Strategic Level Assessment of Cyber Vulnerability – Organizational and Global

Kathleen M. Carley, Ph.D.

kathleen.carley@cs.cmu.edu
www.casos.cs.cmu.edu

Carnegie Mellon

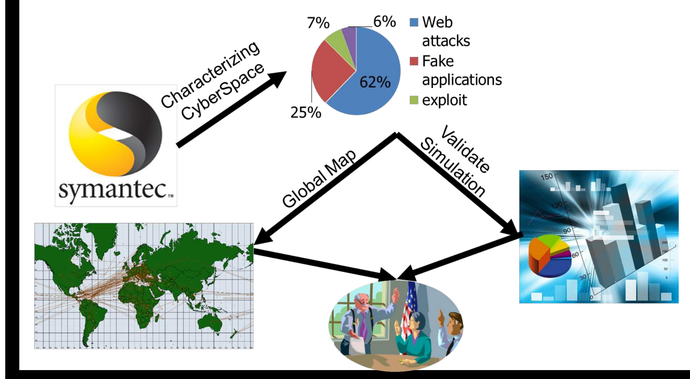
CASOS

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

Workshop on
People, Power, and CyberPolitics
MIT, December 6 and 7, 2014

Problem

- Goal: Strategic Cyber Assessment
- Global - Identify nation-states likely to have or develop offensive Cyber capability
  - Assess motivation based on social influence
  - Assess capability based on research, trade and pharmaceutical industry
- Organizational Identify Resilient Designs



Summary of Results

- Global threat is universal
- Threatening Countries
  - Computers, Poor process, High Corruption
- Web exploits increasingly common
- Organizations at risk
  - Distributed/Networked
- General
  - Any attack increases leaks
  - Most attacks irrelevant

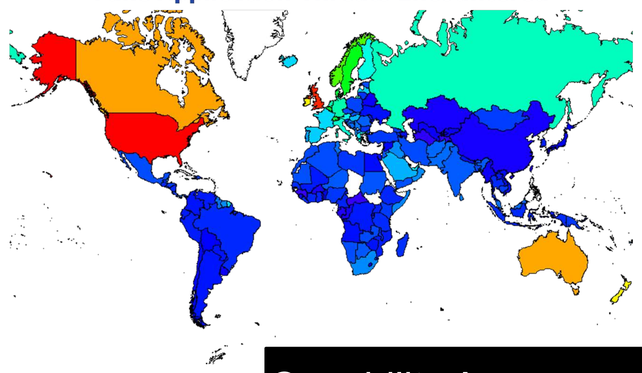
Global Context
Organizational Impact

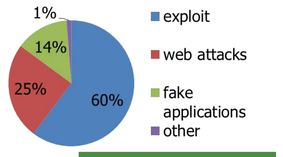
Cyber Attack Facilitator

- Analyze # attacks originating from countries
  - Based on Symantec's WINE data (from ~10 million machines worldwide)
- Findings:
  - Many Eastern European countries among top countries
  - Countries with middle IT usage are those that act as attack facilitators (good infrastructure, bad management

Vulnerability Assessment

Fake Application Threats Encountered

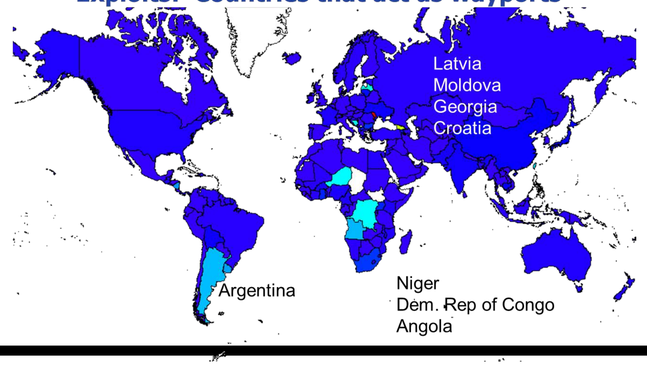




Attacks encountered.
Total ~ 35.9 M

Capability Assessment

Exploits: Countries that act as wayports



Resiliency

Ve: Value at initial equilibrium

Vmin-d: Minimum value reached during disruption

Vr-e: Value when equilibrium is restored

Ti: Time when the organization began tracking this measure of performance.

Te: Time when the organization first reaches stability of the measure of interest.

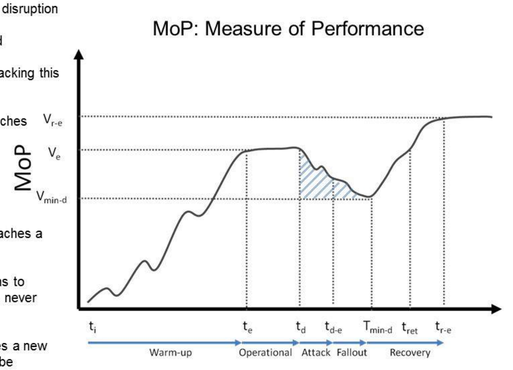
Td: Time when the disruption begins.

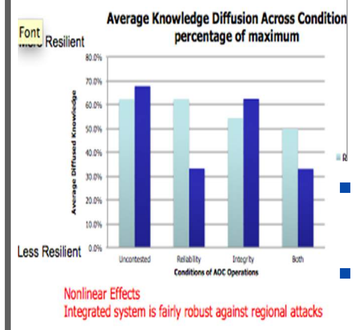
Td-e: Time when the disruption ends.

Tmin-d: The time when performance reaches a minima.

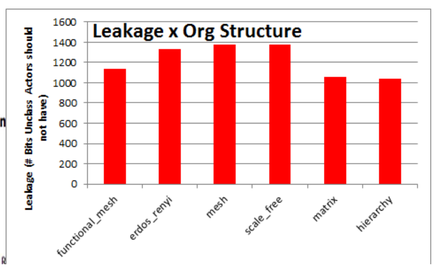
Tret: The time when performance returns to previous performance. The system may never reach this.

Tr-e: Time when the organization reaches a new equillbrium. This new stable value may be different than the previous stable value.





Nonlinear Effects
Integrated system is fairly robust against regional attacks



- Redundancy increases Resiliency
- Hierarchies minimally impacted by integrity attacks
- Leadership relatively insulated from attacks

Acknowledgement

Various portions of this research were funded by the Office of Naval Research, the Air Force Office of Sponsored Research, the Defense Threat Reduction Agency, and the Army Research Office.