

# Ghosts in the machine:

## The role of human factors in cybersecurity

**Adam Houser**

PhD Student, Formal Human Systems Laboratory  
Junior Cognitive Systems Engineer, Resilient Cognitive Solutions  
Pittsburgh PA

**Kylie Molinaro**

PhD Student, Formal Human Systems Laboratory  
Research Associate, Johns Hopkins Applied Physics Laboratory  
Laurel MD



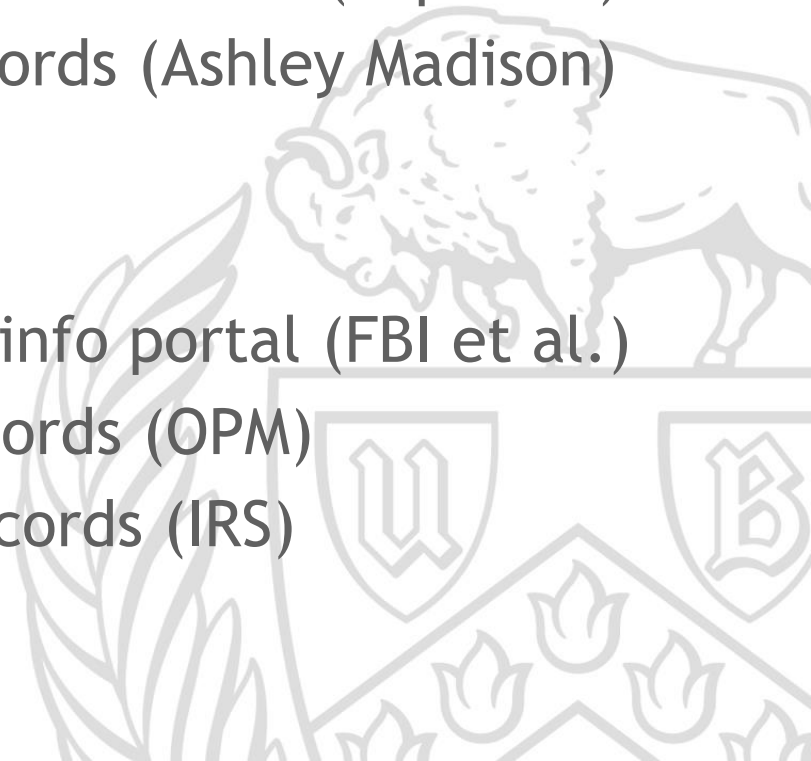
# The 21<sup>st</sup> century battlefield

## 2015 Private Sector

- November: 70m prison phone records (Securus)
- October: 15m T-Mobile customer records (Experian)
- September: 37m customer records (Ashley Madison)

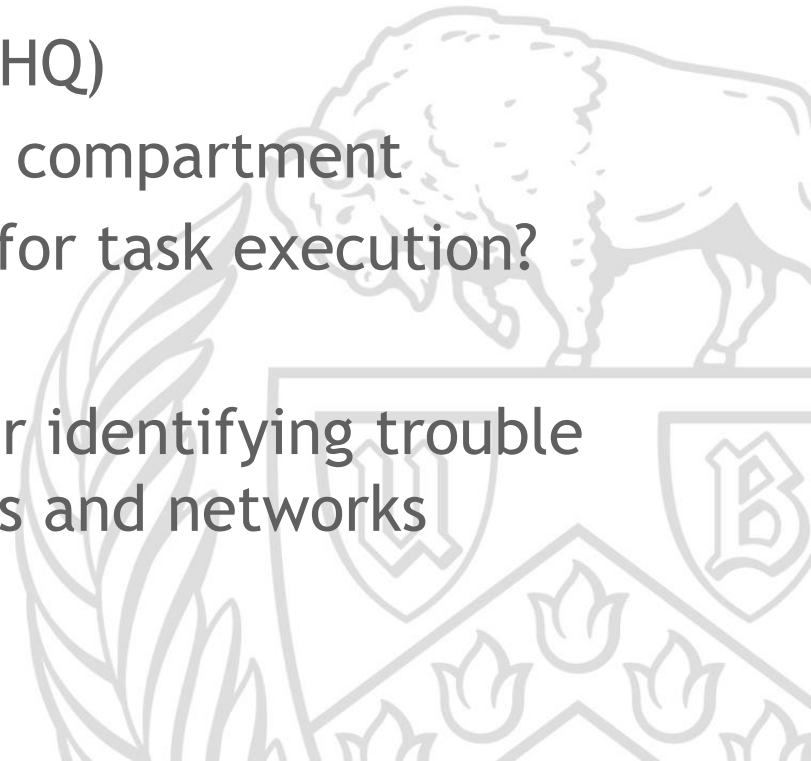
## 2015 Public Sector

- November: US arrest records, info portal (FBI et al.)
- June: 22m highly-sensitive records (OPM)
- May: 100k tax and personal records (IRS)



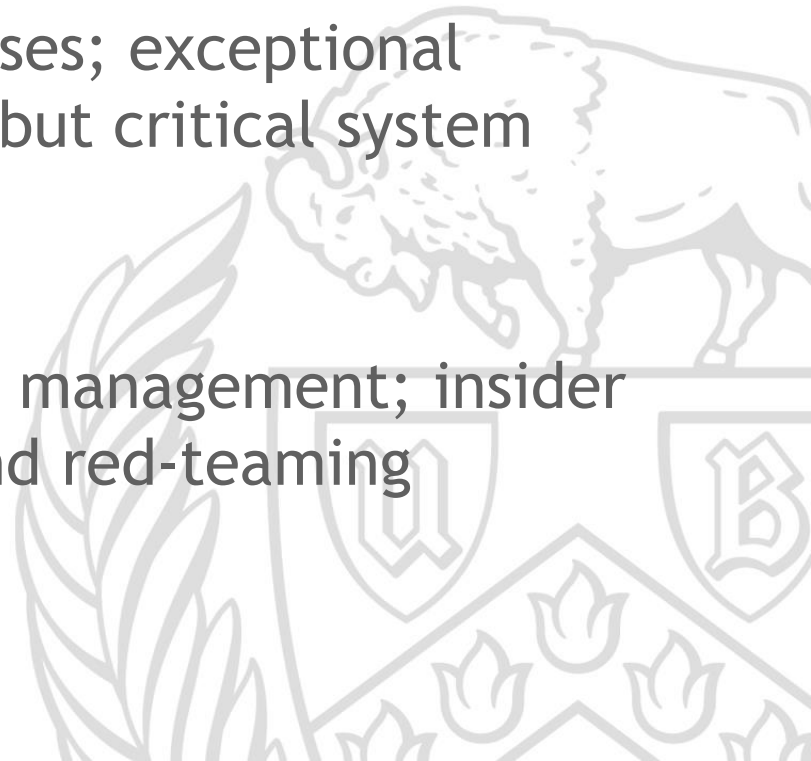
# AA&R in cybersecurity domains

- Authority, autonomy, responsibility
- Multi-user or multi-agency systems:
  - Lots of employees (NSA/GCHQ)
  - Each has clearance level or compartment
  - Who is on the critical path for task execution?
- AA&R is a useful framework for identifying trouble spots in large sensitive systems and networks



# A research agenda

- Formal methods can be used for system modeling and exploration
- Very good at finding corner cases; exceptional combinatoric conditions; rare but critical system behavior
- Potential use cases: personnel management; insider threat analysis; pen-testing and red-teaming



# Understanding the response to phishing emails

- Goal:
  - Use the lens model to understand and predict how people synthesize cues into judgments when assessing a potential phishing email
- Phishing emails & their impact
- The *n*-system lens model
- Known information sources
  - Expertise matters



# Research aims

- Aim 1: Identifying Cues
  - Literature review
  - Interviews
  - Surveys
- Aim 2: Logistic-based Modeling & Analysis
  - Human subjects experiment
  - Logistic Regression
- Aim 3: Identifying General Judgment Strategies
  - Which strategies are most successful?



# Thanks!

Radicati, S. (2014). Email statistics report, 2014-2018. The Radicati Group. *Inc., London.*

McAfee. (2014). Phishing Deceives the Masses. McAfee, Inc.

Microsoft Computing Safety Index. (2014). 2013 Microsoft Computing Safety Index (MCSI) Worldwide Results Summary. *Trustworthy computing.* Microsoft Corporation.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, April). Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 905-914). ACM.

Brunswik, E. (1955). Representative design and probabilistic theory in a functional psychology. *Psychological review*, 62(3), 193.

Cooksey, R. W. (1996). Judgment analysis: Theory, methods, and applications. Academic Press.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006, July). Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security* (pp. 79-90). ACM.

Kim, C. N., & McLeod Jr, R. (1999). Expert, linear models, and nonlinear models of expert decision making in bankruptcy prediction: a lens model analysis. *Journal of Management Information Systems*, 189-206.

