Updating economic methods for strategic reasoning in cybersecurity:

When Advanced Persistent Threat (APT) became Mutual Assured Destruction (MAD)

Dusko Pavlovic
University of Hawaii

C3E
27 October 2021

Outline

Background: Security = Economy

Insight: mutual APT = cyber MAD

Research: New protocols for new strategies

Security = Economy

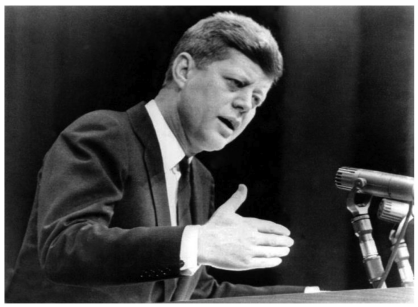
Economy ⊆ Security

- A resource is an economic asset ***only if*** it can be secured.

Security ⊆ Economy

- An economic asset can be secured ***only if*** its value is greater than the cost of securing it.

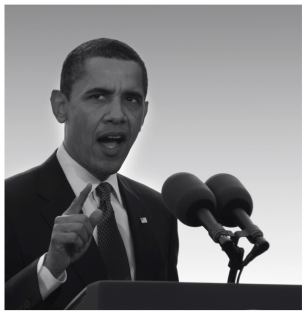
mutual APT = cyber MAD

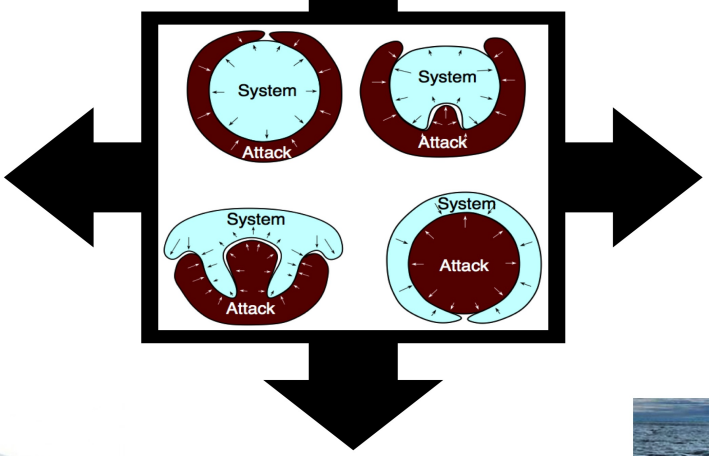


	disarm	arm
disarm	2, 2	3, −1
arm	−1, 3	1, 1

Mutual Assured Destruction (MAD)

mutual APT = cyber MAD





Advanced Persistent Threat (APT)

mutual APT = cyber MAD

Strategic balance

- Attacker
  has penetrated
  Defender's systems.
  - (How deep??)
- Defender
  has penetrated
  Attacker's systems.
  - (How deep??)

Research: New protocols for new strategies

Task 1: Protocol Science for MAD

- model and analyze MAD protocol interactions
- system security through detection and retaliation
- protocols with defense-by-offense options

Research: New protocols for new strategies

Task 2: Game and Decision Theory for APT

- model and analyze APT incentives and utility
- games of incomplete information:
  - *"Gaming Security by Obscurity"*
- case and process studies:
  - *Attack Vectors*, *FlipIt*. . .