Moving Away From Threat-Based Analysis

David L. Alderson, Gerald G. Brown, W. Matthew Carlyle

Operations Research Department, Naval Postgraduate School, Monterey, CA 93943

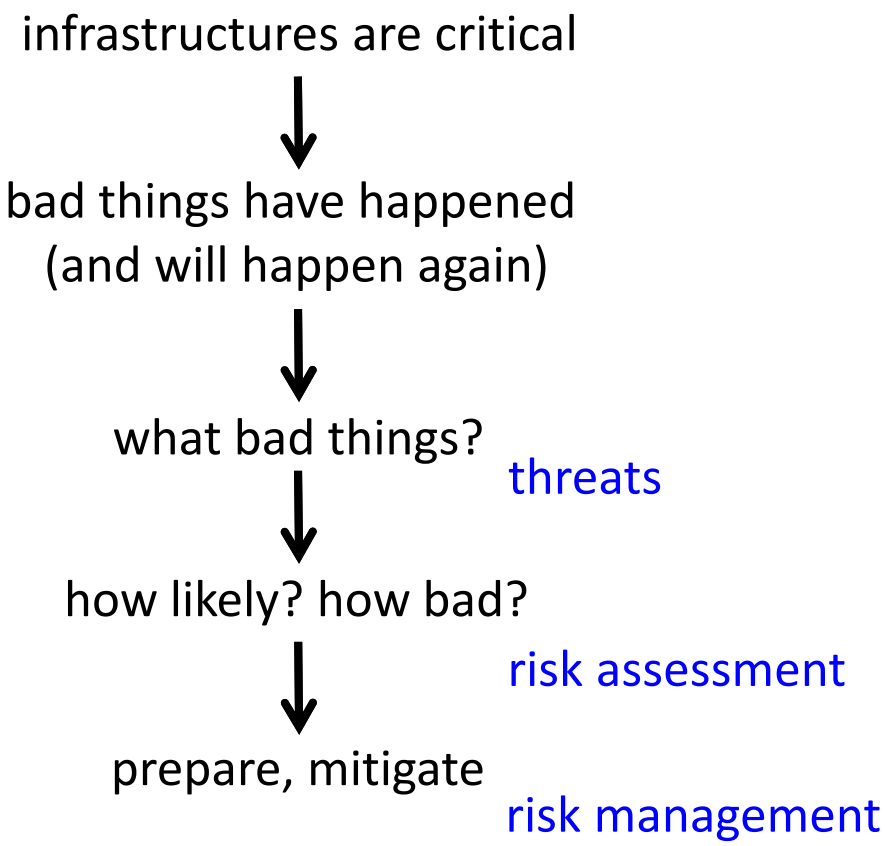
dlalders, gbrown, mcarlyle @nps.edu

1st National Symposium on Resilient Critical Infrastructure Systems

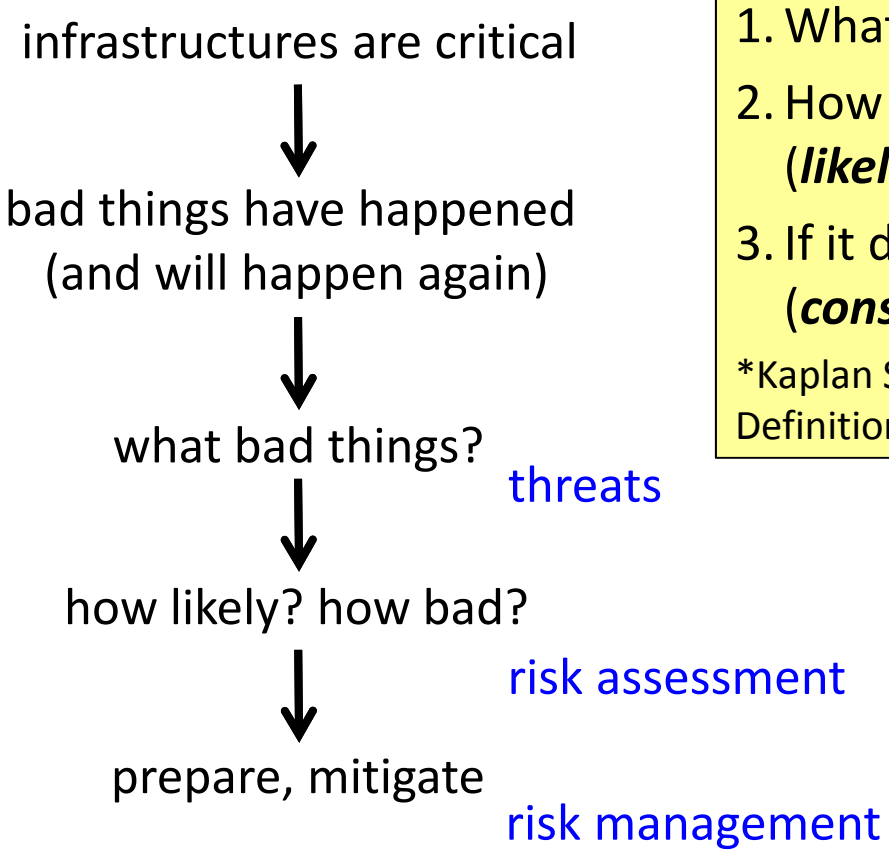
19 August 2014

This research was supported by the Office of Naval Research, the Air Force Office of Scientific Research, and the Defense Threat Reduction Agency.

current cycle of threat-based thinking



current cycle of threat-based thinking



Risk as a triplet*:

1. What can happen? (***scenario***)
2. How likely is it that it will happen? (***likelihood***)
3. If it does happen, how bad will it be? (***consequences***)

*Kaplan S, Garrick BJ, 1981, "On the Quantitative Definition of Risk," *Risk Analysis* 1(1):11–27.

current cycle of threat-based thinking

Risk as a triplet*:

1. What can happen? (***scenario***)
2. How likely is it that it will happen? (***likelihood***)
3. If it does happen, how bad will it be? (***consequences***)

*Kaplan S, Garrick BJ, 1981, "On the Quantitative Definition of Risk," *Risk Analysis* 1(1):11–27.

Claim: we need to think "like an operator"!

How to break this cycle?

"Surprise is constant."
–David Woods (Ohio State)

thinking like an operator

1. focus: continuity of function

thinking like an operator

1. focus: continuity of function

2. loss of components = loss of function

thinking like an operator

1. focus: continuity of function

2. loss of components = loss of function

3. agnostic about the source of disruption

thinking like an operator

1. focus: continuity of function
2. loss of components = loss of function
3. agnostic about the source of disruption
4. outage response = part of normal operations

thinking like an operator

1. focus: continuity of function
2. loss of components = loss of function
3. agnostic about the source of disruption
4. outage response = part of normal operations
5. what is “mission success”?

Our focus should be on ***operational resilience***.

National Strategy for Homeland Security (2007)

"We will not be able to deter all terrorist threats, and it is impossible to deter or prevent natural catastrophes. We can, however, mitigate the Nation's vulnerability to acts of terrorism, other man-made threats, and natural disasters by **ensuring the structural and operational resilience** of our critical infrastructure and key resources" (p. 27)

"We must now focus on the **resilience of the system as a whole** – an approach that centers on investments that make the system better able to absorb the impact of an event without losing the capacity to function" (p.28)

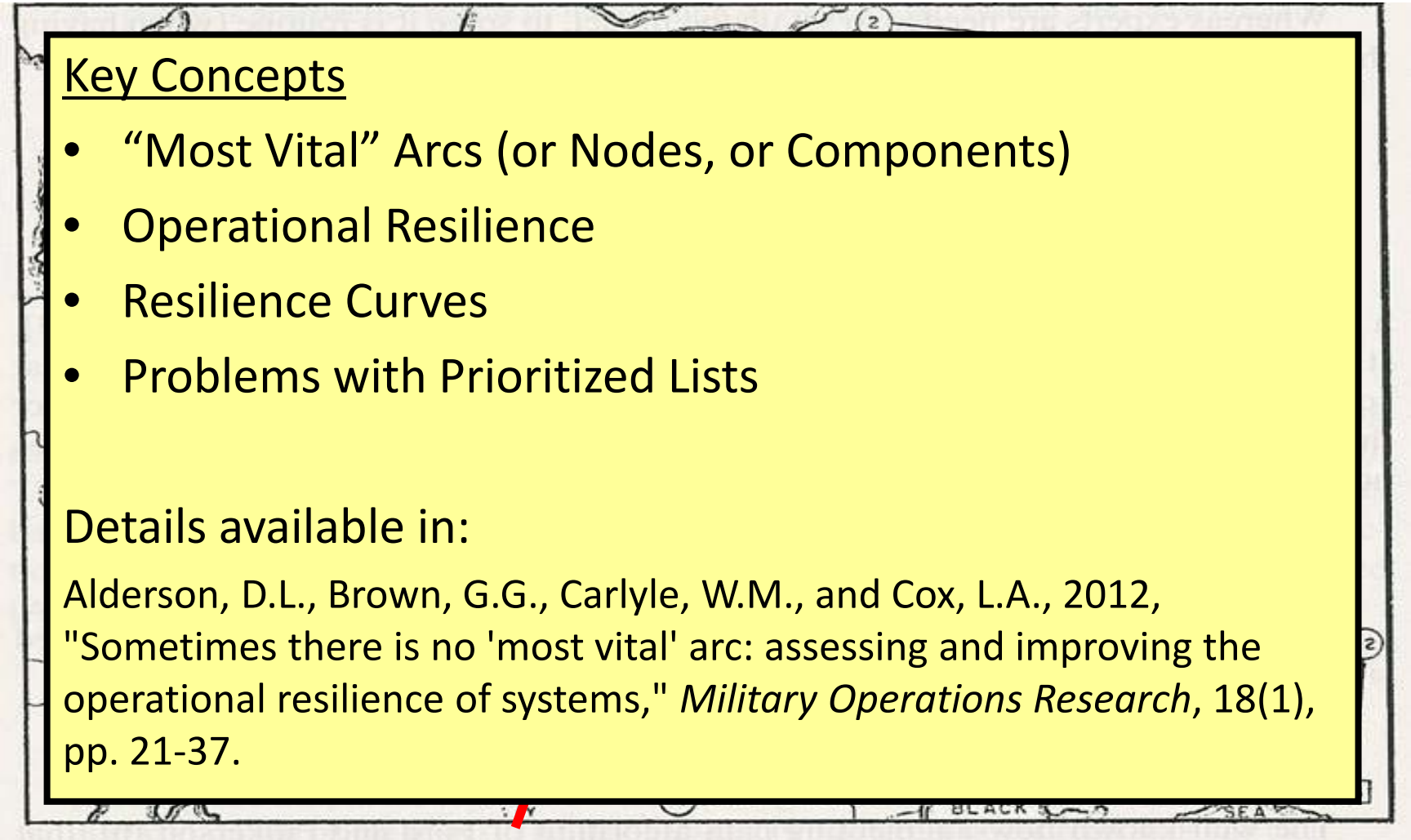
How we assess operational resilience:

- *Model the function of the infrastructure*
  - A *system of components* that work together
  - Domain-specific physics, protocols, operating rules, etc.
  - *Operator makes decisions* about system activities
  - What we want (objectives) vs. What is feasible (constraints)
- What-if scenario analysis: loss of *sets of components*

How we assess operational resilience:

- *Model the function of the infrastructure*
  - A *system of components* that work together
  - Domain-specific physics, protocols, operating rules, etc.
  - *Operator makes decisions* about system activities
  - What we want (objectives) vs. What is feasible (constraints)
- What-if scenario analysis: loss of *sets of components*
- *Discover the scenarios of concern*
- *Explore "worst-case" disruptions*
  - Hypothetical intelligent adversary
  - Worst-case adversary behavior: use of limited capability to inflict maximum damage
- In summary, we use *System Interdiction Models*

Using attack-based strategies to identify critical infrastructure components is not a new idea



Key Concepts

- "Most Vital" Arcs (or Nodes, or Components)
- Operational Resilience
- Resilience Curves
- Problems with Prioritized Lists

Details available in:

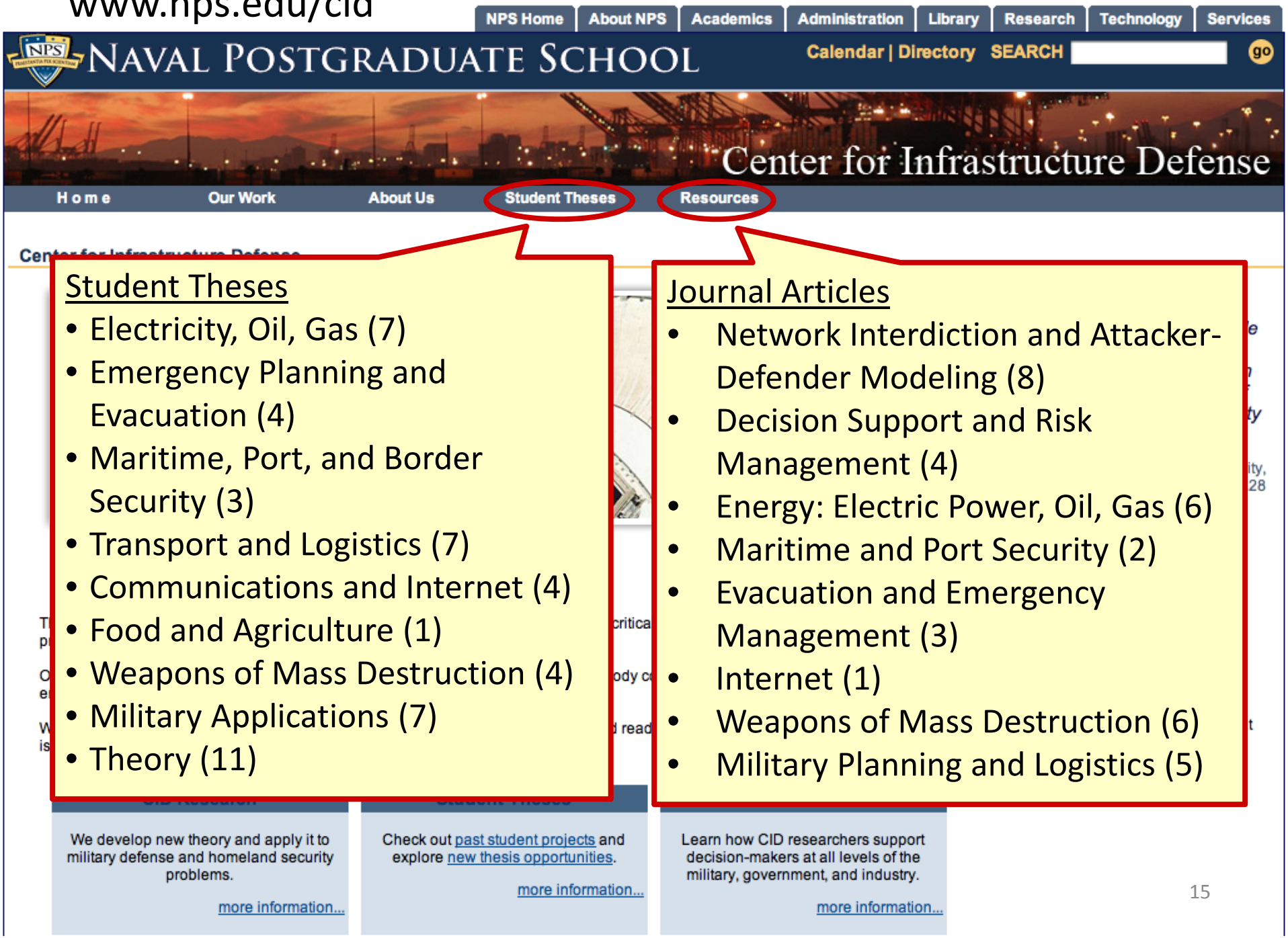
Alderson, D.L., Brown, G.G., Carlyle, W.M., and Cox, L.A., 2012, "Sometimes there is no 'most vital' arc: assessing and improving the operational resilience of systems," *Military Operations Research*, 18(1), pp. 21-37.

- Harris, T.E., and Ross, F.S. (1955), *Fundamentals of a Method for Evaluating Rail Net Capacities* (SECRET, declassified 1999), RM-1573, RAND Corp.

How does this help?

- Avoid the two biggest gotchas:
  - "We didn't know that X would cause Y…"
  - "We never thought that could happen…"
- We don't have to guess at scenarios
  - (or try to assess the intent of bad guys)
- Infrastructure is changing slowly
  - models: build once, and re-use again later

www.nps.edu/cid



Student Theses

- Electricity, Oil, Gas (7)
- Emergency Planning and Evacuation (4)
- Maritime, Port, and Border Security (3)
- Transport and Logistics (7)
- Communications and Internet (4)
- Food and Agriculture (1)
- Weapons of Mass Destruction (4)
- Military Applications (7)
- Theory (11)

Journal Articles

- Network Interdiction and Attacker-Defender Modeling (8)
- Decision Support and Risk Management (4)
- Energy: Electric Power, Oil, Gas (6)
- Maritime and Port Security (2)
- Evacuation and Emergency Management (3)
- Internet (1)
- Weapons of Mass Destruction (6)
- Military Planning and Logistics (5)