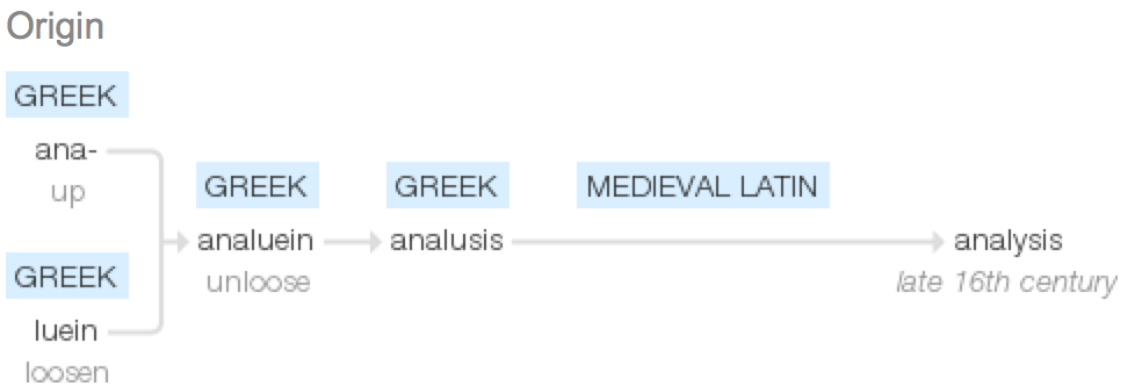
Analysis of Competing Hypotheses

An Analytical Process by former CIA analyst Richards J Heuer, Jr.

What is analysis?



google

- Detailed examination of the elements or structure of something, typically as a basis for discussion or interpretation
- The process of breaking an object down into its constituent parts

Types of Analysis

- Descriptive
  Articulate elements
- Exploratory
  Discover relationships
- Inferential
  Extrapolation of data
- Predictive
  Determine future based on past
- Causal
  Discover relationships between variables
- Mechanistic
  Describe exact relationships of all variables

http://datascientistinsights.com/2013/01/29/six-types-of-analyses-every-data-scientist-should-know/

The Problem of Precision

- CTI analysts have a technical background
- Operate with finite state machines
  - Lend themselves to precise conclusions
  - Mechanistic analysis
- Understanding threats means understanding people
  - People are not stochastic
  - People are not mechanistic
- Understanding people means understanding *motives*

Divergent needs of CTI analysis

Factual Conclusions

(we're good at this)

- Descriptive, Inferential, Mechanistic
- How did intrusion progress (the "what")?
- How does malware operate?
- What conditions determined success or failure?
- Are observations new, or repeated?

Interpretive Conclusions

(we kinda suck at this)

- Exploratory, Predictive, Causal
- Who?
- Why?
- What will precipitate next intrusion?
- How can we change calculus of adversaries?

How We See Hypothesis Formulation and Testing

Factual

1. "Maybe this string is XOR encoded with 0x85"
2. Data is XORed with 0x85
3. Result is a valid, documented data structure (like a file)
4. Proof!

Interpretive

1. THE CHINESE DID IT! I mean, uh, maybe the Chinese did it?
2. ????
3. Publish a report
4. Profit! I mean, uh, Proof!

Our domain lacks discipline in analysis where our hypotheses are not deterministically and immediately testable

ACH: (another) "borrowed" model to aid CTI analysts

- Many CTI models are borrowed from parallel domains
  - Kill Chain from military
  - Courses of Action matrix from military
- Why stop now?
- Classic intelligence analysts have been wrestling with this problem for years…
- Analysis of Competing Hypotheses: how "traditional" intelligence analysts formulate assessments

ACH Process Steps

1. Enumerate
2. Support
3. Compare
4. Refine
5. Prioritize
6. Dependence
7. Report
8. Qualify

1 – Enumerate Hypotheses

Account for all evidence

- Not every hypothesis has to include all evidence

Include others

- Brainstorm
- Seek perspectives

Do not consider feasibility

Include unproven hypotheses

Exclude disproven hypotheses

2 – Support the Hypotheses

- Seek additional evidence
  - Supporting
  - Refuting
- Include as evidence
  - Deductions
  - Assumptions
- Discuss missing evidence

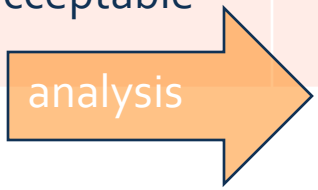
istockphoto.com

3 – Compare the Evidence

Will Iraq Retaliate for US Bombing of Its Intel HQ?

1. No
2. Will sponsor minor terrorist acts
3. Iraq planning major terrorist attack

	H1	H2	H3
E1. Saddam public statement of intent not to retaliate	+	+	+
E2. Absence of terrorist offensive during 1991 Gulf War.	+	+	-
E3. Assumption that Iraq would not want to provoke another US attack	+	+	-
E4. Increase in freq/length of Iraqi agent radio broadcasts	-	+	+
E5. Iraqi embassies told to increase security precautions	-	+	+
E6. Assumption that failure to retaliate would be unacceptable loss of face for Sadaam	--	+	+



4 – Refine the Matrix

Remove non-diagnostic evidence

Add overlooked evidence now applicable

Include formulation of new hypotheses

Document evidence excluded

5 – Prioritize the Hypotheses

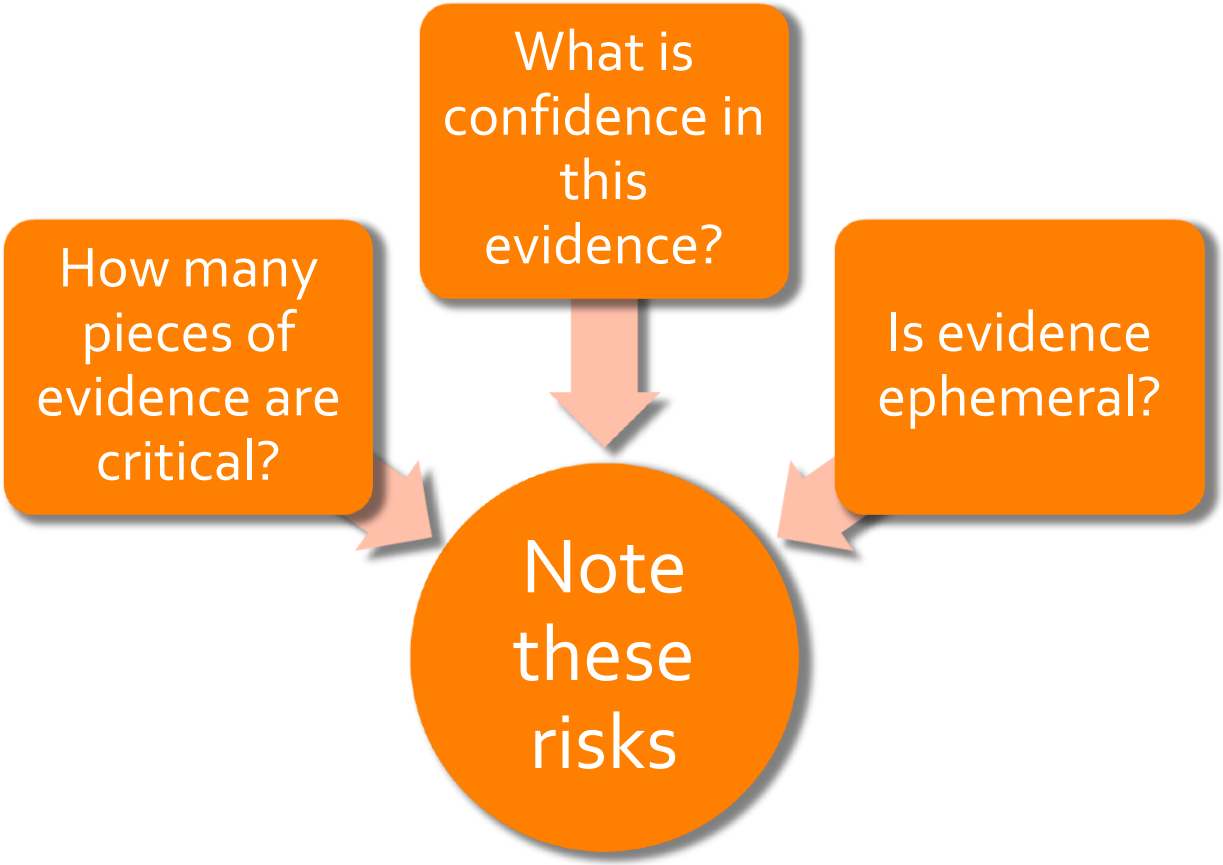
Will Iraq Retaliate for US Bombing of Its Intel HQ?

1. No
2. Will sponsor minor terrorist acts
3. Iraq planning major terrorist attack

analysis

	H1	H2	H3
E1. Saddam public statement of intent not to retaliate	+	+	+
E2. Absence of terrorist offensive during 1991 Gulf War.	+	+	-
E3. Assumption that Iraq would not want to provoke another US attack	+	+	-
E4. Increase in freq/length of Iraqi agent radio broadcasts	-	+	+
E5. Iraqi embassies told to increase security precautions	-	+	+
E6. Assumption that failure to retaliate would be unacceptable loss of face for Sadaam	--	+	+

6 – Determine Evidentiary Dependence



7 – Report Conclusions

Final report

- Hypotheses considered
- Key evidence
- Proper estimative language

Estimative Language

High Confidence

- Supported by preponderance of evidence
- No evidence against
- All but certain

Moderate Confidence

- Significant evidence missing
- New evidence could invalidate

Low Confidence

- Other equally likely hypotheses exist
- Little evidence available to support

8 – Identify Milestones

Analytical conclusions should always be regarded as tentative
-Heuer, p107

- Evidence may change in time
- Changes may affect outcome
- Note circumstances under which evidence may change
- Note how changes would effect conclusions

A Case Study!

Who's ready to play intel analyst?

Thank You!

e: mike@cloppert.org

t: mikecloppert

References

Heuer, Richards J. *Psychology of intelligence analysis*. cia.gov, 1999.