Doctrine for Cybersecurity

Fred B. Schneider

Samuel B Eckert Professor of Computer Science,
Chief Scientist, NSF “TRUST” Science and Technology Center

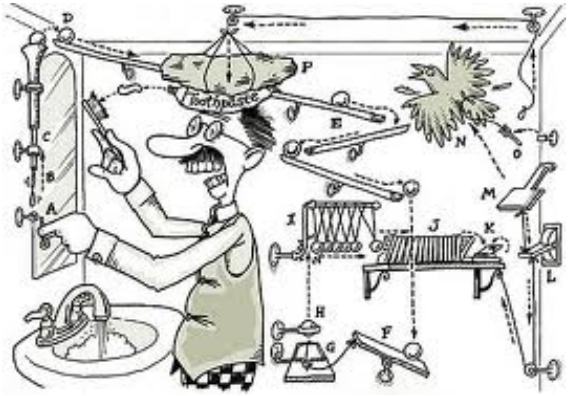
Department of Computer Science
Cornell University
Ithaca, New York 14853
U.S.A.

Joint work with Deirdre Mulligan,
Univ of California, Berkeley

Trustworthy Networked Systems?

A **trustworthy** system
- does what is expected
- does not do the unexpected

despite attacks, failures, ...



Today's networked systems are not trustworthy.

The problem is both policy and technology.
- Existing technical solutions are not being deployed.
- New technical solutions are needed, too.

Problems caused by bad technology don't always have technology solutions.

Security Is Not Free

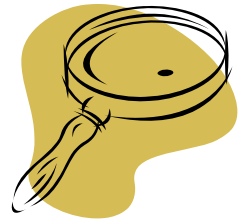
- Development costs
- Function
- Convenience
- Societal values:
  - Privacy and openness
  - Freedom of expression
  - Freedom to innovate

How to resolve trade-offs?

Cybersecurity Doctrines

- **Goals** define
  - kinds and levels of cybersecurity sought
  - acceptable trade-offs and costs.
- **Means** include
  - Technical / education / regulation
    - Incentives: market-based to coercive

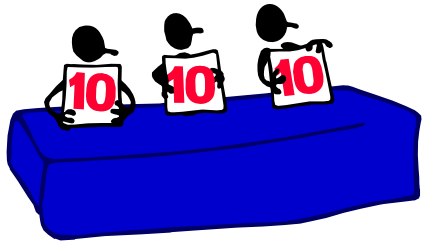
A **lens** for viewing existing policy proposals; an **inspiration** for suggesting new ones.



Early Doctrine:

Doctrine of Prevention

Build systems that don't have vulns.



- Unworkable:
  - Big systems are too complicated to get right.
  - Formal verification infeasible
  - Exhaustive testing infeasible
  - Performance standards would require security metrics.
- Incomplete:
  - Ignores users and operators ("social engineering")
  - Environment not static (attacks, assumptions, uses)
    - Specs must evolve
    - assurance argument must be reconstructed

Early Doctrine:

Doctrine of Risk Management 1

Invest in security to reduce expected losses due to attacks.

- Cost of attack
  - What is value of confidentiality? Integrity?
  - What is the cost of recovery from attack?
  - What about costs to third parties?
- Probability of attack
  - Insufficient data about threats and vulns.

Early Doctrine:

Doctrine of Risk Management 2

- Under-investment is rational.
  - Individuals cannot:
    - reap full benefit from their investments.
    - cannot control vulns.
  - No metrics to predict ROI
  - Insufficient data about threats, vulns, and cost of losses
  - Continuing investments would be needed
    - Threats co-evolve with defenses
    - Replacement systems and upgrades constantly deployed
    - New domains mean new forms of security needed.
  - Actuarial models and insurance unfounded.

Recent Doctrine:

Doctrine of Accountability

Deter attacks through threats of retribution.

- Retrospective and punitive
  - No concern about keeping systems up and running.
- Attribution of action is often infeasible.
  - Cross border enforcement?
  - Non-state actors?
  - Binding of machines to individuals is weak
- Incomplete:
  - Narrow set of policy options for privacy.
  - Presumes attacks are crimes.

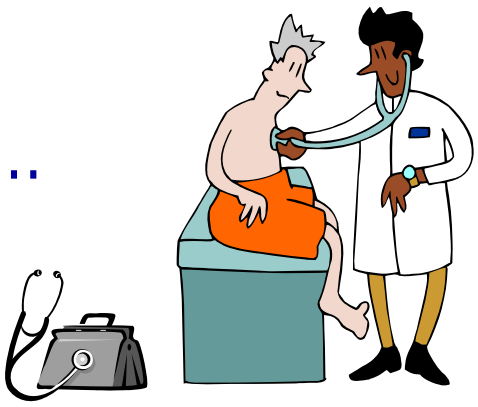
A New Doctrine:

Public Goods

Thesis: Cybersecurity is a **public good**.

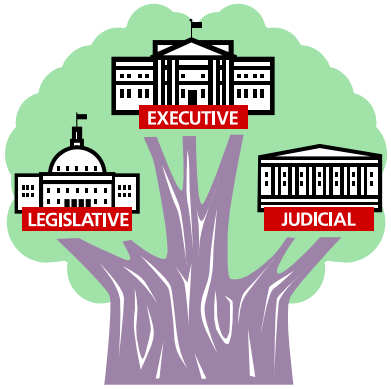
- Non-rivalrous: Consumption of the good by one individual does not reduce availability for consumption by others.
- Non-excludable: No individual can be excluded from having access to the good.

"Public health" is a public good, too...



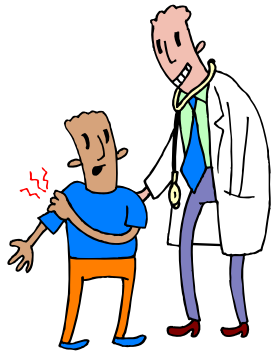
Public Health?

… duties and power of the state to assure health of the population (not individual) and limitations on that power to protect the interests of individuals.



- Herd immunity vs individual vaccination risk
- Stem an epidemic vs individual privacy
- Incentives vs externalities

Doctrine for Public Health



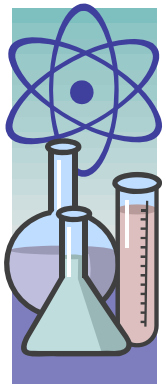
Goals: Prompt production
Manage its absence

Means: Education, prevention, surveillance, containment (quarantine), diversity, mitigation, recovery.

- Eschew: punishment, compensation, restitution

Requires new research and always will.

- Pathogens evolve.
- Expectations and health needs grow.



Public Health → Public Cybersecurity

- Network: people → computers (+ people)
- Positive state: health → cybersecurity
  - Produce: health → produce cybersecurity
  - Manage: disease → manage insecurity (vulns)

Public Health → Public Cybersecurity

- Network: people → computers (+ people)
- Positive state: health → cybersecurity
  - Produce: health → produce cybersecurity
  - Manage: disease → manage insecurity (vulns)

Doctrine(s) of Public Cybersecurity:

- ***Prompt the production of cybersecurity.***
- ***Manage the remaining insecurity.***
- ***Political agreement to balance individual rights and public welfare***

Doctrine of Public Cybersecurity:

Strategy and Tactics: Production

Means to produce increased cybersecurity:

- Formal methods, testing, ...
- Standards in development, analysis, testing, ...
- Developer education, training, and certification.

Incentives:

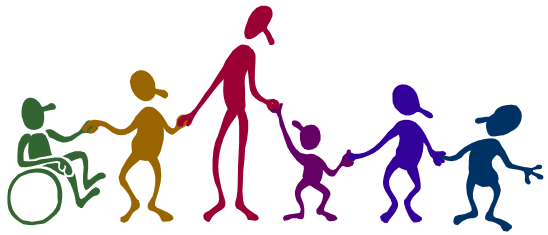
- Liability to producer unless ... (subset of above).

Doctrine of Public Cybersecurity:

Manage Insecurity: Diversity

Require systems to exhibit diversity.

- E.g., Obfuscation / randomization



- Eliminates monocultures
- Probabilistic defense
- Confidentiality / Integrity compromise → Availability compromise

Doctrine of Public Cybersecurity:

Manage Insecurity: Surveillance

- Software self check

- Network traffic-monitoring
  - At significant boundaries
    - Firewalls
    - Networks of firewalls (Einstein x)
  - Coordination among ISPs
    - DoS detection and defense

Doctrine of Public Cybersecurity:

Manage Insecurity: Patching

Why don't people apply patches?

- Under-appreciation of risks
- Unaware of vulnerabilities that are present
- Belief that nobody does it
- Fear destabilizing other software
  - Pre-test standard configurations
  - Include functionality "back-out" installation.
- Time or expertise
- Cost of bandwidth to download patch
- Fear that pirated software will be detected.

Policy challenges to mandate patching:

- Subsidize costs?
- Compensating injured parties
  - VICP (vaccine injury compensation program) analogy

Doctrine of Public Cybersecurity:

Manage Insecurity: Isolation

- Filters require signatures
  - Surveillance as a source of signatures
  - Deep packet inspection vs encryption
  - Fooled by new attacks vs preventing innovation
- Where is boundary?
  - Initiated by a collective (corporate, political, ...)
  - Where is the authority?
- Isolation versus societal values.
  - Press censorship / repress debate

Doctrine of Public Cybersecurity:

Manage Insecurity: Intermediaries

- Require healthy machine for connection.
- Notify subscribers if evidence of compromise.
- ISP's as intermediaries? Disincentives:
  - Costly to deal with individuals
  - Costly to erroneously block service
  - Liability vs subsidy

Metaphors → New Doctrine

- Cyber-attacks as crime
  - Deterence through Accountability

- Cyber-attacks as disease
  - Public Cybersecuirty

- Cyber-attacks as warfare
  - ???

For Additional Information

Doctrine for Cybersecurity. Deirdre Mulligan and Fred B. Schneider. To appear, *Daedalus*. www.cs.cornell.edu/fbs/publications/publicCybersecDaed.pdf