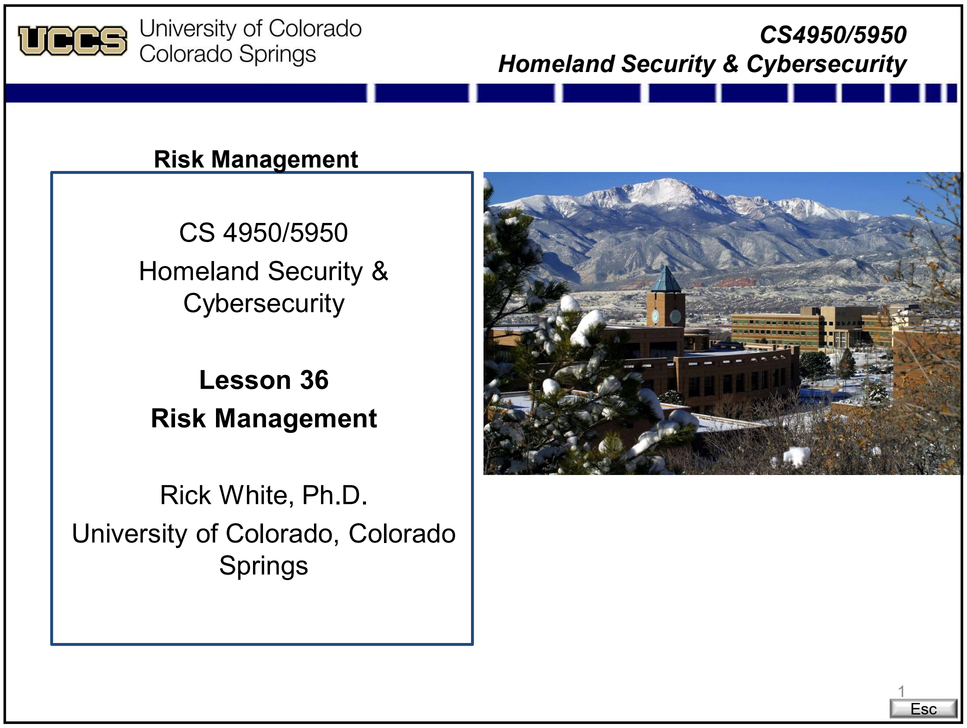
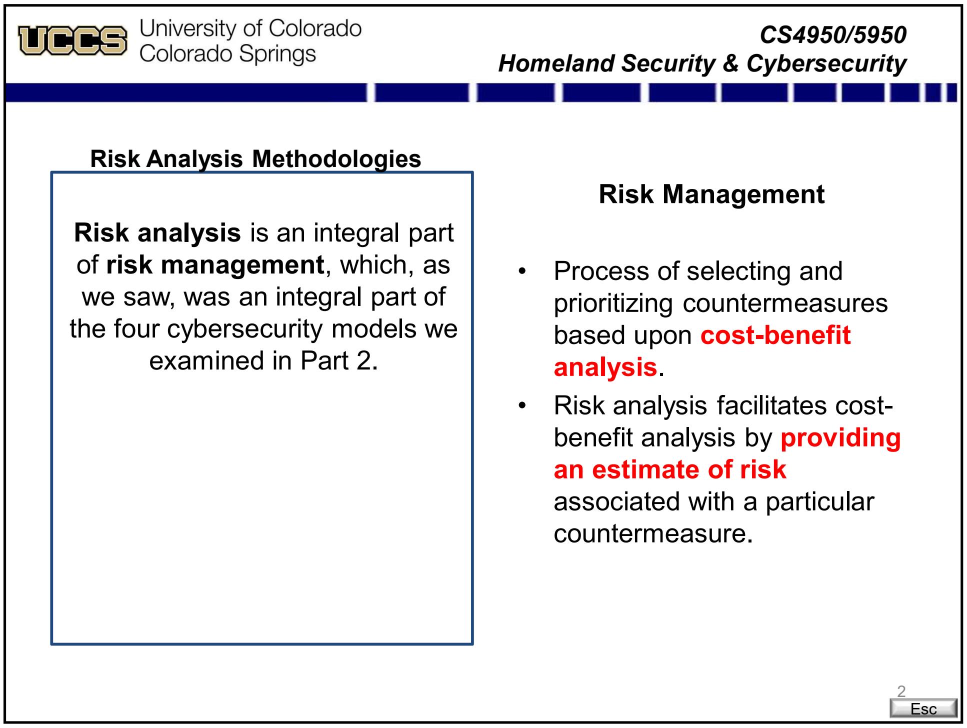


Risk Management

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 36
Risk Management

Rick White, Ph.D.
University of Colorado, Colorado Springs

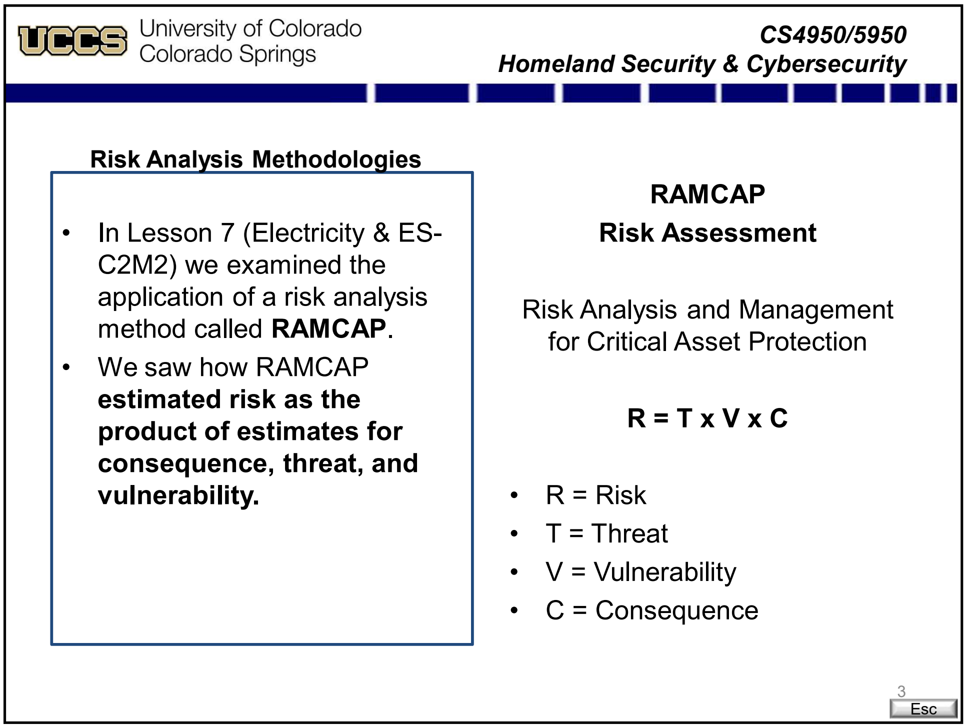


Risk Analysis Methodologies

Risk analysis is an integral part of **risk management**, which, as we saw, was an integral part of the four cybersecurity models we examined in Part 2.

Risk Management

- Process of selecting and prioritizing countermeasures based upon **cost-benefit analysis**.
- Risk analysis facilitates cost-benefit analysis by **providing an estimate of risk** associated with a particular countermeasure.



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- In Lesson 7 (Electricity & ES-C2M2) we examined the application of a risk analysis method called **RAMCAP**.
- We saw how RAMCAP **estimated risk as the product of estimates for consequence, threat, and vulnerability.**

RAMCAP
Risk Assessment

Risk Analysis and Management for Critical Asset Protection

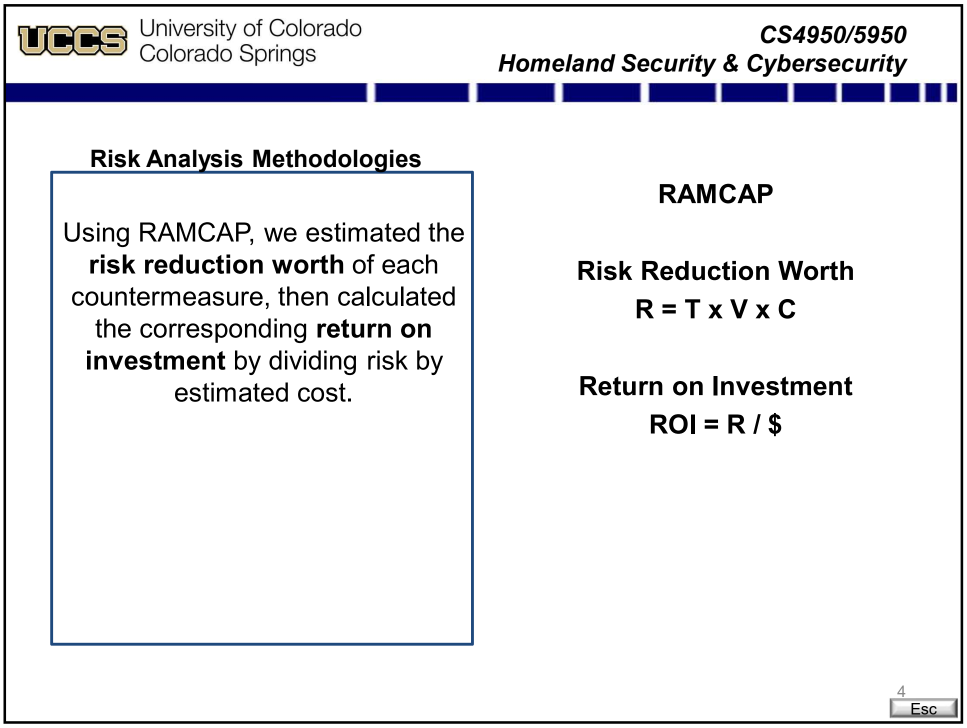
R = T x V x C

- R = Risk
- T = Threat
- V = Vulnerability
- C = Consequence

3

Esc

3



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

Using RAMCAP, we estimated the **risk reduction worth** of each countermeasure, then calculated the corresponding **return on investment** by dividing risk by estimated cost.

RAMCAP

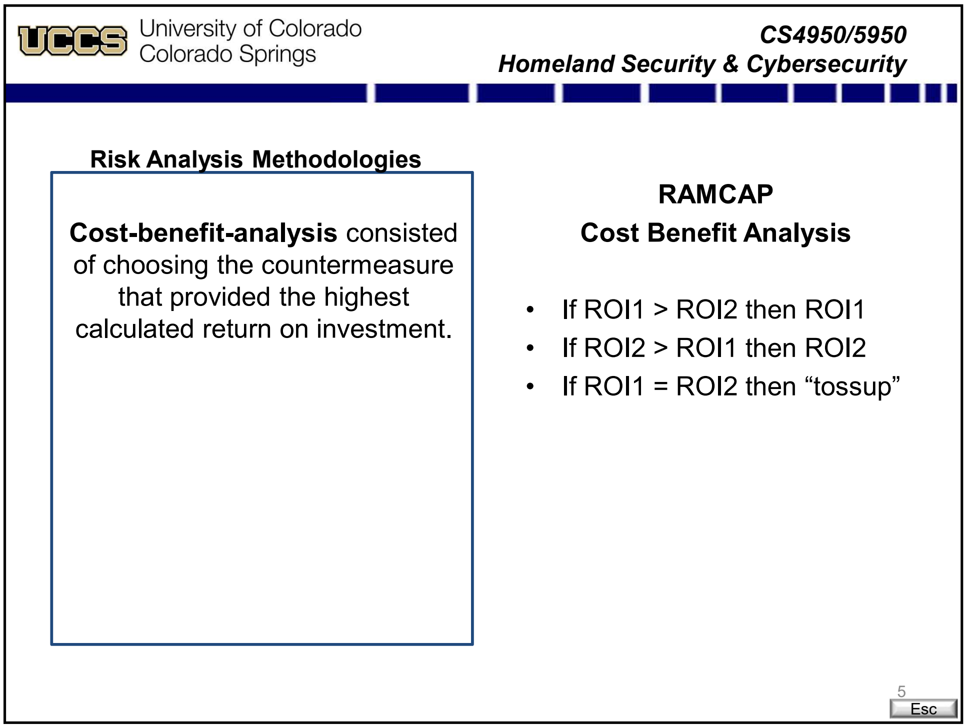
Risk Reduction Worth
R = T x V x C

Return on Investment
ROI = R / $

4

Esc

4



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

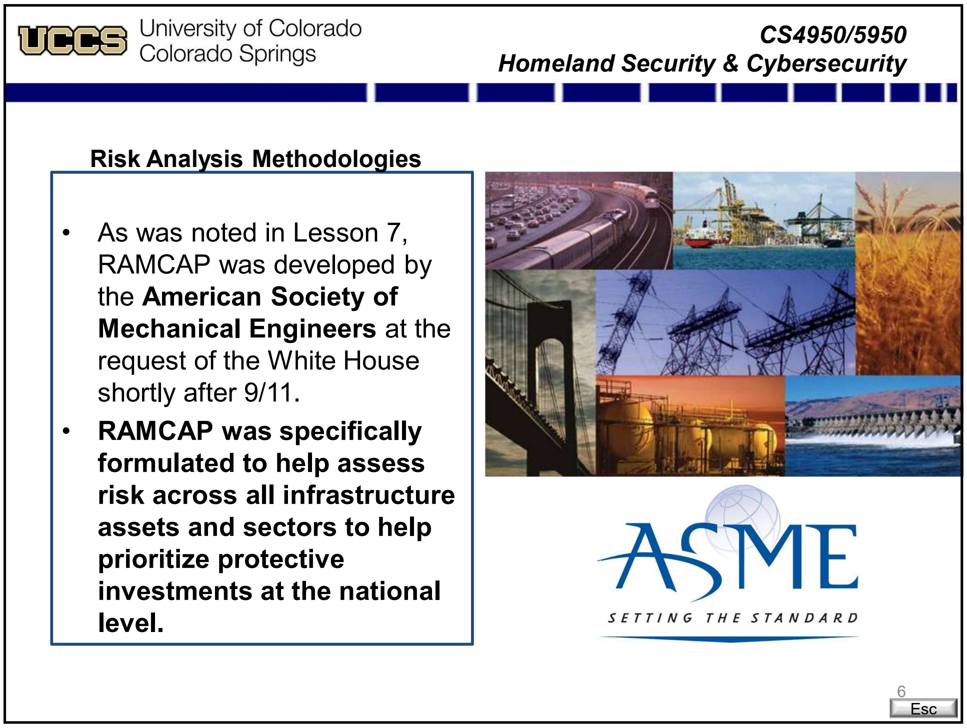
Cost-benefit-analysis consisted of choosing the countermeasure that provided the highest calculated return on investment.

RAMCAP
Cost Benefit Analysis

- If ROI1 > ROI2 then ROI1
- If ROI2 > ROI1 then ROI2
- If ROI1 = ROI2 then “tossup”

5
Esc

5



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- As was noted in Lesson 7, RAMCAP was developed by the **American Society of Mechanical Engineers** at the request of the White House shortly after 9/11.
- **RAMCAP was specifically formulated to help assess risk across all infrastructure assets and sectors to help prioritize protective investments at the national level.**

6
Esc

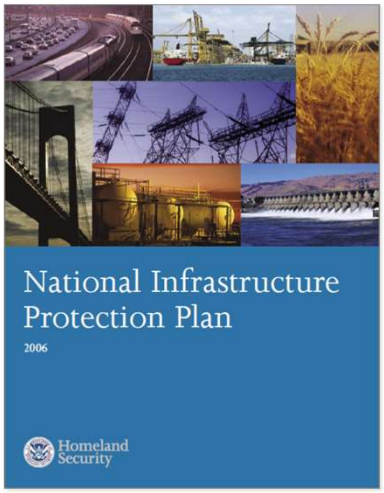
6

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- Unfortunately, RAMCAP fell into obscurity shortly after it was introduced in the 2006 National Infrastructure Protection Plan.
- One of the reasons RAMCAP fell into disuse was that many believe there is no “one size fits all” when it comes to risk analysis.
- Indeed, **there are an estimated 250 critical infrastructure risk methodologies,** which begs the question, **“why so many?”**



7

Esc

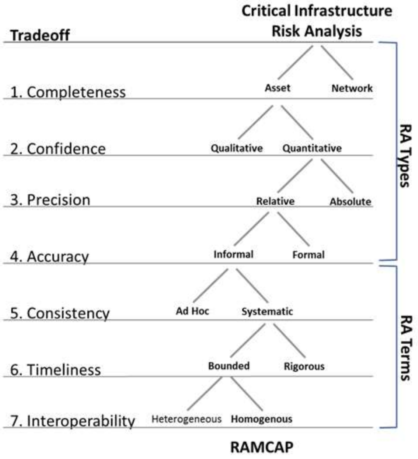
7

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- The answer lies in the fact that **each methodology is the result of a different set of tradeoffs.**
- RAMCAP itself is uniquely distinguished by its own set of tradeoffs.



Tradeoff

Critical Infrastructure Risk Analysis

1. Completeness — Asset / Network

2. Confidence — Qualitative / Quantitative

3. Precision — Relative / Absolute

4. Accuracy — Informal / Formal

5. Consistency — Ad Hoc / Systematic

6. Timeliness — Bounded / Rigorous

7. Interoperability — Heterogeneous / Homogenous

RAMCAP

RA Types

RA Terms

8

Esc

8

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- It begins with the question of **completeness**: **do you analyze the network or the nodes?**
- In other words, **do you also include interdependencies** in your risk analysis?
- RAMCAP does not include interdependencies in its analysis.
- RAMCAP risk analysis focuses on the individual asset.

Tradeoff
Critical Infrastructure Risk Analysis
1. Completeness
Asset
Network

9
Esc

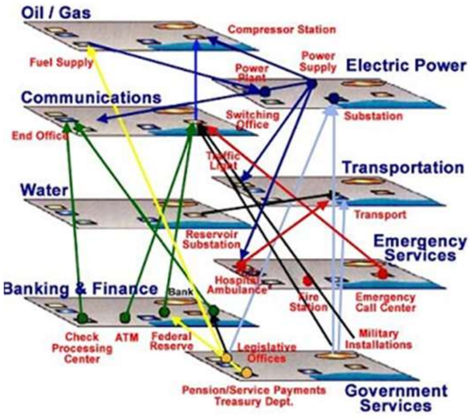
9

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- Many researchers justifiably argue that **risk analysis is incomplete without considering interdependencies**.
- There are at least thirty models specializing in interdependency analysis.
- Interdependency models, though, must be highly detailed to yield reasonable results.

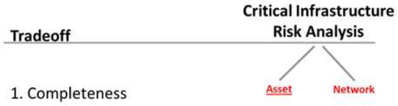


10
Esc

10

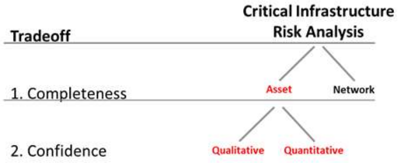
Risk Analysis Methodologies

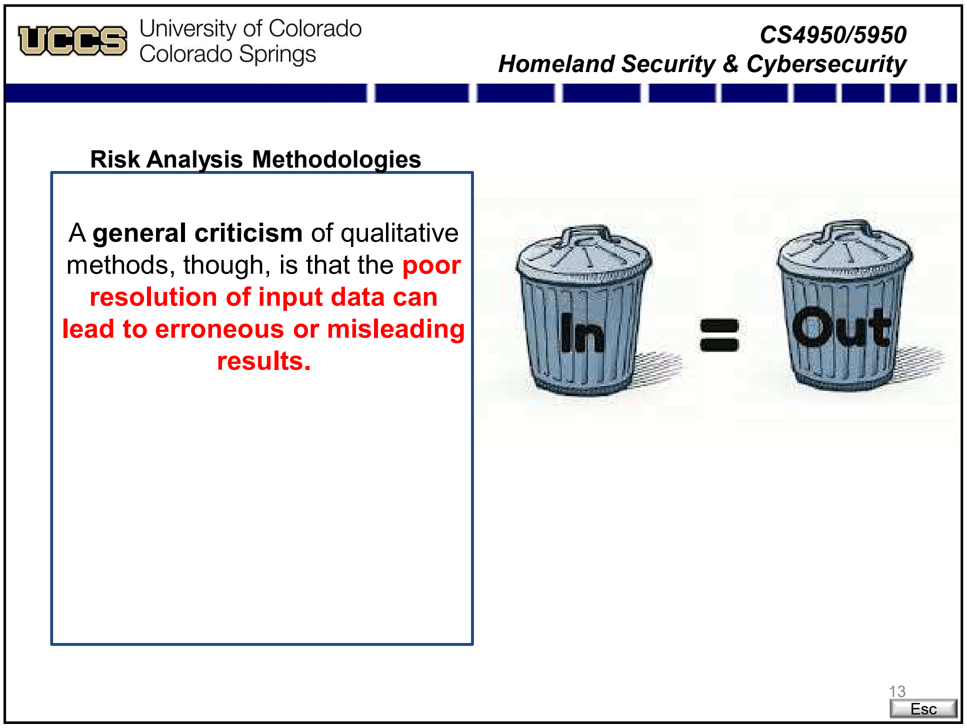
- Since assets are part of the network detail, they must be assessed at some level individually.
- **Thus it is reasonable to begin risk analysis with an asset, but understand the analysis is incomplete without including the network.**
- This was the path chosen by RAMCAP.



Risk Analysis Methodologies

- In analyzing an asset, the next tradeoff is **qualitative versus quantitative risk analysis**.
- **Qualitative risk analysis** simplifies risk assessments by reducing inputs to a manageable set of judgments.
- The Risk and Vulnerability Analysis method employed in Denmark provides one example of a qualitative approach.





University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

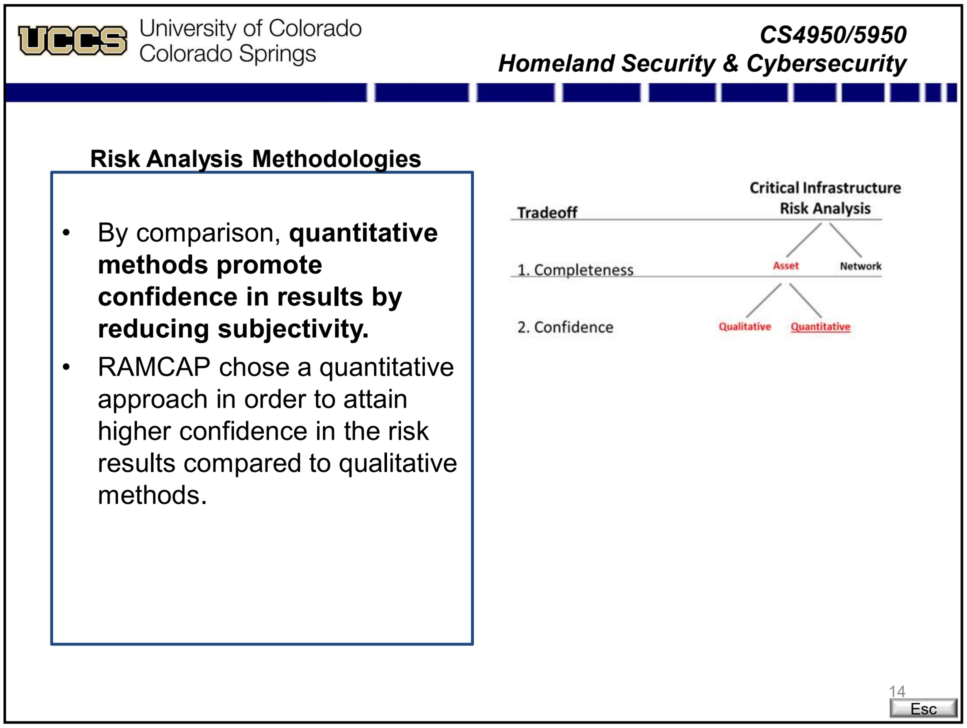
Risk Analysis Methodologies

A **general criticism** of qualitative methods, though, is that the **poor resolution of input data can lead to erroneous or misleading results.**

13

Esc

13



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- By comparison, **quantitative methods promote confidence in results by reducing subjectivity.**
- RAMCAP chose a quantitative approach in order to attain higher confidence in the risk results compared to qualitative methods.

Tradeoff

Critical Infrastructure Risk Analysis

1. Completeness — Asset, Network

2. Confidence — Qualitative, Quantitative

14

Esc

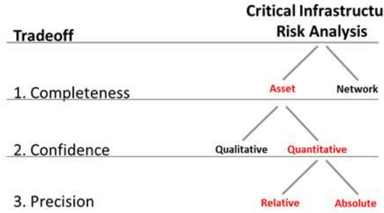
14

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- The quantitative approach, however, is tempered by **precision**.
- Various methods are advocated to achieve a high level of precision in estimating risk, including **Bayesian Networks, Conditional Linear Gaussian Networks, Stochastic Models** and other formal quantitative methods with **proven records of performance in diverse fields of engineering, finance, healthcare, and meteorology.**



Critical Infrastructure Risk Analysis

Tradeoff

1. Completeness — Asset, Network

2. Confidence — Qualitative, Quantitative

3. Precision — Relative, Absolute

15

Esc

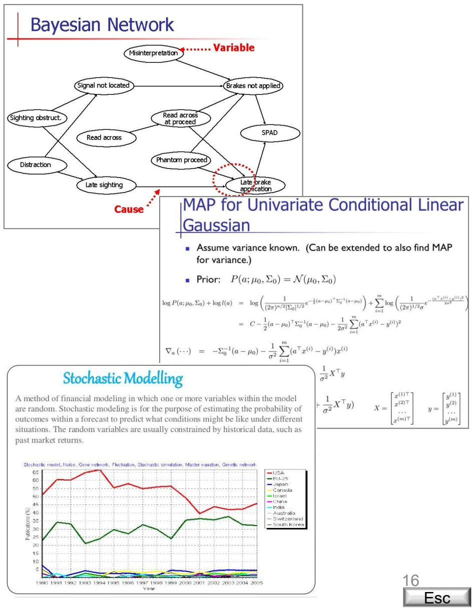
15

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- **What trips up these methods with critical infrastructure** is the **lack of data for statistical analysis** of manmade catastrophic incidents.
- RAMCAP encourages precision at every step in the risk analysis process, but accepts that in the absence of complete data, **precision is an unattainable goal.**



Bayesian Network

MAP for Univariate Conditional Linear Gaussian

- Assume variance known. (Can be extended to also find MAP for variance.)
- Prior: $P(a;\mu_0,\Sigma_0)=\mathcal{N}(\mu_0,\Sigma_0)$

$$\log P(a;\mu_0,\Sigma_0)+\log l(a) = \log\left(\frac{1}{(2\pi)^{n/2}|\Sigma_0|^{1/2}}e^{-\frac{1}{2}(a-\mu_0)^\top\Sigma_0^{-1}(a-\mu_0)}\right)+\sum_{i=1}^{m}\log\left(\frac{1}{(2\pi)^{1/2}\sigma}e^{-\frac{(a^\top x^{(i)}-y^{(i)})^2}{2\sigma^2}}\right)$$

$$= C-\frac{1}{2}(a-\mu_0)^\top\Sigma_0^{-1}(a-\mu_0)-\frac{1}{2\sigma^2}\sum_{i=1}^{m}(a^\top x^{(i)}-y^{(i)})^2$$

$$\nabla_a(\cdots) = -\Sigma_0^{-1}(a-\mu_0)-\frac{1}{\sigma^2}\sum_{i=1}^{m}(a^\top x^{(i)}-y^{(i)})x^{(i)}$$

$$\frac{1}{\sigma^2}X^\top y$$

$$+\frac{1}{\sigma^2}X^\top y) \qquad X=\begin{bmatrix}x^{(1)\top}\\x^{(2)\top}\\\dots\\x^{(m)\top}\end{bmatrix} \qquad y=\begin{bmatrix}y^{(1)}\\y^{(2)}\\\dots\\y^{(m)}\end{bmatrix}$$

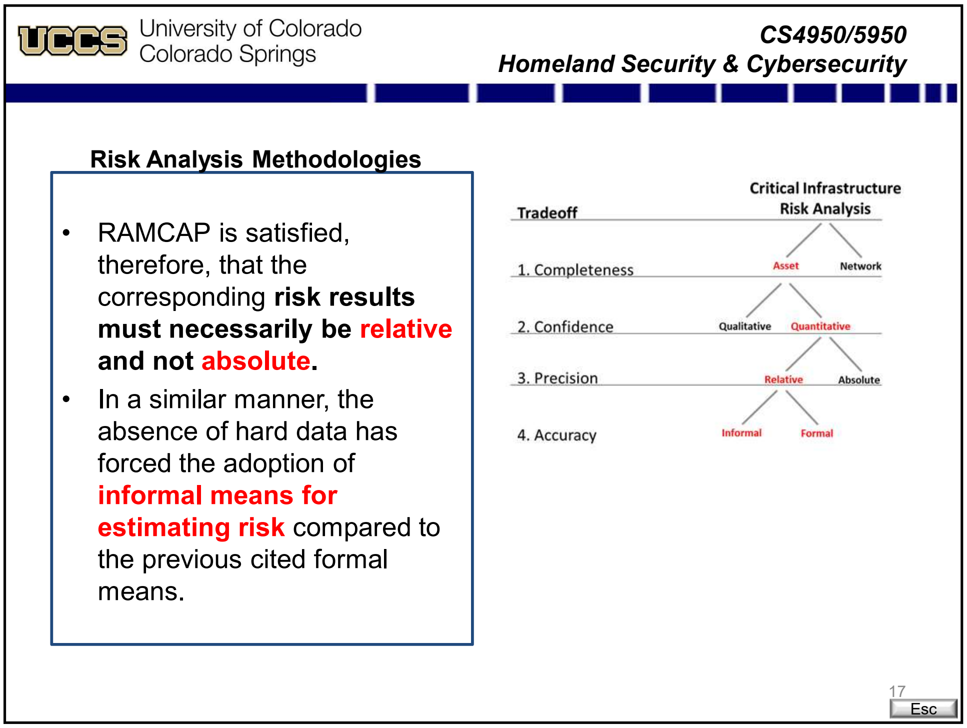
Stochastic Modelling

A method of financial modeling in which one or more variables within the model are random. Stochastic modeling is for the purpose of estimating the probability of outcomes within a forecast to predict what conditions might be like under different situations. The random variables are usually constrained by historical data, such as past market returns.

16

Esc

16



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

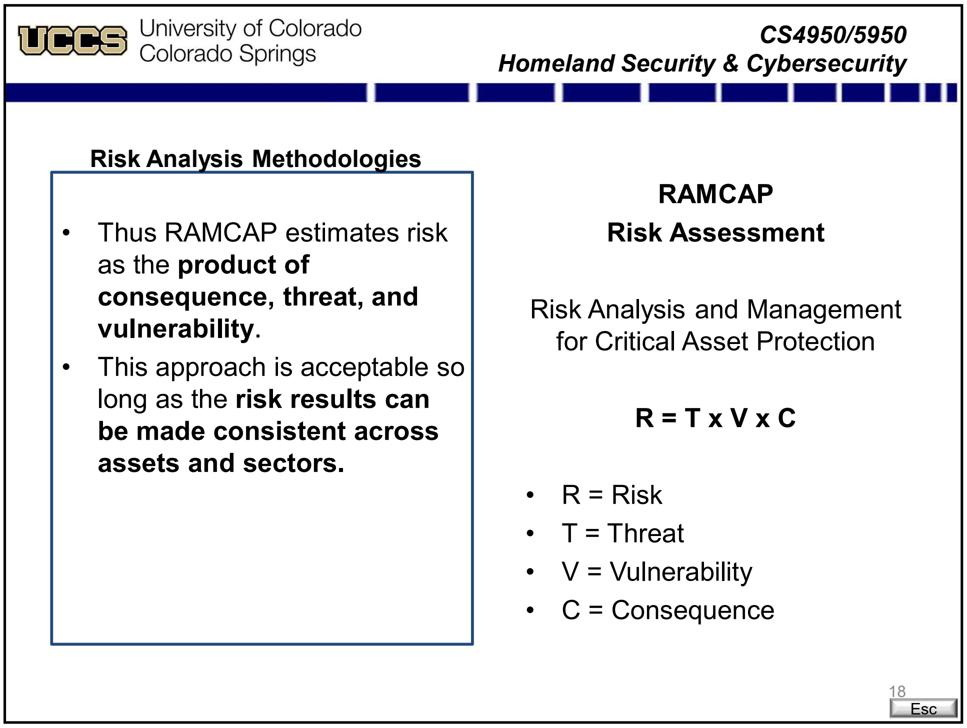
- RAMCAP is satisfied, therefore, that the corresponding **risk results must necessarily be relative and not absolute.**
- In a similar manner, the absence of hard data has forced the adoption of **informal means for estimating risk** compared to the previous cited formal means.

Tradeoff — Critical Infrastructure Risk Analysis

1. Completeness — Asset / Network
2. Confidence — Qualitative / Quantitative
3. Precision — Relative / Absolute
4. Accuracy — Informal / Formal

17
Esc

17



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- Thus RAMCAP estimates risk as the **product of consequence, threat, and vulnerability**.
- This approach is acceptable so long as the **risk results can be made consistent across assets and sectors.**

RAMCAP
Risk Assessment

Risk Analysis and Management for Critical Asset Protection

R = T x V x C

- R = Risk
- T = Threat
- V = Vulnerability
- C = Consequence

18
Esc

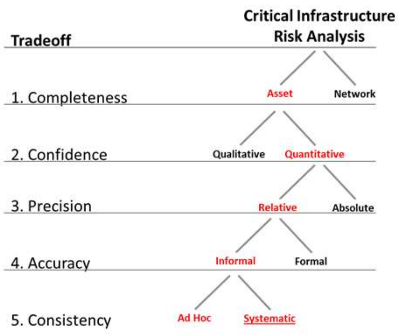
18

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- RAMCAP achieves consistency by systematically applying the same risk formulation across assets and sectors.
- **Consistency** can be further improved by applying **rigorous methods for estimating terms** in the RAMCAP formulation.



19
Esc

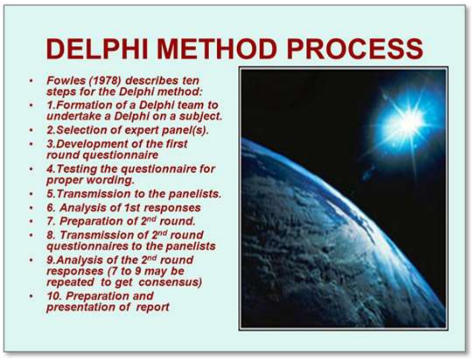
19

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- **Rigorous methods** for estimating consequence, threat, and vulnerability values **encompass various means of elicitation and modeling.**
- The **Delphi Method** is perhaps the best known rigorous system among elicitation methods.

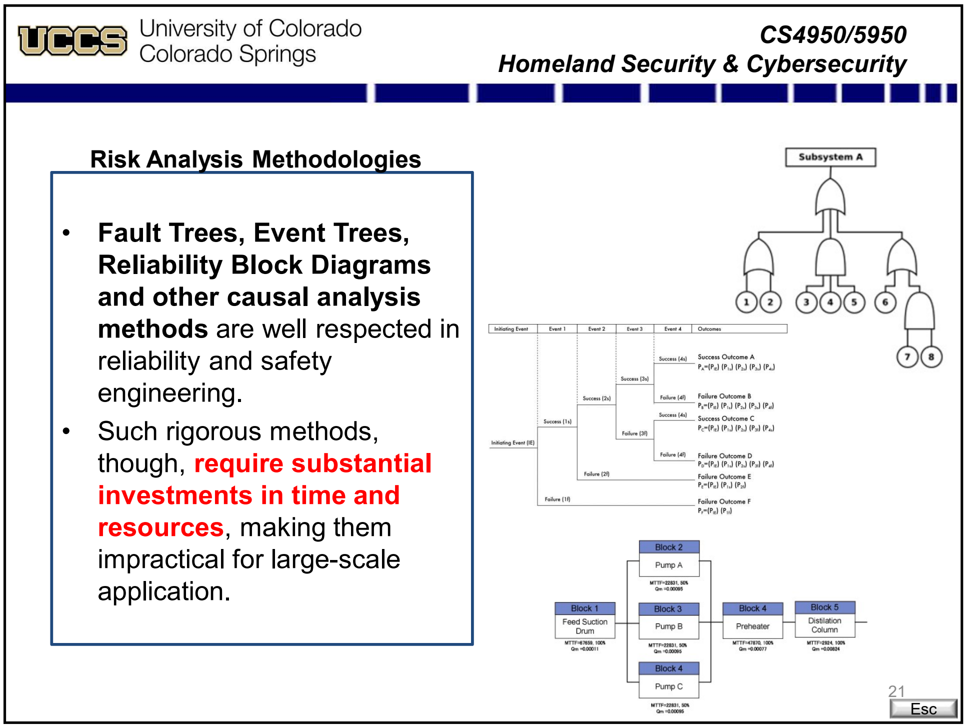


DELPHI METHOD PROCESS

- *Fowles (1978) describes ten steps for the Delphi method:*
- *1.Formation of a Delphi team to undertake a Delphi on a subject.*
- *2.Selection of expert panel(s).*
- *3.Development of the first round questionnaire*
- *4.Testing the questionnaire for proper wording.*
- *5.Transmission to the panelists.*
- *6. Analysis of 1st responses*
- *7. Preparation of 2nd round.*
- *8. Transmission of 2nd round questionnaires to the panelists*
- *9.Analysis of the 2nd round responses (7 to 9 may be repeated to get consensus)*
- *10. Preparation and presentation of report*

20
Esc

20



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

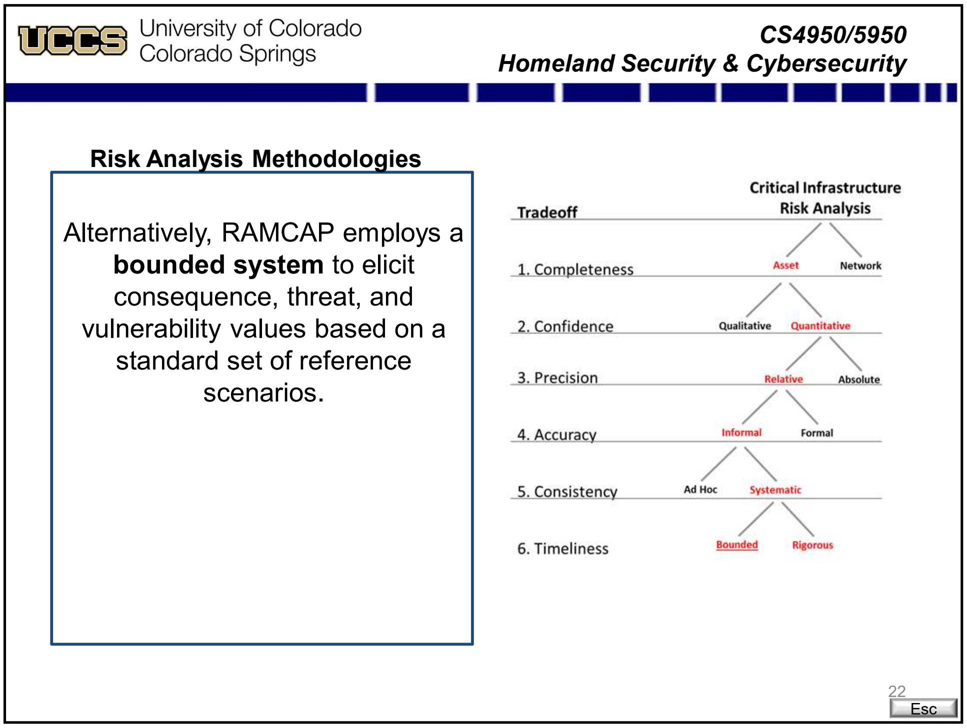
Risk Analysis Methodologies

- **Fault Trees, Event Trees, Reliability Block Diagrams and other causal analysis methods** are well respected in reliability and safety engineering.
- Such rigorous methods, though, **require substantial investments in time and resources**, making them impractical for large-scale application.

21

Esc

21



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

Alternatively, RAMCAP employs a **bounded system** to elicit consequence, threat, and vulnerability values based on a standard set of reference scenarios.

22

Esc

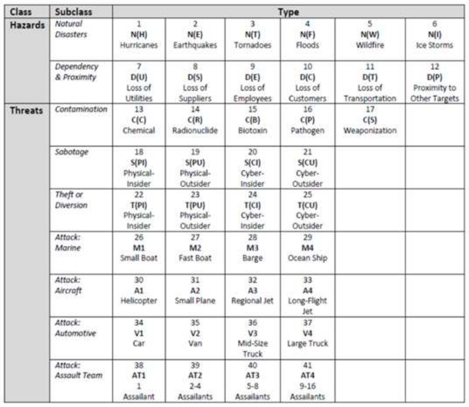
22

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

- These scenarios currently include **forty-one different natural and manmade hazards**.
- Using these same reference scenarios also **promotes interoperability** by facilitating comparison of RAMCAP risk results across infrastructure assets and sectors.



Class	Subclass	Type					
Hazards	*Natural Disasters*	1 **N(H)** Hurricanes	2 **N(E)** Earthquakes	3 **N(T)** Tornadoes	4 **N(F)** Floods	5 **N(W)** Wildfire	6 **N(I)** Ice Storms
	Dependency & Proximity	7 **D(U)** Loss of Utilities	8 **D(S)** Loss of Suppliers	9 **D(E)** Loss of Employees	10 **D(C)** Loss of Customers	11 **D(T)** Loss of Transportation	12 **D(P)** Proximity to Other Targets
Threats	*Contamination*	13 **C(C)** Chemical	14 **C(R)** Radionuclide	15 **C(B)** Biotoxin	16 **C(P)** Pathogen	17 **C(S)** Weaponization	
	Sabotage	18 **S(PI)** Physical-Insider	19 **S(PU)** Physical-Outsider	20 **S(CI)** Cyber-Insider	21 **S(CU)** Cyber-Outsider		
	Theft or Diversion	22 **T(PI)** Physical-Insider	23 **T(PU)** Physical-Outsider	24 **T(CI)** Cyber-Insider	25 **T(CU)** Cyber-Outsider		
	Attack: Marine	26 **M1** Small Boat	27 **M2** Fast Boat	28 **M3** Barge	29 **M4** Ocean Ship		
	Attack: Aircraft	30 **A1** Helicopter	31 **A2** Small Plane	32 **A3** Regional Jet	33 **A4** Long-Flight Jet		
	Attack: Automotive	34 **V1** Car	35 **V2** Van	36 **V3** Mid-Size Truck	37 **V4** Large Truck		
	Attack: Assault Team	38 **AT1** 1 Assailant	39 **AT2** 2-4 Assailants	40 **AT3** 5-8 Assailants	41 **AT4** 9-16 Assailants		

23

Esc

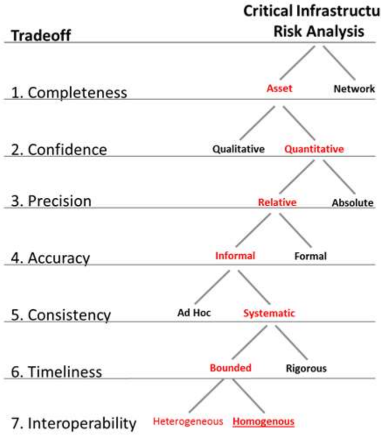
23

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Risk Analysis Methodologies

This ability to compare risk results "apples-to-apples" across assets and sectors perfectly suited the purpose for which **RAMCAP was designed, specifically to make strategic decisions about national investments in critical infrastructure protection.**



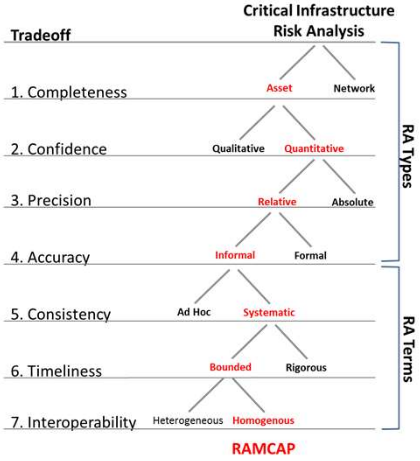
24

Esc

24

Risk Analysis Methodologies

The point of this lesson with respect to cybersecurity is that infrastructure **owners and operators may undergo a similar exercise to develop their own risk analysis methodology that's tailored to their own unique set of circumstance.**



Critical Infrastructure Risk Analysis

Tradeoff

1. Completeness — Asset / Network
2. Confidence — Qualitative / Quantitative
3. Precision — Relative / Absolute
4. Accuracy — Informal / Formal
5. Consistency — Ad Hoc / Systematic
6. Timeliness — Bounded / Rigorous
7. Interoperability — Heterogeneous / Homogenous

RA Types

RA Terms

RAMCAP

Conclusion

Questions?