Assessing and Improving Operational Resilience

David L. Alderson, PhD

Associate Professor, Operations Research Department

Director, Center for Infrastructure Defense

Naval Postgraduate School

2018 Hazard Mitigation and Resilience Workshop
June 14-15, 2018
University of the Virgin Islands St. Thomas Campus

Naval Postgraduate School (NPS)

- Facilities of a graduate research university
- Faculty who work for the U.S. Navy, with clearances
- Students with fresh operational experience

FY2015:

- 85 master's degree programs
- 16 doctoral degree programs
- 656 faculty
- 1494 resident students includes (222 international / 42 countries)
- 997 distributed learning students

History Highlights

1909	Founded at U.S. Naval Academy
1951	Moved to Monterey, CA
	Operations Research Curriculum est.

For an overview of the school, https://my.nps.edu/web/guest/welcome-video

Operations Research at NPS

- Operations Research (OR) is the science of helping people and organizations make better decisions using
  - mathematical models, statistical analyses, simulations
  - analytical reasoning and common sense

  to the understanding and improvement of real-world operations.
- OR originated during World War II. The military uses OR at the strategic, operational, and tactical levels.
- Biggest users of OR: modern corporations.
- NPS has the oldest OR instructional program in existence.
- We conduct **analysis** and develop **decision support tools** that are of immediate operational relevance to the decision-maker.
- Often centered around Masters theses.

What is Critical Infrastructure?

- ***Critical Infrastructure (CI)***: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" ***--Section 1016(e) of the USA PATRIOT Act of 2001***

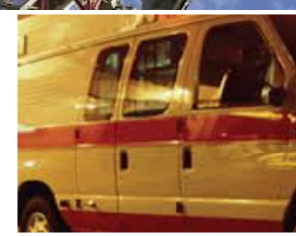












Critical Infrastructure Systems: NPS has a unique perspective and capability

- We have been studying critical infrastructure for decades.
- We look at our own domestic infrastructure through the eyes of intelligent adversaries.
- We have conducted over 150 “red team analyses” to plan attacks on our own infrastructure (and determine how to mount effective hardening and defensive efforts)

Critical Infrastructure Systems: NPS has a unique perspective and capability

- We have been studying critical infrastructure for decades.
- We look at our own domestic infrastructure through the eyes of intelligent adversaries.
- We have conducted over 150 “red team analyses” to plan attacks on our own infrastructure (and determine how to mount effective hardening and defensive efforts)

My Goal For Today

Share my perspective:

10 key ideas for thinking about how to assess and improve operational resilience of critical infrastructures

Idea #1: **Start by focusing on delivery of services**,
not mitigation of hazards/threats

Idea #1: **Start by focusing on delivery of services,** not mitigation of hazards/threats

What we need to do
(operation)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

Idea #1: **Start by focusing on delivery of services,**
not mitigation of hazards/threats

What we need to do
(operation)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

What can go wrong
(interdiction)

- Extreme Weather
  - Coastal Flooding
  - Rainfall Flooding
  - Wind
  - Drought
- Human accident
- Technological failure
- Deliberate attack

Idea #1: **Start by focusing on delivery of services,**
not mitigation of hazards/threats

What we need to do (operation)	**What can go wrong** (interdiction)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

- Extreme Weather
  - Coastal Flooding
  - Rainfall Flooding
  - Wind
  - Drought
- Human accident
- Technological failure
- Deliberate attack

Idea #2: **Avoid getting stuck on predefined threat scenarios.**

- Surprise Happens. Things we have not imagined.
- Tunnel vision (on the last disaster). Need to be proactive, not reactive.

A policy shift toward "operational resilience"

U.S. 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)

Most recently: U.S. Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience, 2013.

“system as a whole” and “capacity to function”

“system as a whole” and “capacity to function”

How to Think About Critical Infrastructure (CI)

- A list of *assets*
- An interconnected (network) *system* that works to achieve a particular function

“system as a whole” and “capacity to function”

How to Think About Critical Infrastructure (CI)

✖ • A list of *assets*

✔ • An interconnected (network) *system* that works to achieve a particular function “system as a whole” and “capacity to function”

How to Think About Critical Infrastructure (CI)

- ✖ A list of *assets*
- ✔ An interconnected (network) *system* that works to achieve a particular function

Idea #3: We need to think in terms of systems.

We want to make our operations (public and private) resilient to disruptive events.

We need our infrastructure systems to continue to function even when “bad things” happen.

What we need to do
(operation)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

What can go wrong
(interdiction)

- Extreme Weather
  - Coastal Flooding
  - Rainfall Flooding
  - Wind
  - Drought
- Human accident
- Technological failure
- Deliberate attack

What we need to do (operation)	**What can go wrong** (interdiction)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

- Extreme Weather
  - Coastal Flooding
  - Rainfall Flooding
  - Wind
  - Drought
- Human accident
- Technological failure
- Deliberate attack

Idea #4: **Study the adversarial relationship** to get insights about vulnerabilities and mitigations.

Our Approach in a Nutshell

Assessing and Improving Operational Resilience

Our Approach in a Nutshell

Assessing and Improving Operational Resilience

1. Using a limited budget, we want to invest so that we still achieve mission success even when bad things happen (operational resilience)

Our Approach in a Nutshell

Assessing and Improving Operational Resilience

1. Using a limited budget, we want to invest so that we still achieve mission success even when bad things happen (operational resilience)

2. To learn how to "defend" these systems, first figure out how to <u>attack</u> them

Our Approach in a Nutshell

Assessing and Improving Operational Resilience

1. Using a limited budget, we want to invest so that we still achieve mission success even when bad things happen (operational resilience)
2. To learn how to "defend" these systems, first figure out how to <u>attack</u> them
3. To learn how to attack CI, first learn how it to operate it (i.e., how it works)

Our Approach in a Nutshell

Assessing and Improving Operational Resilience

1. Using a limited budget, we want to invest so that we still achieve mission success even when bad things happen (operational resilience)
2. To learn how to "defend" these systems, first figure out how to <u>attack</u> them
3. To learn how to attack CI, first learn how it to operate it (i.e., how it works)

We call these Attacker-Defender and Defender-Attacker-Defender models.

Idea #5: Take an ”operational” perspective

What we need to do
(operation)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

Idea #5: Take an "operational" perspective

What we need to do
(operation)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

Need to understand the demands of the population

- Demographics
- Geography
- Population density
- Special needs

Idea #5: Take an ”operational” perspective

What we need to do
(operation)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

Need to understand the demands of the population
- Demographics
- Geography
- Population density
- Special needs

Move goods/services from areas of supply to demands:
- Must include infrastructure owners and operators
- Both public <u>and</u> private!

Idea #5: Take an ”operational” perspective

What we need to do
(operation)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

Idea #6: Often represented as **flows** through **networks**.

Need to understand the demands of the population

- Demographics
- Geography
- Population density
- Special needs

Move goods/services from areas of supply to demands:

- Must include infrastructure owners and operators
- Both public and private!

Idea #5: Take an ”operational” perspective

What we need to do
(operation)

- Electricity
- Fuels
- Transportation
- Communications
- Water & Wastewater
- Emergency response

Idea #6: Often represented as **flows** through **networks**.

Idea #7: Measure **performance.** Define **mission success.**

Need to understand the demands of the population
- Demographics
- Geography
- Population density
- Special needs

Move goods/services from areas of supply to demands:
- Must include infrastructure owners and operators
- Both public and private!

BUT… Systems Are Complicated, Sometimes Complex

- Interactions often non-additive and non-intuitive.
- An event in one location can often affect things that are far away, and it can be hard to predict how this happens.
- The contribution/importance of a single component to system function may depend on interactions with other components.

BUT… Systems Are Complicated, Sometimes Complex

- Interactions often non-additive and non-intuitive.
- An event in one location can often affect things that are far away, and it can be hard to predict how this happens.
- The contribution/importance of a single component to system function may depend on interactions with other components.

Idea #8: Guessing at what is “most critical” is prone to error

Idea #8: Guessing at what is "most critical" is prone to error

- When determining how best to protect systems, a natural question is, *"What components are most critical?"*
- Better yet: *Which components, if lost, would be most disruptive to system function?*

Definition: A component is *critical* if losing it would significantly reduce system function (relative to the reduction from losing other components).

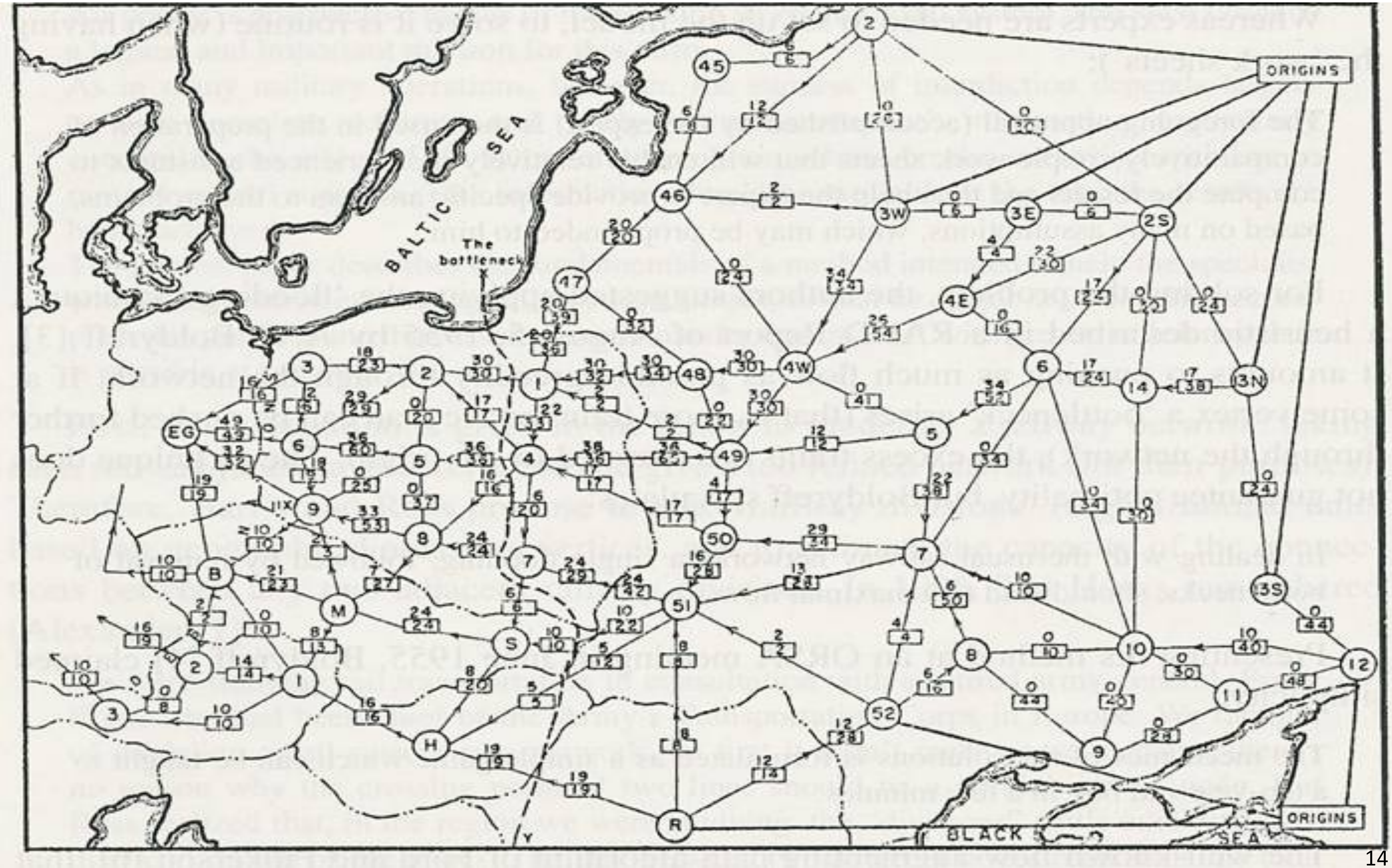
Let's use a historical example to illustrate…

The Russian Rail Network (circa 1955)

Data from Figure 7 of:

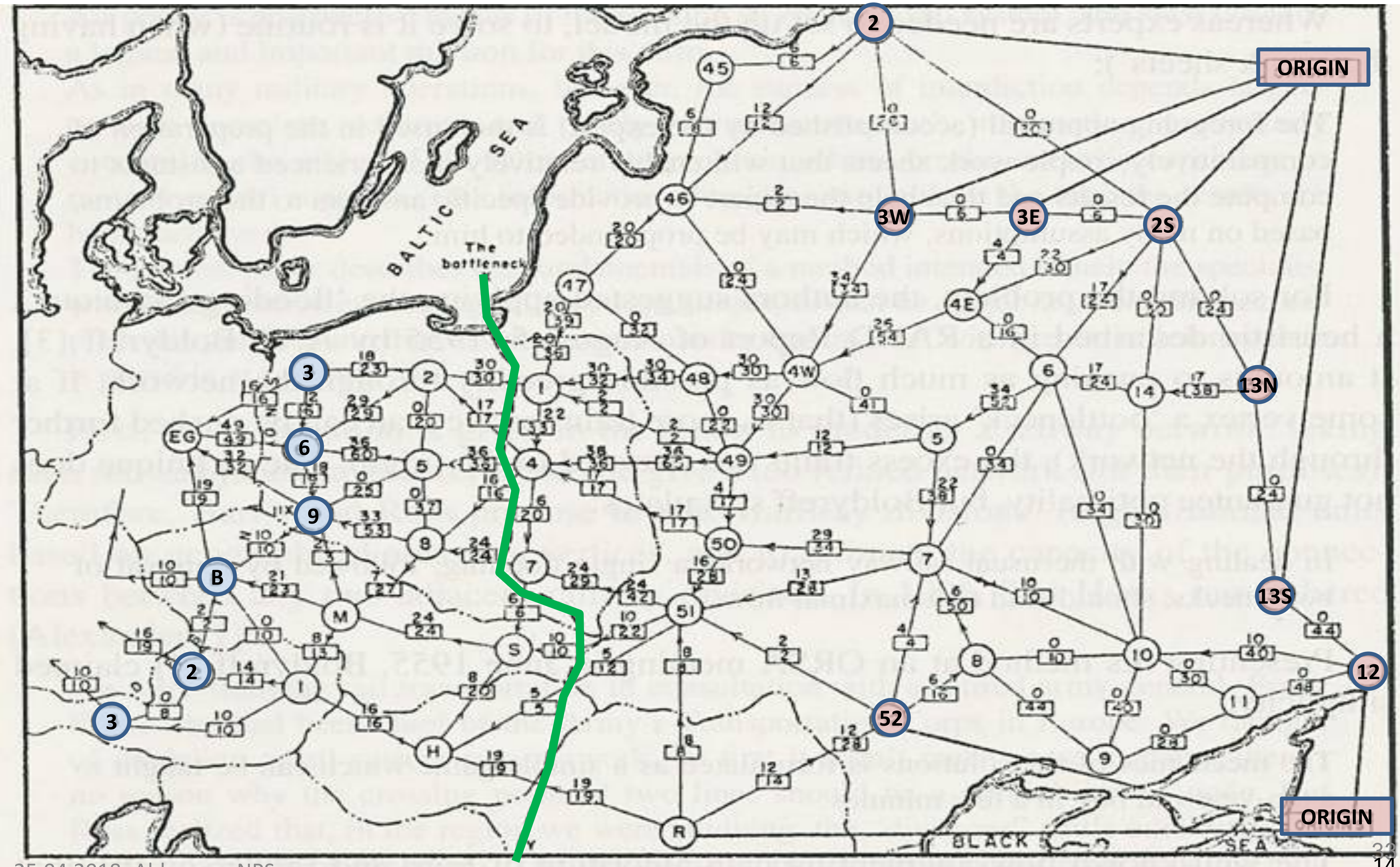
Harris, T.E., and Ross, F.S. (1955), *Fundamentals of a Method for Evaluating Rail Net Capacities* (SECRET, declassified 1999), RM-1573, RAND Corp.

What is the capacity of the USSR to deliver materiel to Europe via rail?



What is the capacity of the USSR to deliver materiel to Europe via rail?

destination nodes minimum capacity cut origin nodes

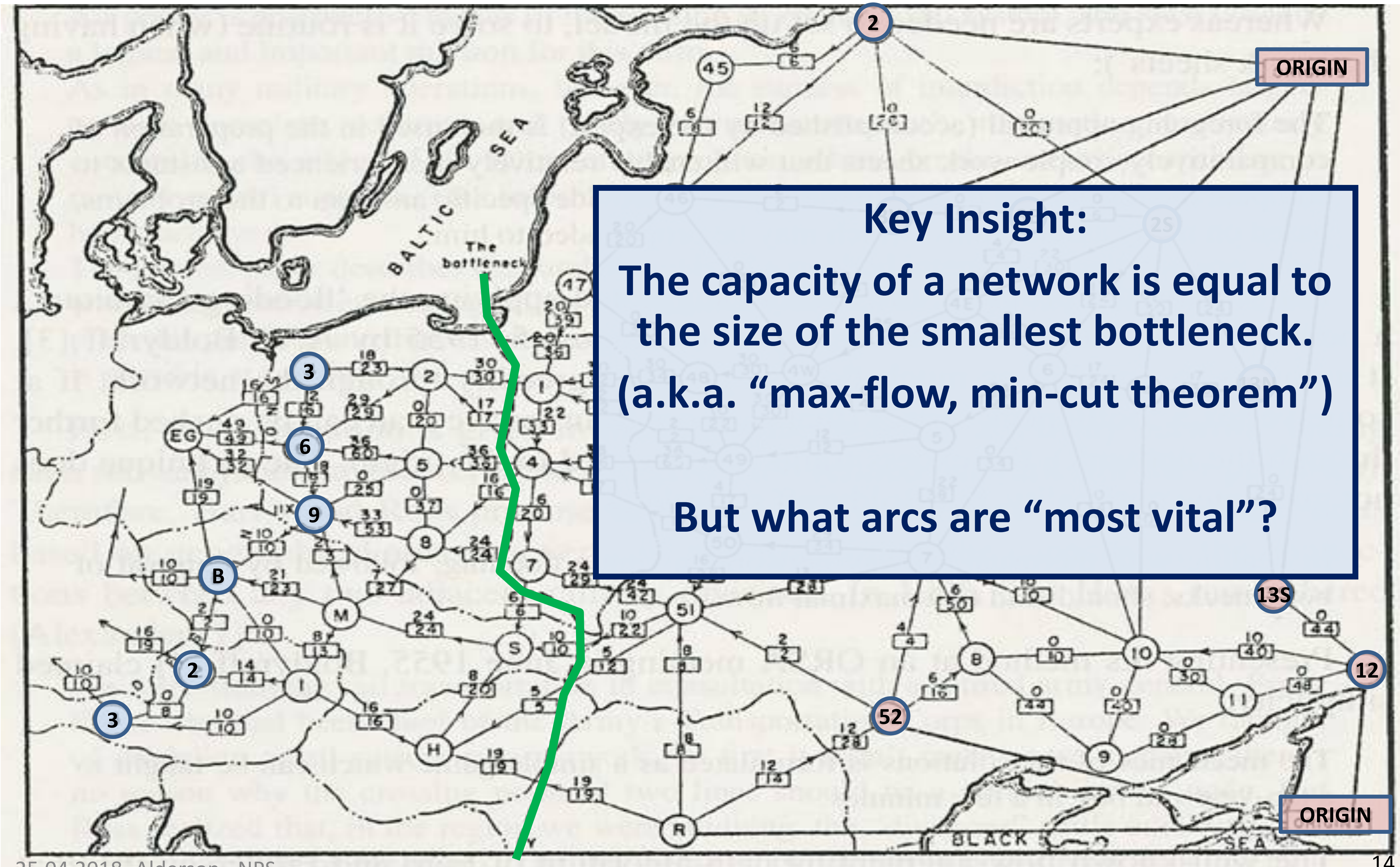


What is the capacity of the USSR to deliver materiel to Europe via rail?

destination nodes

minimum capacity cut

origin nodes



Key Insight:

The capacity of a network is equal to the size of the smallest bottleneck.

(a.k.a. "max-flow, min-cut theorem")

But what arcs are "most vital"?

Finding the “Most Vital” Arc(s) is not trivial!

- It requires you to consider not only the current paths through the network but also any alternate paths
- Because… the system can adjust its flows in response to a disruption!

Finding the "Most Vital" Arc(s) is not trivial!

- It requires you to consider not only the current paths through the network but also any alternate paths
- Because… the system can adjust its flows in response to a disruption!

Possible "guessing rules" for determining what is most vital

(Ahuja, Magnanti, and Orlin, "Network Flows", Prentice-Hall, 1993)

- An arc having the *largest capacity*
- An arc carrying the *largest flow in the optimal solution*
- An arc having the *largest capacity in a minimum-capacity cut*
- *Any most-vital arc is in some minimum-capacity cut*

Finding the “Most Vital” Arc(s) is not trivial!

- It requires you to consider not only the current paths through the network but also any alternate paths
- Because… the system can adjust its flows in response to a disruption!

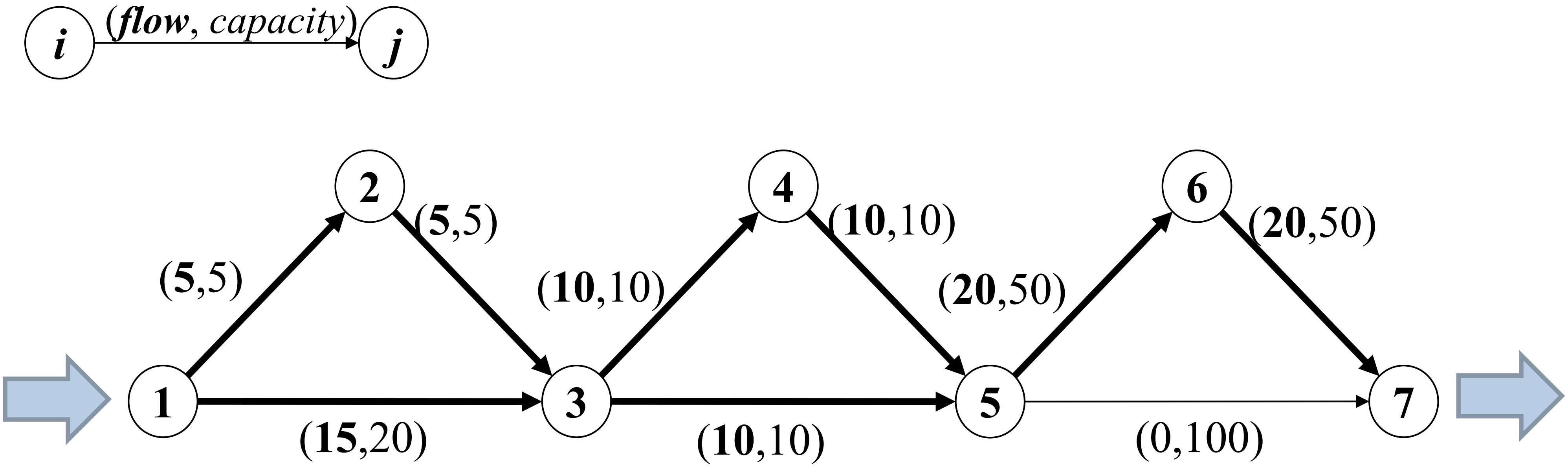
Possible “guessing rules” for determining what is most vital

(Ahuja, Magnanti, and Orlin, “Network Flows”, Prentice-Hall, 1993)

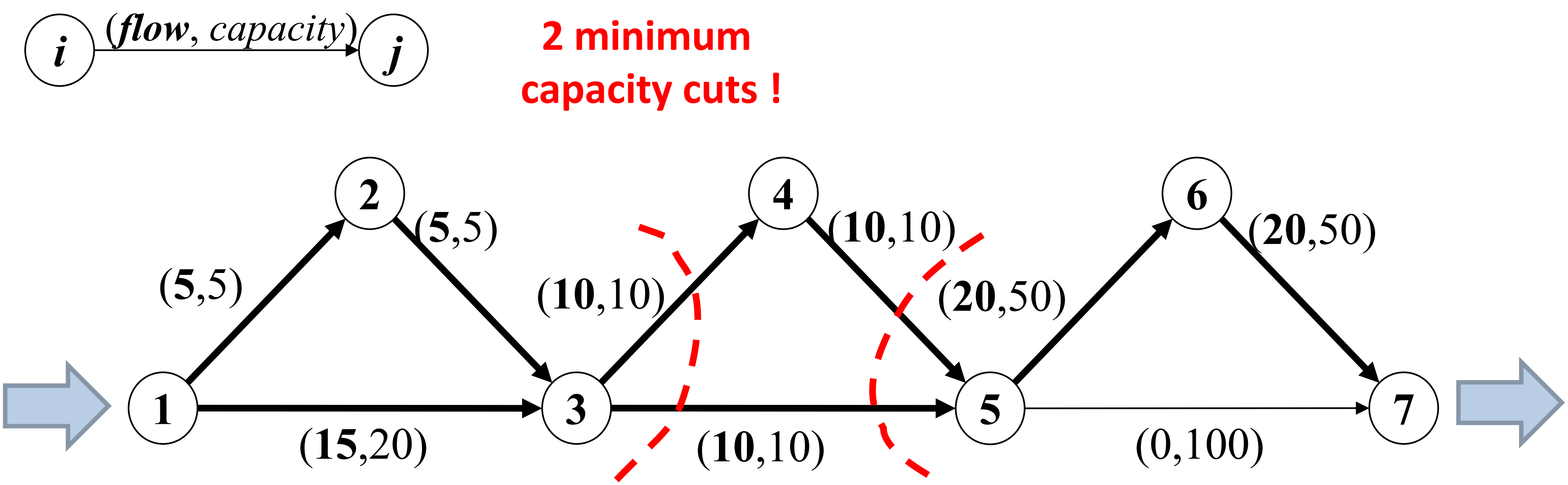
- An arc having the *largest capacity*
- An arc carrying the *largest flow in the optimal solution*
- An arc having the *largest capacity in a minimum-capacity cut*
- *Any most-vital arc is in some minimum-capacity cut*

In general, none of these “guessing rules” work!

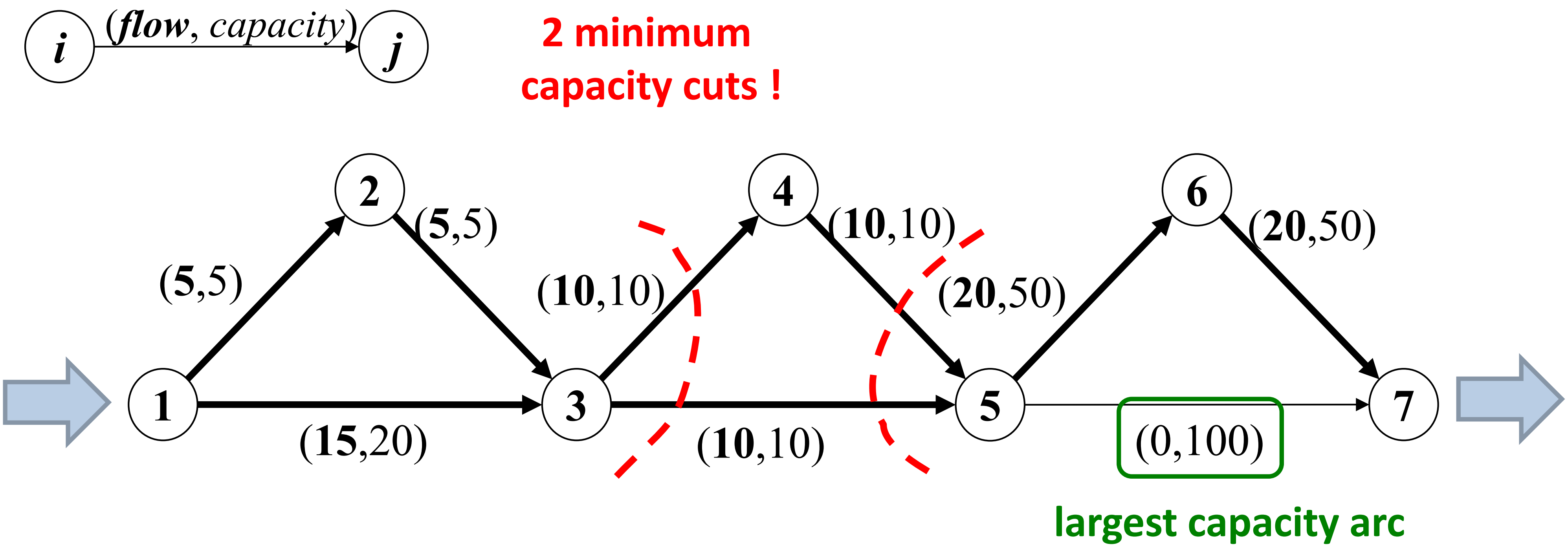
counter-example: guessing to find most vital arc



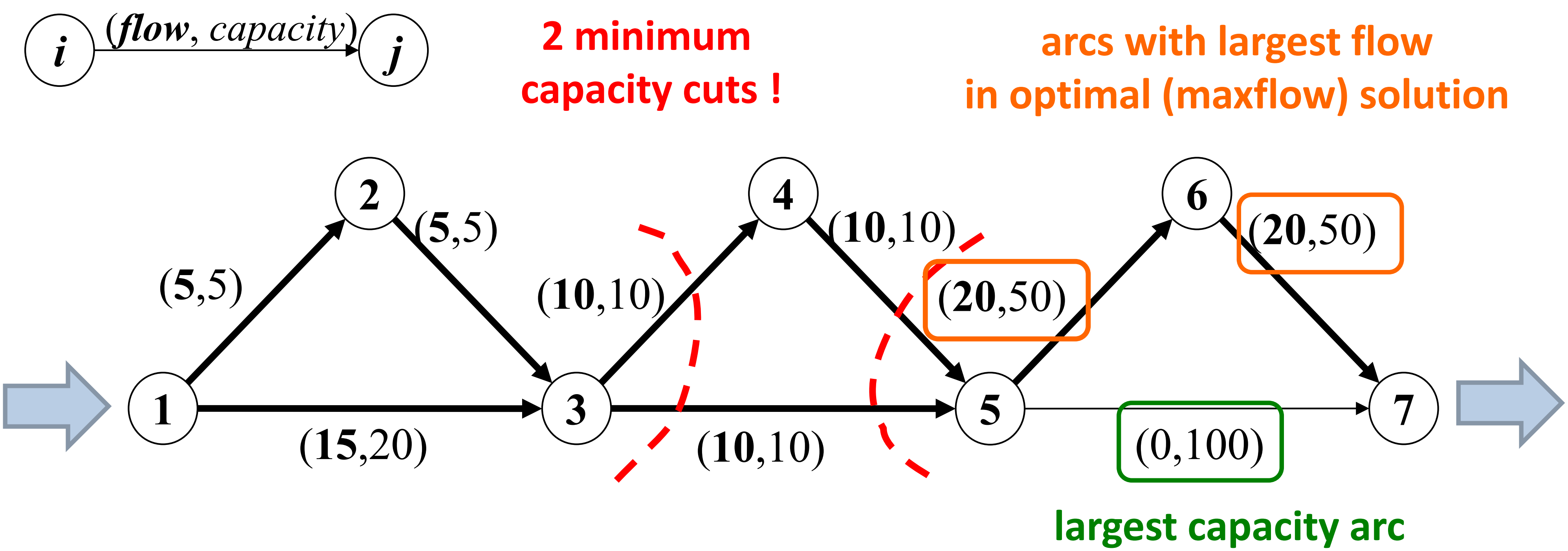
counter-example: guessing to find most vital arc



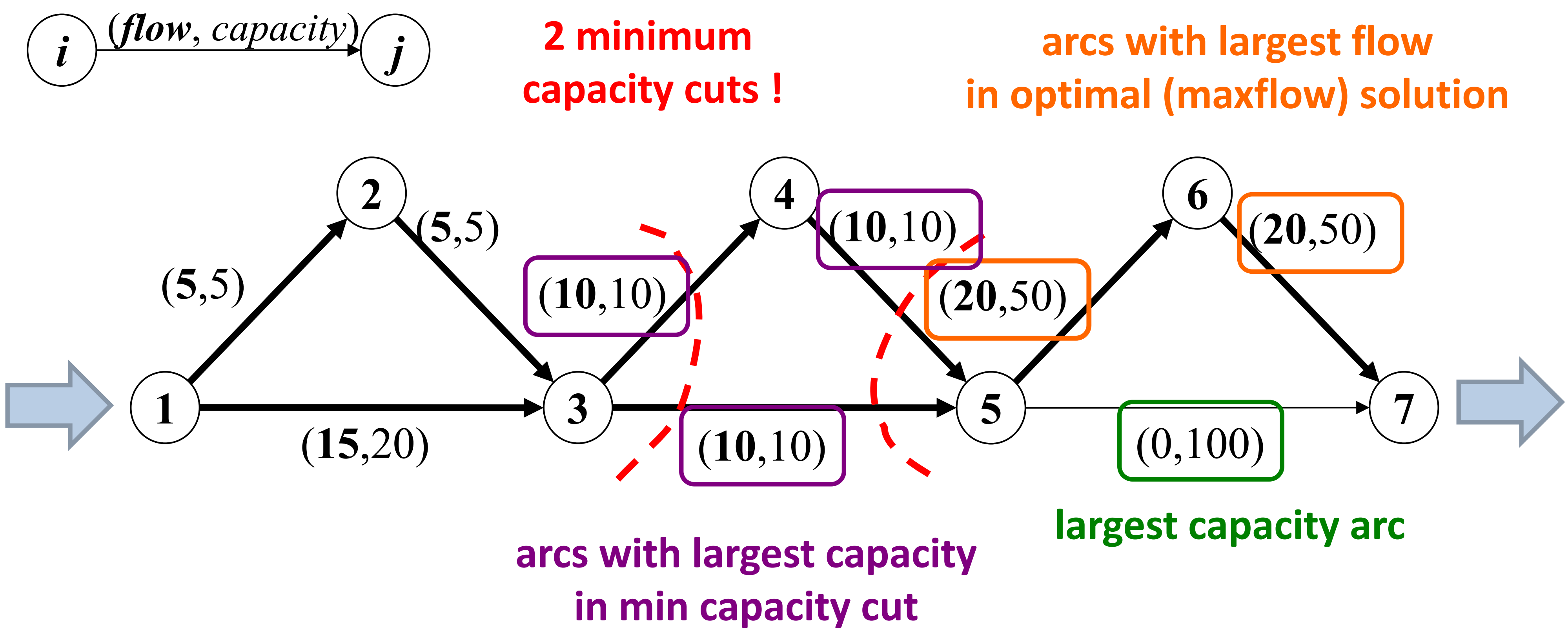
counter-example: guessing to find most vital arc



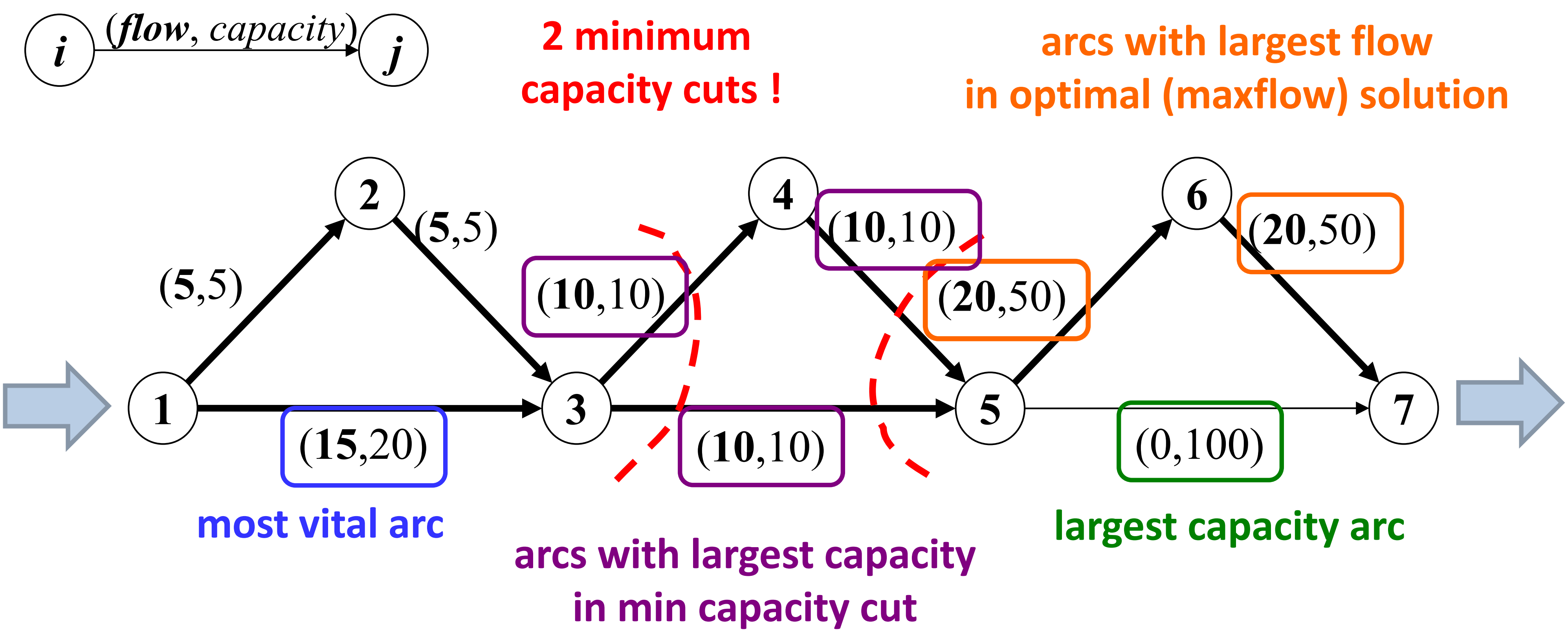
counter-example: guessing to find most vital arc



counter-example: guessing to find most vital arc



counter-example: guessing to find most vital arc



In general, you cannot reliably guess. Instead, determining a most vital arc requires solving a *network interdiction problem*.

Idea #9: Use an attack-based (adversarial) perspective for planning. (This is also sometimes called “red teaming”.)

- It helps to focuses on system operation.
- It helps to discover vulnerabilities.
- It helps to uncover interdependencies.
- It helps to think about mitigation.

Idea #9: Use an attack-based (adversarial) perspective for planning. (This is also sometimes called “red teaming”.)

- It helps to focuses on system operation.
- It helps to discover vulnerabilities.
- It helps to uncover interdependencies.
- It helps to think about mitigation.

Idea #10: Large-scale, long-term interruptions in critical infrastructure services can be caused by things much smaller than two Category-5 hurricanes!

Idea #11: **Investing for resilience can work better** when you to think about the system as a whole.

- Hardening (reinforcement)
- Redundancy (backups, spares)
- Capacity expansion
- New infrastructure

This means studying more than just "how we actually do it now".

It requires we also consider "how could we do it now (and in the future)"!

References and Acknowledgments

- Alderson, D.L., Brown, G., Carlyle, W.M., and Wood, R.K., 2017, **"Assessing and Improving the Operational Resilience of a Large Highway Infrastructure System to Worst-Case Losses,"** *Transportation Science*, doi.org/10.1287/trsc.2017.0749.
- Alderson, D.L., Brown, G., and Carlyle, W.M., 2015, **“Operational Models of Infrastructure Resilience,”** *Risk Analysis* 35(4): 562-586 (received Award for Best Paper of 2015 in Risk Analysis).
- Alderson, D.L., G.G. Brown, W.M. Carlyle. 2014. **“Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems.”** A. Newman, J. Leung, eds., *Tutorials in Operations Research: Bridging Data and Decision*. Institute for Operations Research and Management Science, Hanover, MD, 180-215.
- Alderson, D.L., G.G. Brown, W.M. Carlyle, L.A. Cox. 2013. **“Sometimes there is no ‘most vital’ arc: assessing and improving the operational resilience of systems.”** *Military Operations Research* 18(1) 21-37.
- Brown, G., Carlyle, M., Salmerón, J. and Wood, K., 2006, **“Defending Critical Infrastructure,”** *Interfaces*, 36, pp. 530-544.

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

We have used scores of these models to assess resilience for a wide range of systems

Operator Models

- Shortest-path problems
- Max-flow problems
- Min-cost network flow problems
- Multi-commodity flow problems
- Project scheduling problems
- Linear programs
- Integer-Linear programs
- Nonlinear programs
- Nonlinear-Integer programs

Applications

- Electric power
- Potable water
- Fuel pipelines
- Roadway transportation
- Multi-modal shipping
- Ports
- Supply chains
- Telecommunications
  - Undersea cables
  - Wireless network design
- Interdependent infrastructures

These techniques scale up to realistic size and fidelity, and admit a host of standard models, many already in use by system operators.

Case Study: Guam Power Authority

Guam Power Authority's transmission system (115-13.8 kV):

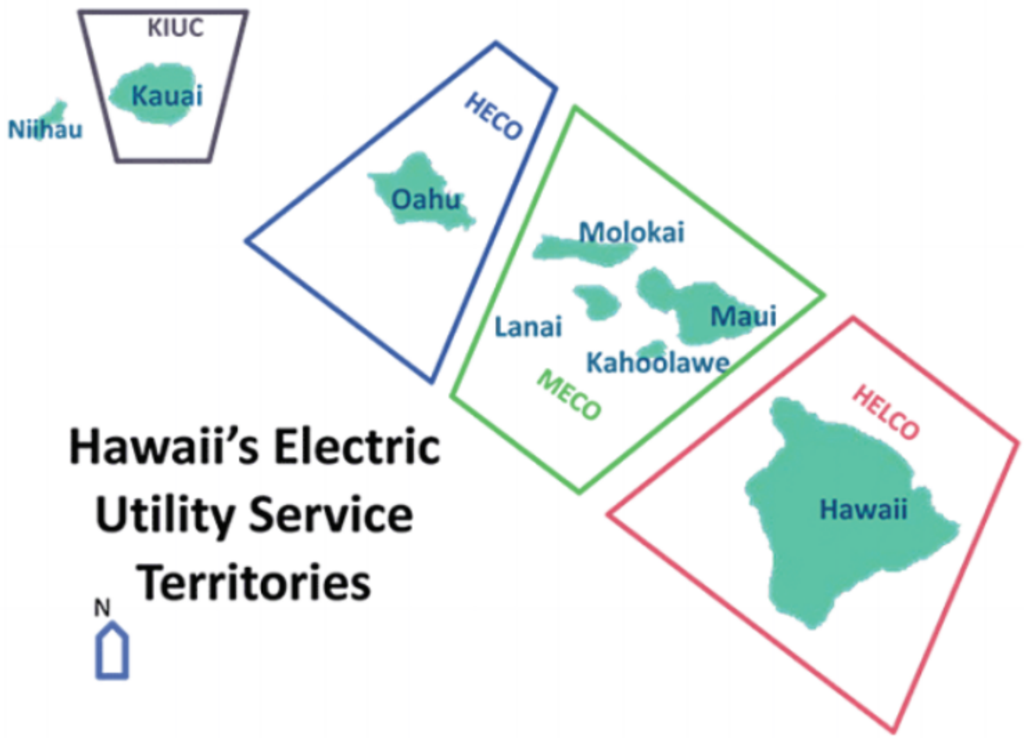
- ~100 buses
- ~50 HV lines
- ~50 transformers
- 10s of substations
- 10s of generating units:
  - >550 MW

Both Attacker and Defender Analysis

<u>Reference</u>: Salmerón, J., Alderson, D., Brown, G., and Wood, R.K., 2012, **Resilience Report: The Guam Power Authority Electric Power Grid: Analyzing Vulnerability to Physical Attack (U)**, Center for Infrastructure Defense Technical Report NPS-OR-12-002, May. *Distribution authorized to DoD and DoD Contractors only due to infrastructure vulnerability analysis (10 May 2012). Other requests for this document must be referred to President, Code 261, Naval Postgraduate School, Monterey, CA 93943-5000 via the Defense Technical Information Center, 8725 John J. Kingman Rd., STE 0944, Ft. Belvoir, VA 22060-6218.*

Prepared for: Air Force Research Lab (AFRL), Airbase Technologies Division, 139 Barnes Drive, Suite 2, Tyndal Air Force Base, FL 32403-5323.

Case Study: Hawaii



Map credit: "Hawai'i Energy Facts and Figures: May 2015," Hawai'i State Energy Office

- 10s buses
- ~100 high-voltage AC transmission lines
- no DC lines
- ~100 transformers
- 10s generating units: total gen. capacity of ~2,500 MW
- Total load: ~1,200 MW

Attacker, Defender, & Spare Parts Analysis

- Can a small number of coordinated attacks inflict significant damage for which repair would require considerable reconstitution time? What is the best means of hardening against such attacks?
- How can a limited stockpile of medium- and high-voltage spare transformers contribute most to mitigating vulnerability, i.e., to "increasing system resilience."

Reference: Salmerón, J., Alderson, D., and Brown, G., 2018, **Resilience Report: Analysis of Hawaiian Electric Power Grid to Physical Attack (U)**, NPS Technical Report NPS-OR-18-001R, February. Restricted distribution (PCII).

Prepared for: Department of Homeland Security, Infrastructure Protection Division.

We have used scores of these models to assess resilience for a wide range of systems

Jack Heide: "if you can keep people safe in their homes with food and water, then…"

How in the USVI do people get the things they need? How else could they get these things?

Applications

- Electric power
- Potable water
- Fuel pipelines
- Roadway transportation
- Multi-modal shipping
- Ports
- Supply chains
- Telecommunications
  - Undersea cables
  - Wireless network design
- Interdependent infrastructures

These techniques scale up to realistic size and fidelity, and admit a host of standard models, many already in use by system operators.

Contact Information

- Dr. David Alderson

Director, Center for Infrastructure Defense
Naval Postgraduate School
831-656-1814, dlalders@nps.edu
http://faculty.nps.edu/dlalders

- NPS Center for Infrastructure Defense

http://www.nps.edu/cid

- Resilience Week, August 20-24, Denver

http://www.resilienceweek.com