Analytical Methodologies - ACH

Table of Contents

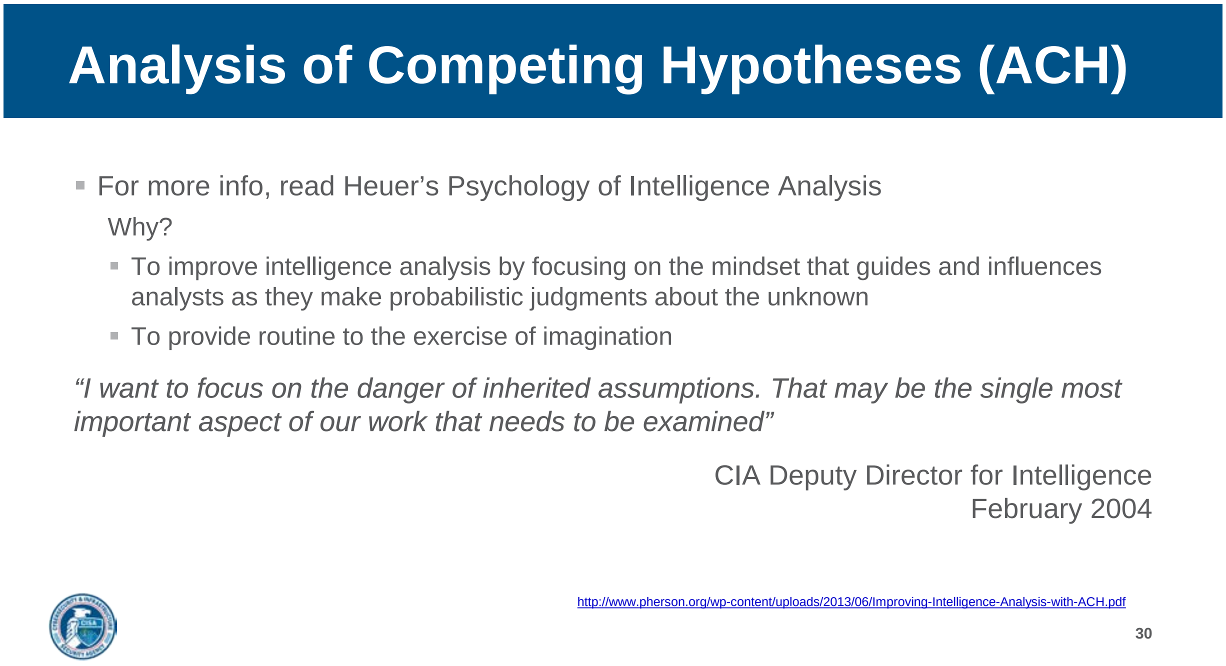
Analytic Methodologies - ACH

Analytic Methodologies - ACH

29

**029 I want to introduce ACH, or the Analysis of Competing Hypotheses, quickly. We will not go in depth right now, but I recommend reading about it later on at another time.

Analysis of Competing Hypotheses (ACH)



Analysis of Competing Hypotheses (ACH)

- For more info, read Heuer’s Psychology of Intelligence Analysis

  Why?

  - To improve intelligence analysis by focusing on the mindset that guides and influences analysts as they make probabilistic judgments about the unknown
  - To provide routine to the exercise of imagination

“I want to focus on the danger of inherited assumptions. That may be the single most important aspect of our work that needs to be examined”

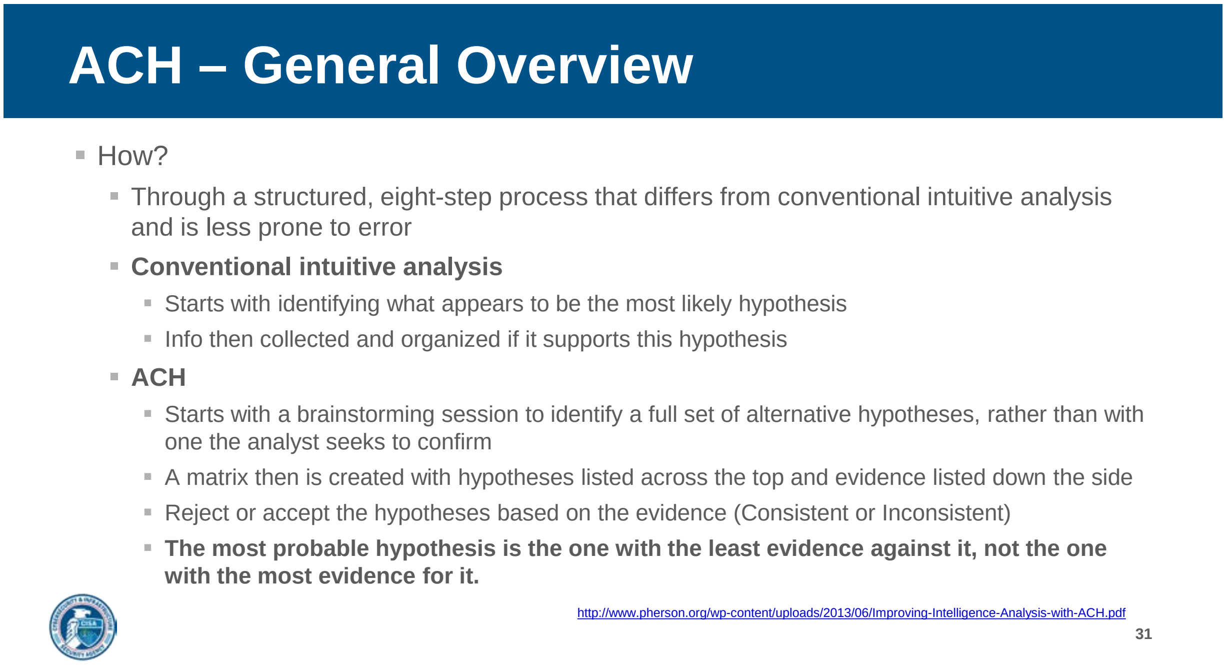
CIA Deputy Director for Intelligence
February 2004

http://www.pherson.org/wp-content/uploads/2013/06/Improving-Intelligence-Analysis-with-ACH.pdf

30

**030 So why would a cyber intelligence use ACH? Well, this is why they would use it and how they would use it. They use it to improve the intelligence analysis by focusing on the mindset that guides and influences analysts as they make probabilistic judgments about something that is unknown. It is good to provide routine exercise for your own specific imagination. So you're trying to think of hypotheses and things that may or may not happen.

ACH – General Overview



ACH – General Overview

- How?
  - Through a structured, eight-step process that differs from conventional intuitive analysis and is less prone to error
  - **Conventional intuitive analysis**
    - Starts with identifying what appears to be the most likely hypothesis
    - Info then collected and organized if it supports this hypothesis
  - **ACH**
    - Starts with a brainstorming session to identify a full set of alternative hypotheses, rather than with one the analyst seeks to confirm
    - A matrix then is created with hypotheses listed across the top and evidence listed down the side
    - Reject or accept the hypotheses based on the evidence (Consistent or Inconsistent)
    - **The most probable hypothesis is the one with the least evidence against it, not the one with the most evidence for it.**

http://www.pherson.org/wp-content/uploads/2013/06/Improving-Intelligence-Analysis-with-ACH.pdf

31

**031 At a very basic level, this is what you do with ACH. Let's say you have a hypothesis that Country X conducted cyberattacks against OPM, or another hypothesis-- whatever it may be-- you have a bunch of hypotheses some country or some hack happened at OPM. Now conventional analysis generally entails looking for evidence to confirm your favorite hypothesis that Country X conducted cyberattacks against OPM. You're looking for all the information to confirm that hypothesis.

The Analysis of Competing Hypotheses takes a different approach. It involves doing something different where you're seeking evidence to refute hypotheses. You're trying to reject hypotheses rather than confirm them.

So generally this is what you do. You start with a brainstorming session to identify a full set of all hypotheses rather than the one the analyst seeks to just confirm and you maybe write those on the top of a spreadsheet, and then you create a matrix on the left-hand side of the spreadsheet. You write down all the evidence that could be used to refute or approve or confirm the hypothesis, and you and your team go through this matrix where, again, you have all the hypotheses listed on the top and the evidence lifted on the left-hand side, and you go through the matrix and you say, "Well this evidence confirms or rejects this hypothesis," and you go through this entire list with your team, and what happens is, for this to work, is the most probable hypothesis for an event is usually the one with the least evidence against it, not the one with the most evidence for it, and that is how the Analysis of Competing Hypotheses works. Again, that is just an overview of it, but you can read more about it.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM20-0262