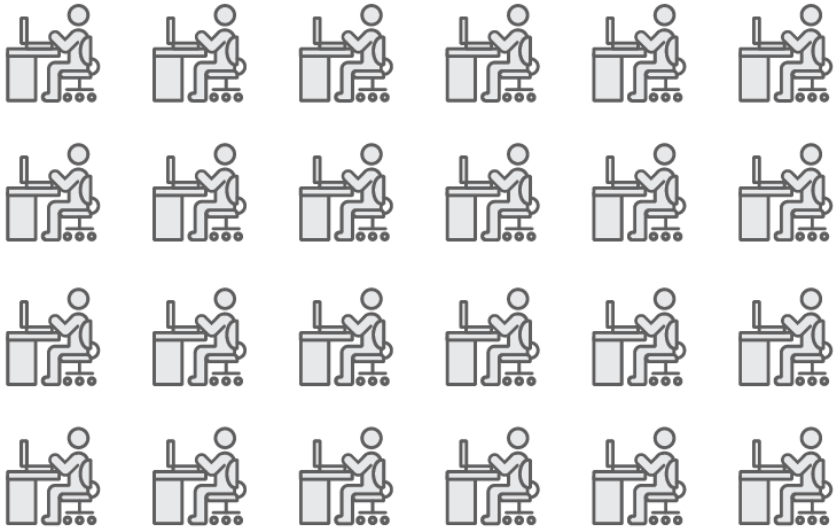
Cyber Intelligence Research Scope

Nov 2017 → **Feb 2019**

On-site Interviews



Online Surveys



Factors Likely Shaping the Cyber Intelligence Landscape Since 2013

- More data
- Data analytics
- Effective communication

Polling Questions - Session ID AIR-W04

1. **Does your organization prioritize cyber threats?**

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3800

2. **Does your leadership provide feedback on your cyber intelligence reports?**

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3801

What we are hearing, so far…

- **Applying a strategic lens to cyber intelligence analysis**
- **Adopting a common cyber lexicon and tradecraft**
- **Communicating “cyber” to leadership**
- **Difficulty capturing return on investment**

What we are hearing, so far…

Remember…

Alexa cannot help you play hide-and-seek at this time.

Joking!!!

Cyber intelligence can help protect your organization

- Get clear terminology
- Know your environment so that you can collect the right data, do relevant analysis, and brief decision makers
- Start to learn about advanced computing, applied AI/ML, and human-machine interaction

Apply what you learned today

1 week

- Read the Cyber Intelligence Tradecraft Project
  https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_40212.pdf
- Figure out what cyber intelligence means to your organization
- Start learning about technologies that will impact cyber intelligence

Apply what you learned today

3 - 6 months

- Get to know your environment

6 months – 1 year

- Start gathering the right data
- Design a workflow to do micro and macro analysis

Questions

jeettinger@sei.cmu.edu

Jared Ettinger
Cyber Intelligence Researcher
Carnegie Mellon University, Software Engineering Institute

Tomorrow: **Birds of a Feather:**
Room: **Marriott | Golden Gate B - Table A | 7:00AM – 7:45AM**

My Interests: Cyber Intelligence, Intelligence, National Security, AI/ML, Cognitive Everything, Brain-Computer Interfaces, Robots, Automation, AR/VR, Geo-politics, Steelers, Penguins