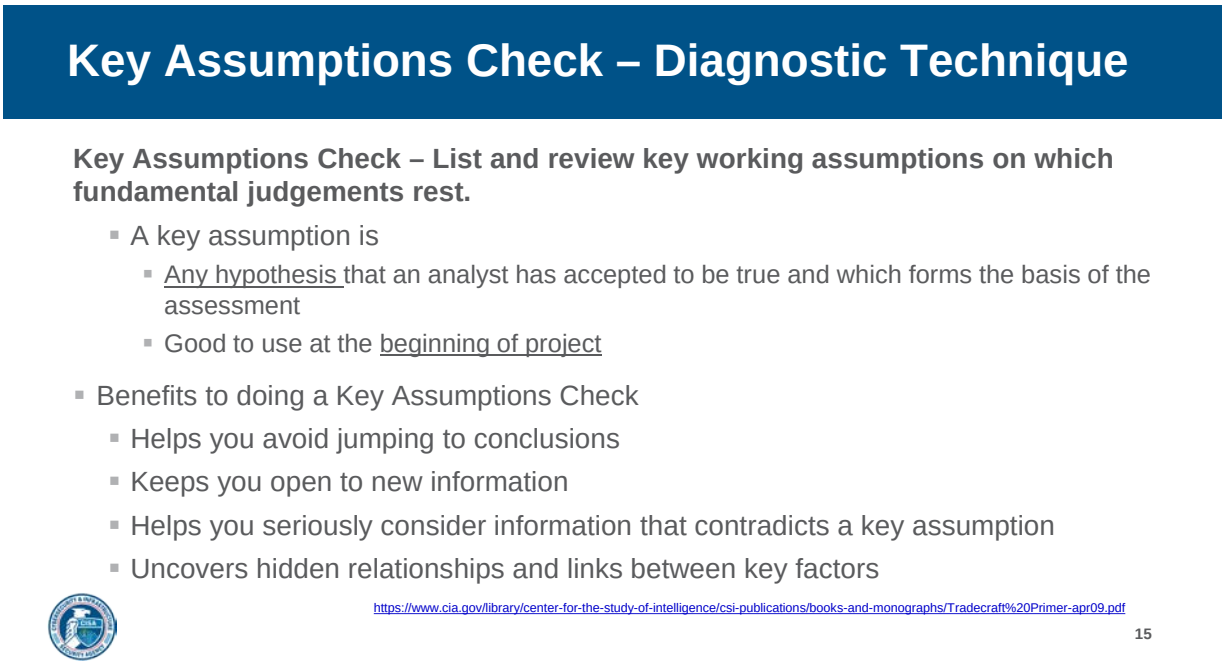
Analytic Methodologies - Diagnostic Technique

Table of Contents

Analytic Methodologies – Diagnostic Technique

**014 Let's look at how to do a key assumptions check, which is a diagnostic technique. Again, diagnostic techniques aim to make analytical judgments, assumptions, or intelligence gaps more transparent.



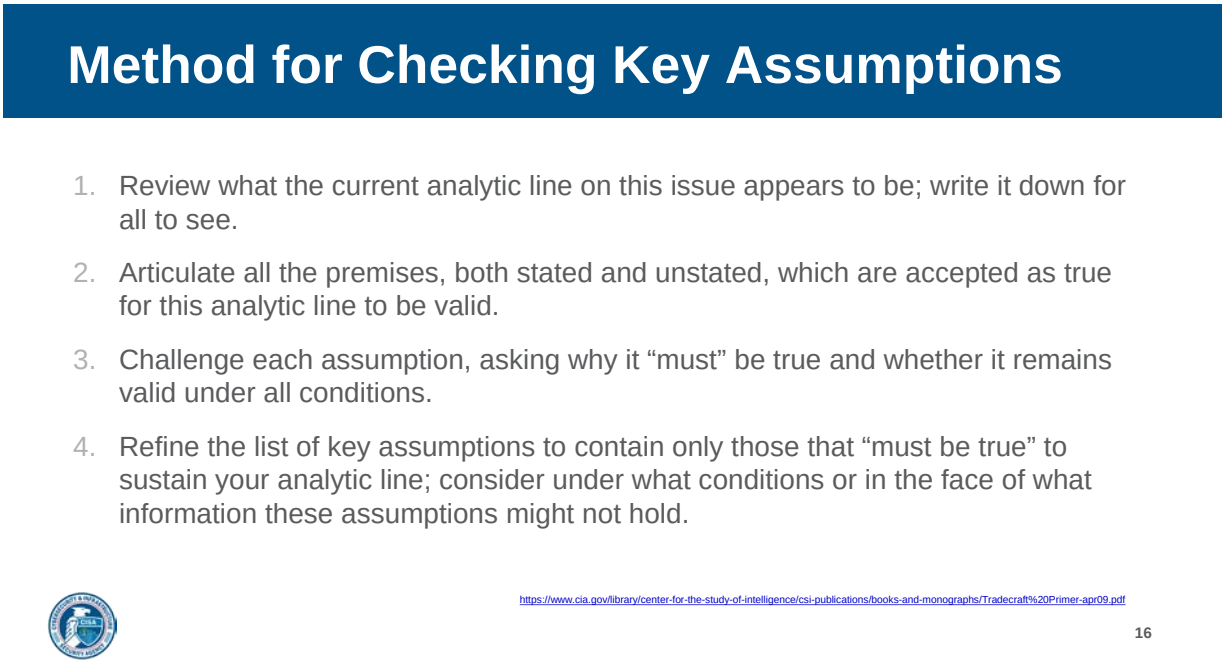
**015 So for a key assumptions check, here you're basically listing and reviewing key working assumptions on which fundamental judgments rest. A key assumption is any hypothesis that an analyst has accepted to be true and which forms the basis of an assessment.

Generally speaking, this technique, as a key assumption check, is a good thing to do at the beginning of a project, and there is value added to doing this. When you are identifying and listing the working assumptions of something, it helps you by explaining the logic of the analytical argument and exposes faulty logic. It helps you avoid jumping to new conclusions. It stimulates thinking about an issue and keeps you open to new information, and it also helps you

uncover hidden relationships and links between key factors.

Lastly, one of the things that a key assumptions check could do is it helps you identify developments that would cause you to abandon an original assumption.

Method for Checking Key Assumptions



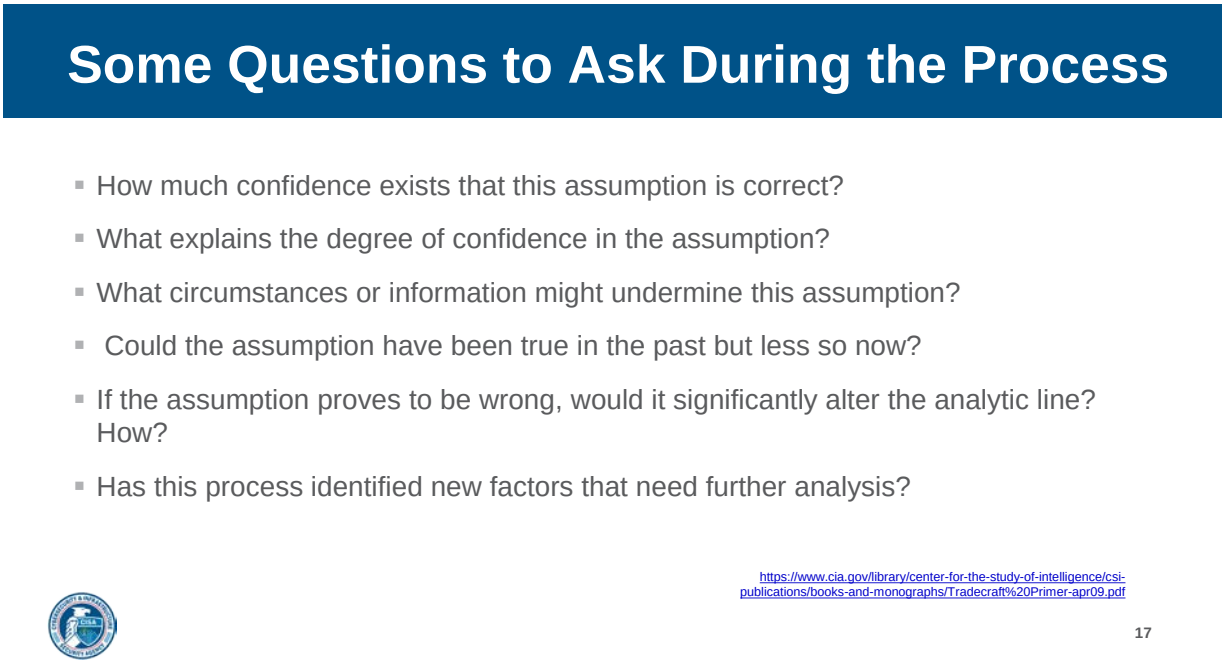
**016 So here is the method for checking key assumptions. The first thing that you're going to do is review the current analytical line on this issue, on what the issue appears to be, and you write it down for everyone to see. The next step is you're going to articulate all premises, both stated and unstated, which are accepted as true for this analytical line to be valid.

The next step is you're going to challenge each assumption.

Specifically you're going to ask, "Why must this assumption be true?" and whether it remains valid under all conditions. So for example, "Why must it be true that this particular threat actor is using these servers and this type of malware?" "Why must it be true that our organization was attacked by a spear-phishing campaign?" "Why must it be an insider threat?"

The next step is to refine the list of key assumptions to contain only those that it must be true to sustain your analytical line.

Some Questions to Ask During the Process



**017 These are some questions that might help you walk through a key assumptions exercise. For example: How much confidence do you have that your assumption is correct? Do you have high

confidence, moderate confidence, or low confidence, and why?

For example, we have high confidence that both foreign actors and domestic actors will attempt to influence the election with disinformation. We have low confidence, however, that nation-states would not attempt to conduct hacks into the election systems themselves due to fear of retribution.

Another question is: What explains the degree of confidence in the assumption? What evidence do you have to support your assumption? What circumstances or information might undermine this assumption? Ask yourself: Could the assumption have been true in the past but is no longer relevant today? Have things changed which make your assumption no longer valid, and are you willing to admit that your original line of assumption is no longer valid based on new information, or are you going to hold the line? If your assumption is wrong, what could have happened, and have any new insights been discovered during this process that could add to your analysis?

So that is basically how a key assumptions check works that you could apply to a situation that you are encountering as a cyber-intelligence analyst.

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.

DM20-0262