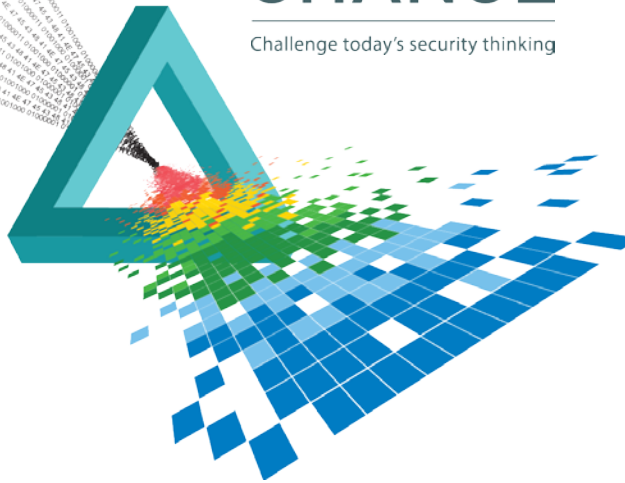
RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

CHANGE
Challenge today's security thinking

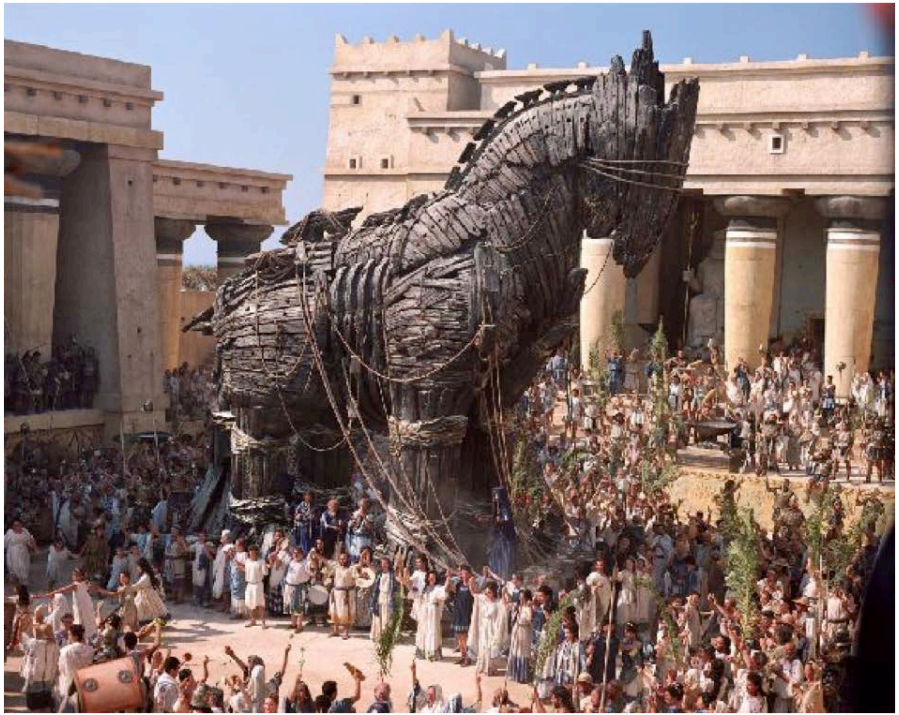


SESSION ID: PST-R05

State of the Art in Strategic Decision-Making Exercises in Cyber Security

Lauri Almann

Member of the Executive Board
Lauri Almann
@LauriAlmann



The Laocoön Dilemma

Decision-making as a Security Risk

- An unknown: the ability to take strategic decisions at the strategic level in cyber crises
- Reasons:
  - The regulatory “comfort zone”
  - The “interface problem”
  - Lack of awareness
- What are the strategic decision-makers **really** worried about?

New Approach in Exercises

- Based on experience in 6 different countries (geographically, politically, etc.) in last 2 years
- Premise of the exercises:
  - Cyber crisis is NOT similar to “any other” crisis
  - Routine drill is NOT a good way to exercise, because there are no routines
  - High stress level does NOT provide good results at the strategic level
  - Secrecy is NOT helpful

Exercise set-up

- Model scenario – key to collecting comparative data
- Ensuring the “flow”
- Covering as wide array of technical risks as possible; “simple” threats as great learning tools
- Present technical options
- Working Groups and issues of cooperation
- **Include private sector**

Substance and Form

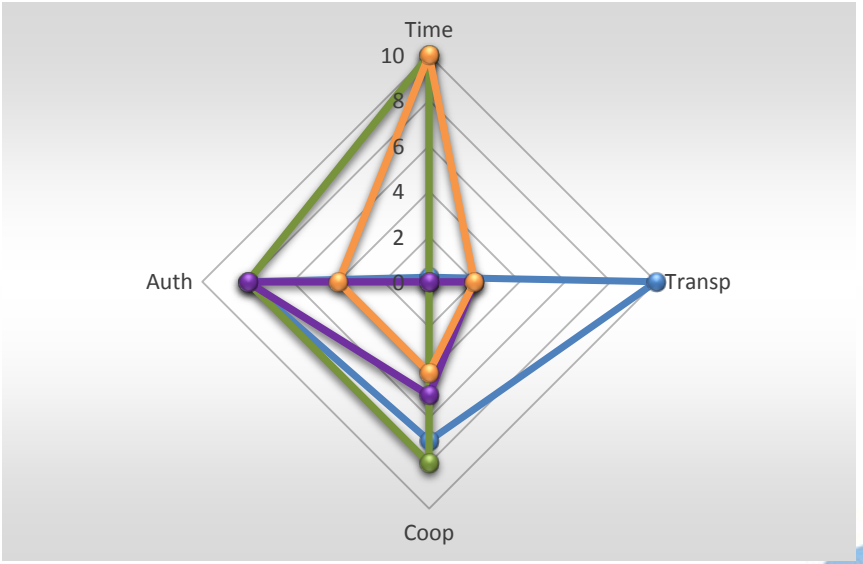
- Substantive questions: Deciding an issue substantively is just a starting point
- Framework questions: Where the problem lies
- Challenge: Mapping the mind of a decision-maker
  - Timeline
  - Transparency
  - Cooperation
  - Authority

“Ransomware”

Substantive Answers

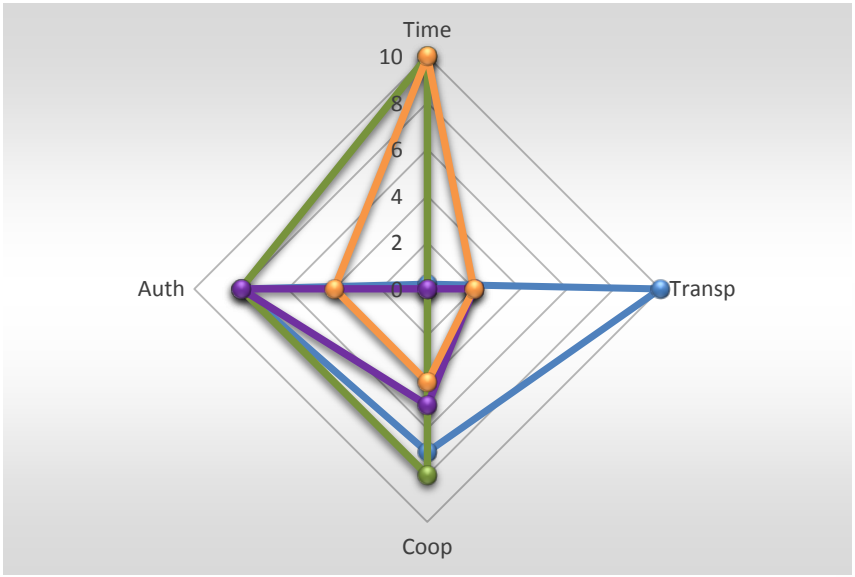
Deciding how to react to the “ransomware” incident. Pay the ransom or not?	
• Government	No
• Military & Intel	No
• Police & Justice	No
• Private Sector	N/A

“The Grid of Disgreements”

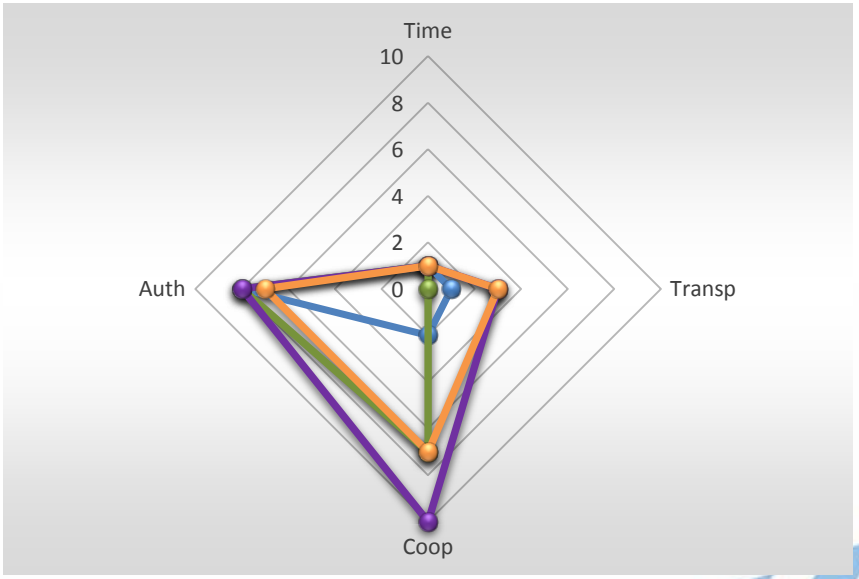


“Ransomware” The Issue of Time.

Country 1

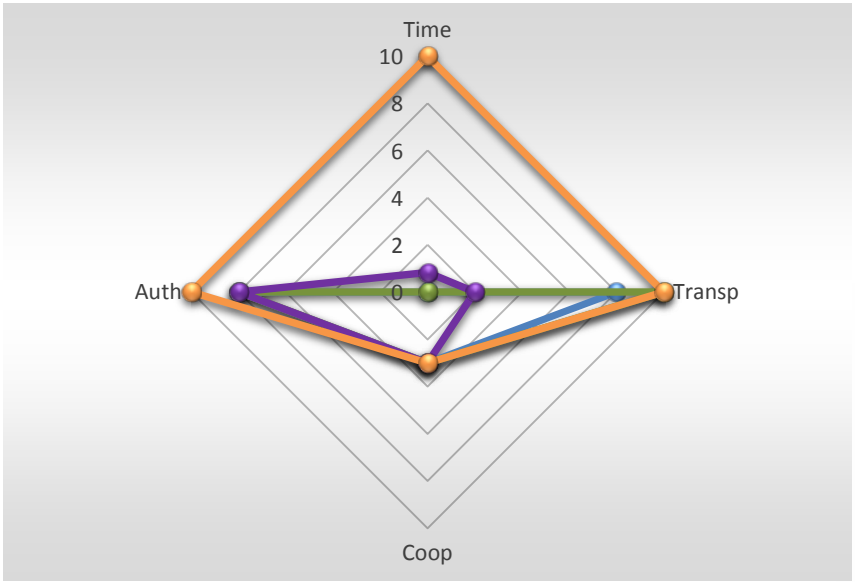


Country 2

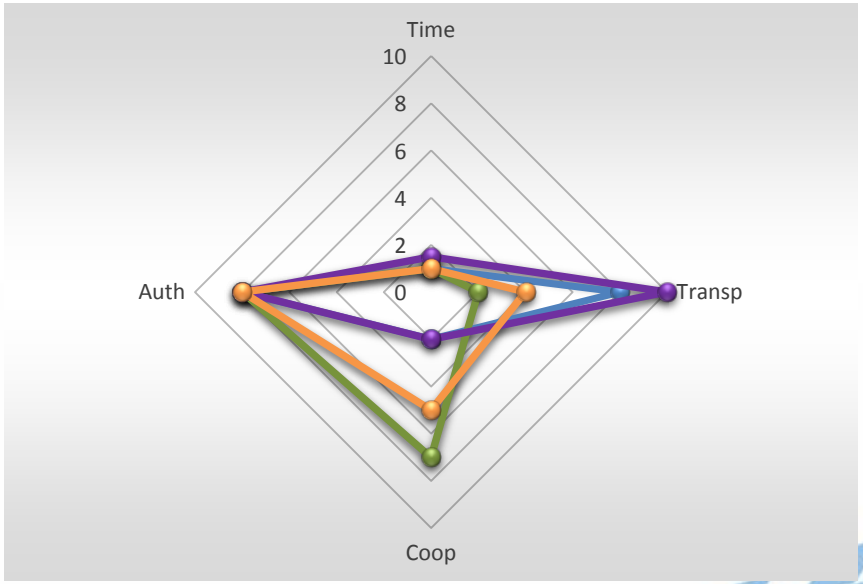


SCADA-Attack. The Issue of Transparency

Country 1

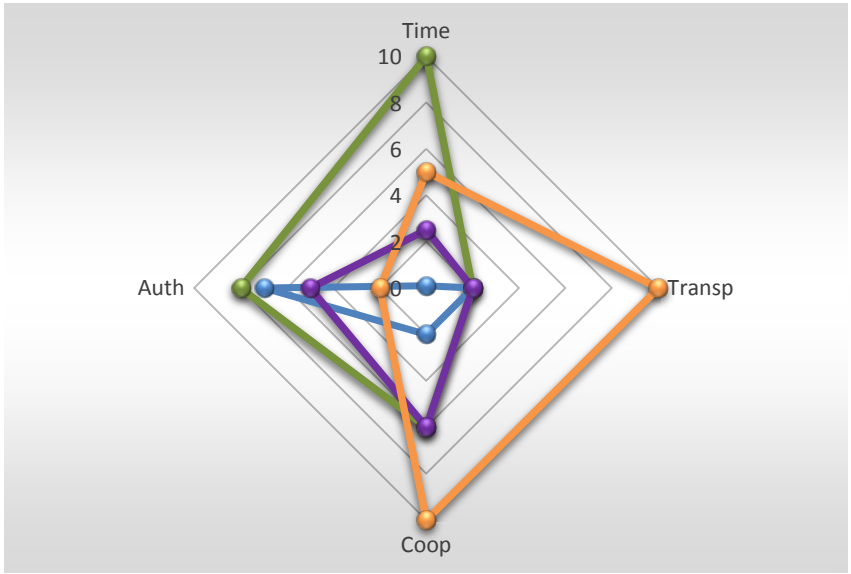


Country 2

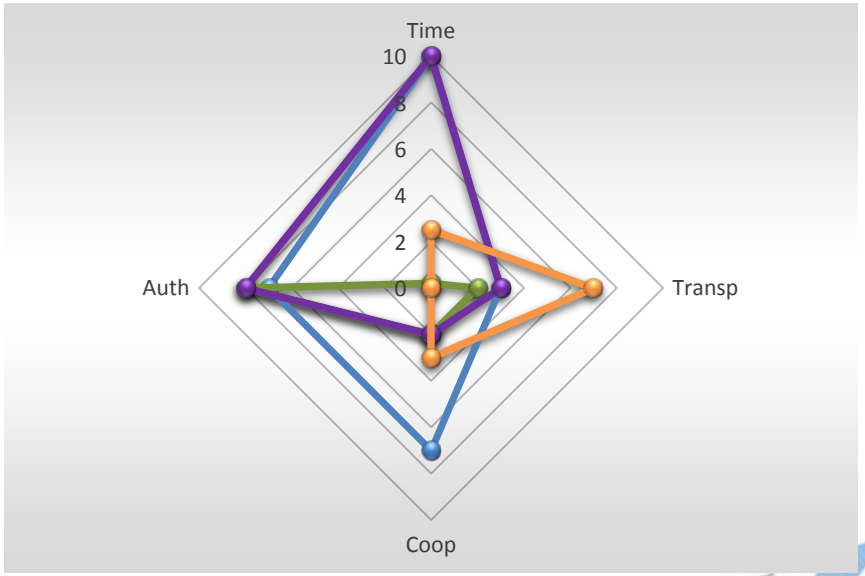


DDoS Attack. The Issue of Cooperation

Country 1

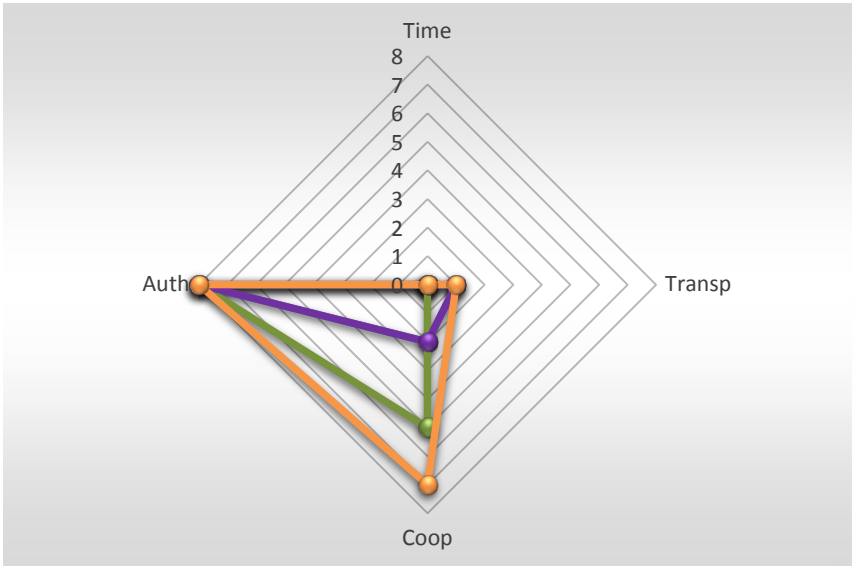


Country 2

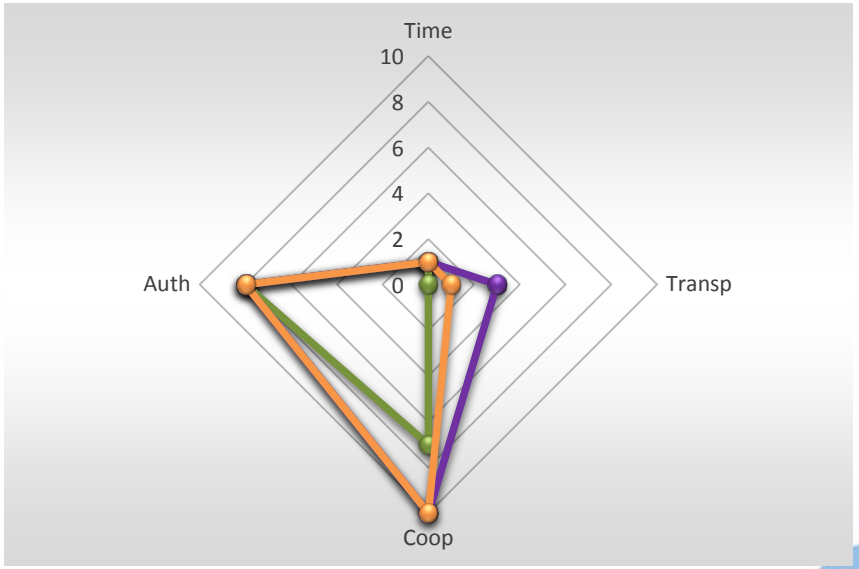


“Hack-back”: The Triangle of Impossibility

Country 1

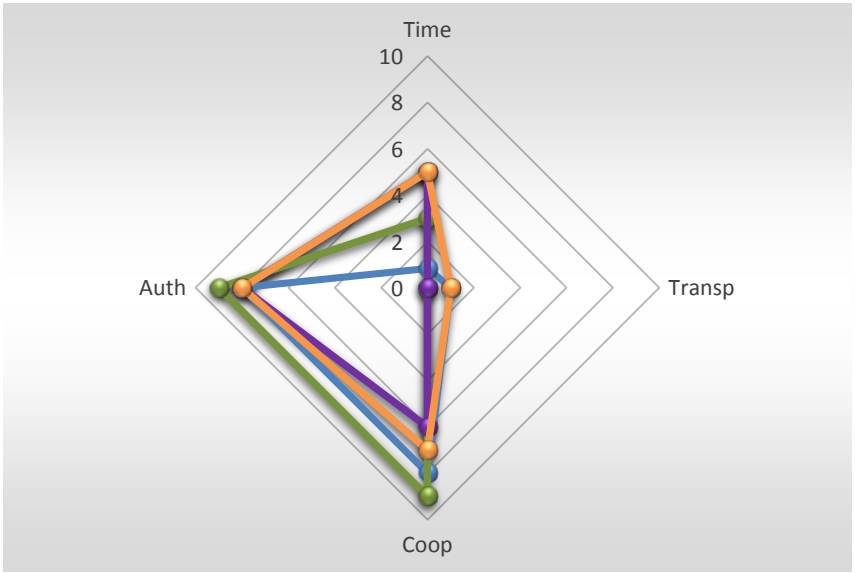


Country 2

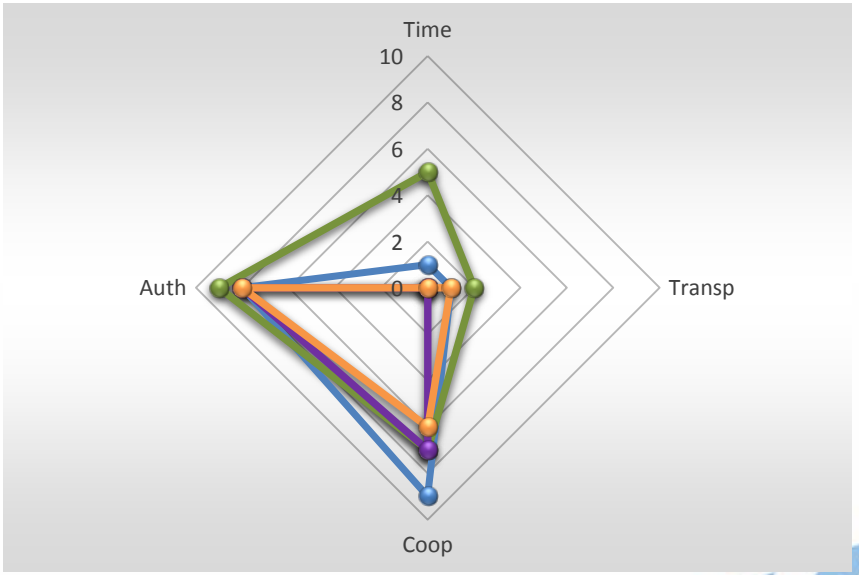


The Hard Questions

Cyber Attack Against a Military Target



Kinetic Attack Against a "Cyber Target"



BHC LABORATORY

Summary

- Universal, “model approach” that has been proven in several countries
- Comparable data that is basis for discussion, improvement and change
- “Why are we doing this?” concern is addressed
- Actual impact to drafting regulations, strategic documents, policy
- Enormous scalability

Apply

- Immediately:
  - Discuss how to apply this in a commercial environment
- 2-5 weeks
  - Try to identify the strategic-level decision-makers in your organization
  - Try to identify the scenarios and threats that the decision-makers should be trained
- 3-4 Months
  - Create a model scenario for your organization
  - Applying the methodology organize an exercise on decision-making

Thank You!
Questions?

Lauri.Almann@bhclab.com