

Cognitive Bias and Critical Thinking in Open Source Intelligence (OSINT)

Benjamin Brown

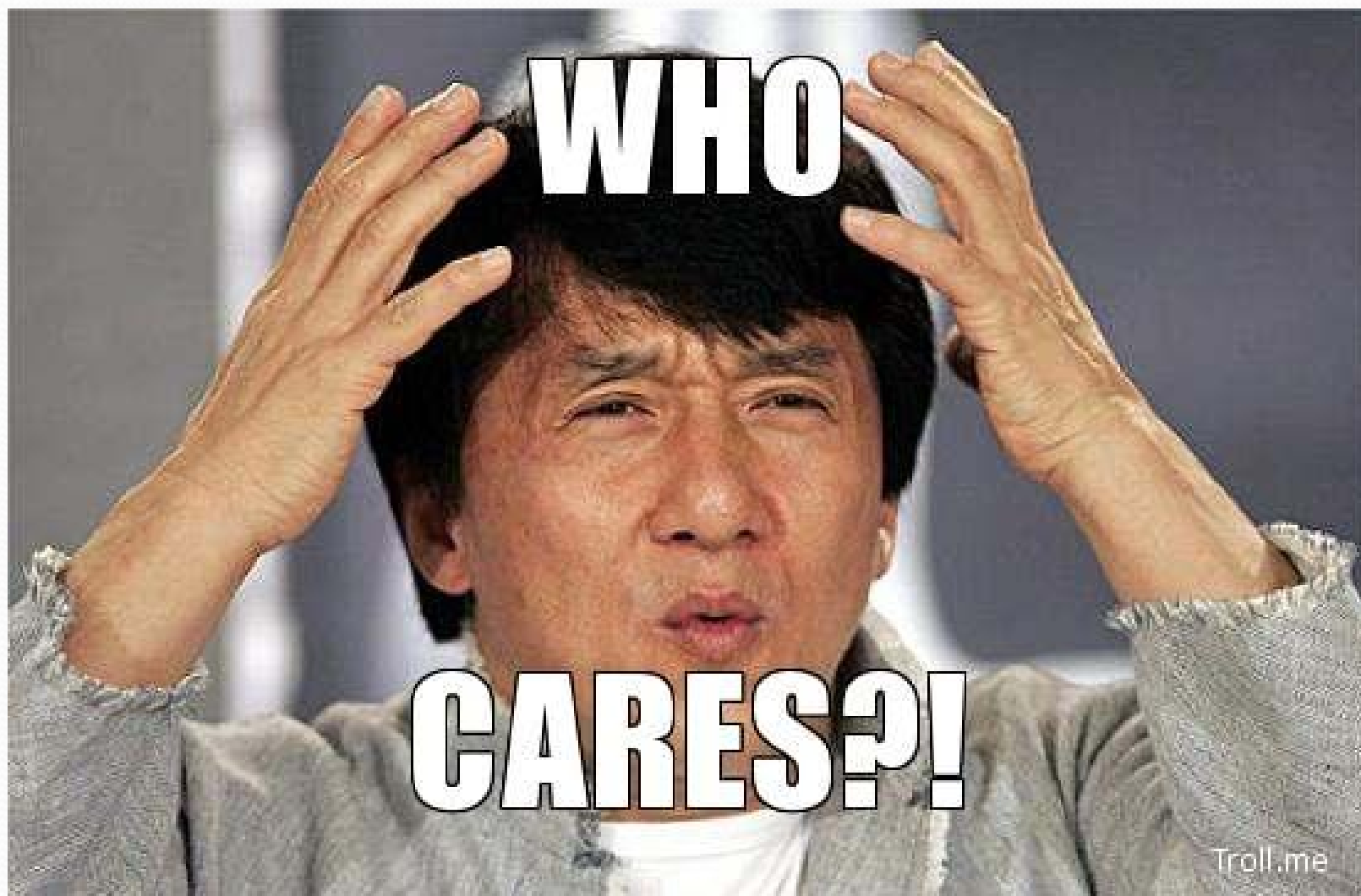
Akamai Technologies

Security Architecture

- * Law Enforcement Engagement**
- * Systems Safety**
- * Threat Intelligence**
- * Security Research**
 - Novel Attack Vectors**
 - Multilayered Attacks**

Coming To Terms

- Cognitive Biases**
- Open Source Intelligence**
- Intelligence Analysis**
- Metacognition**
- Critical Thinking**
- Frameworks for Structured Analysis**



Why We Care

Actionable Intelligence

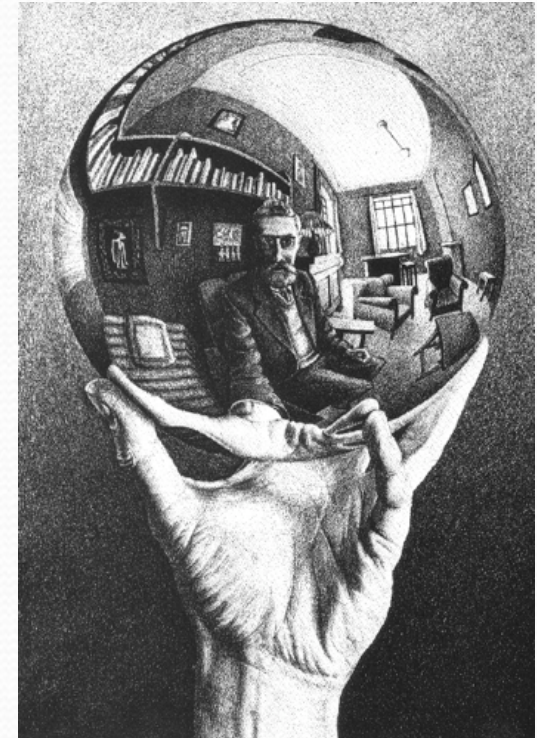
- Accurate conclusions
- Properly framed

Cognitive Biases (faulty heuristics)

- Can lead to inaccurate conclusions

Metacognition and Critical Thinking

- Recognize and correct for cognitive biases
- Arrive at more accurate solutions more often



Why We Care

Bad Data

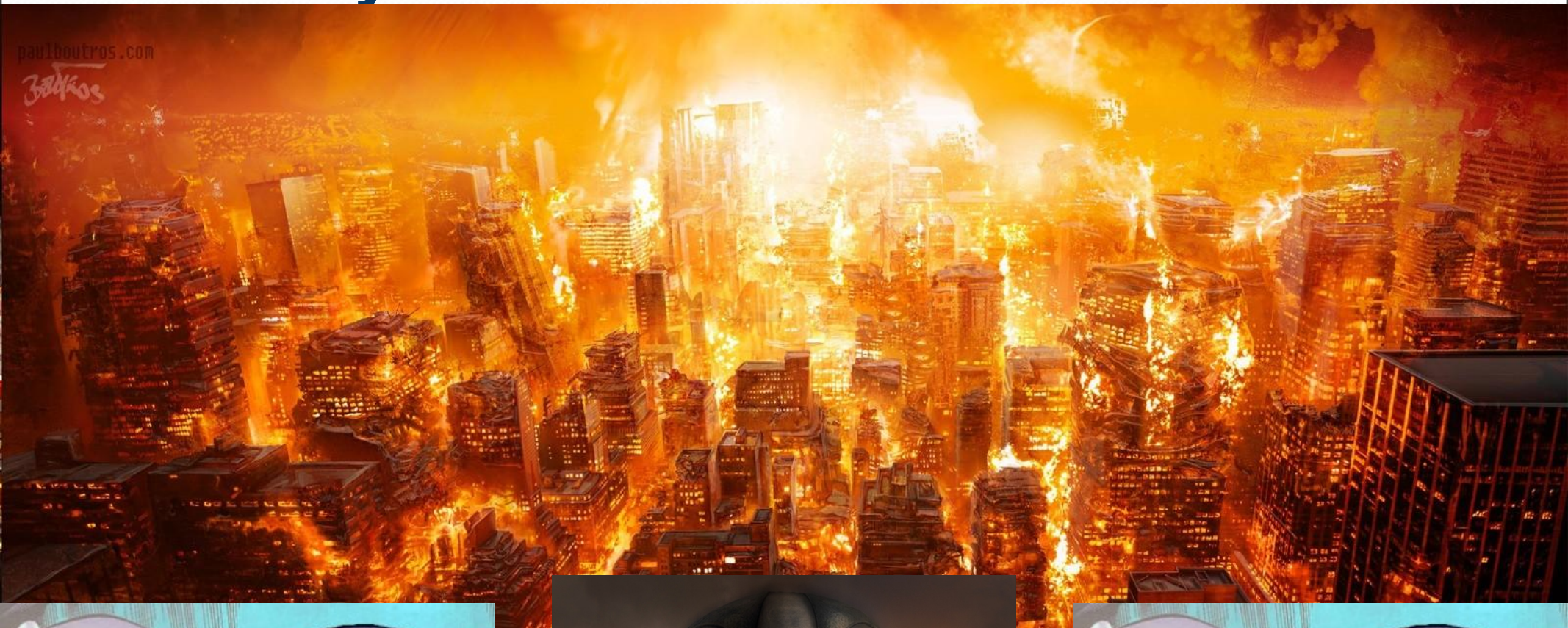
Biased Analysis

```
graph TD; A[Bad Data] --> D[False Conclusions]; B[Biased Analysis] --> D; D --> C[Bad Intelligence];
```

False Conclusions

Bad Intelligence

Why We Care



Open Source Intelligence (OSINT)

Defining OSINT

"Intelligence produced
from publicly available
information"

Defining OSINT

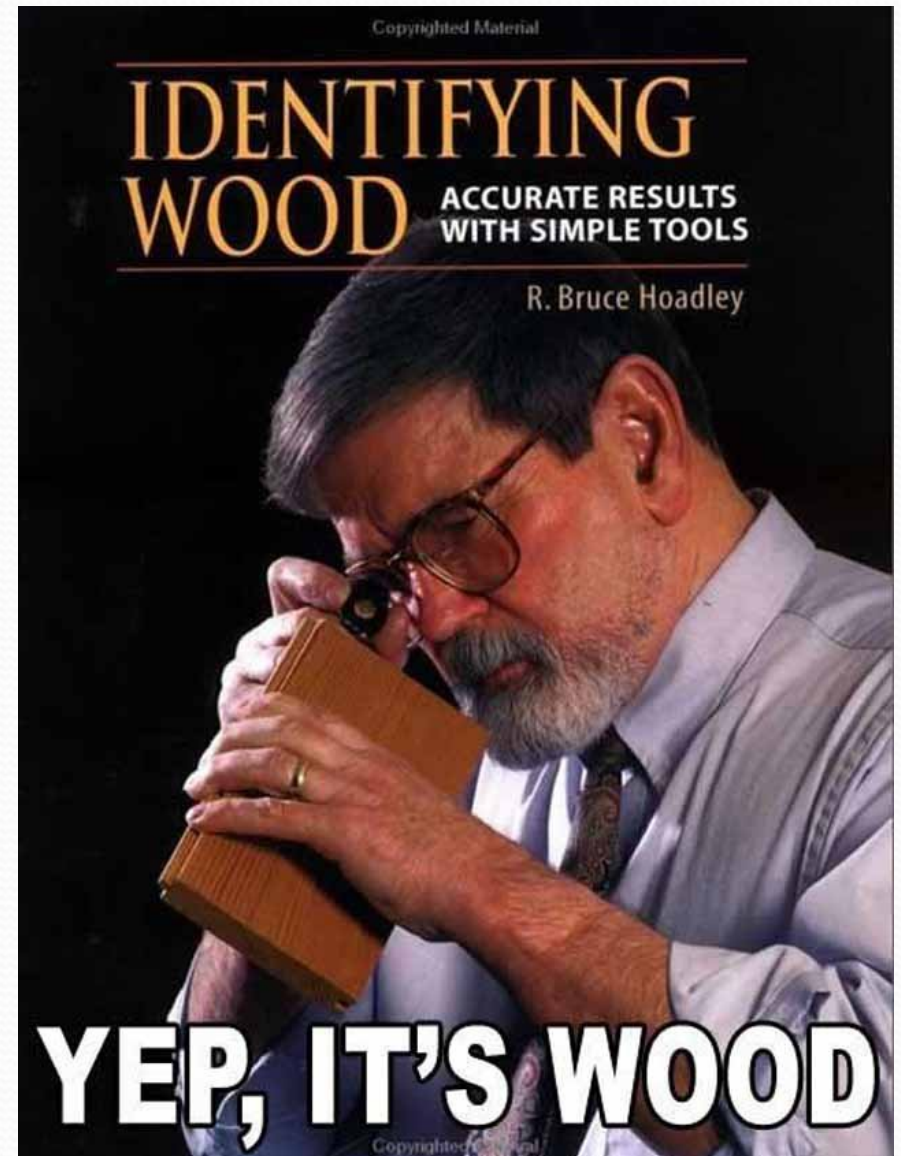
Typical Quality of
Publicly Available Information:



Intelligence vs Information

- Timely
- Relevant
- Actionable

VS



OSINT Sources

- Search engines
- Social networks
- Communication services
- E-commerce site profiles
- Business / tax records
- Media



OSINT Tools

- Recon-ng
- ExifTool
- theHarvester
- Maltego
- Cree.py
- fierce.pl
- TAPIR
- DNSRecon

Defining Cognitive Bias

Defining Cognitive Bias

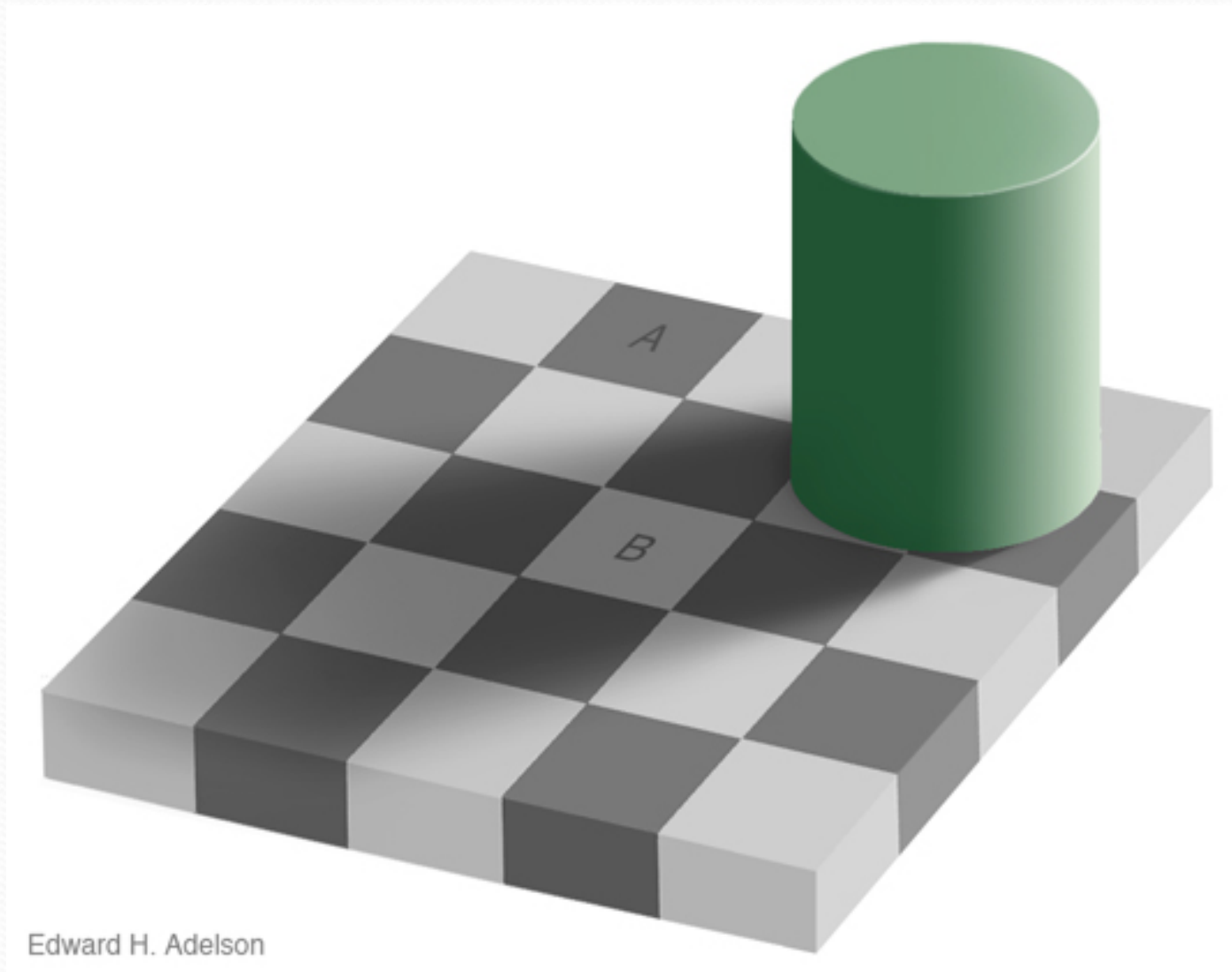
Note: Emotional, intrinsically cultural, spiritual, or faith-based biases are **out of scope.**



Defining Cognitive Bias

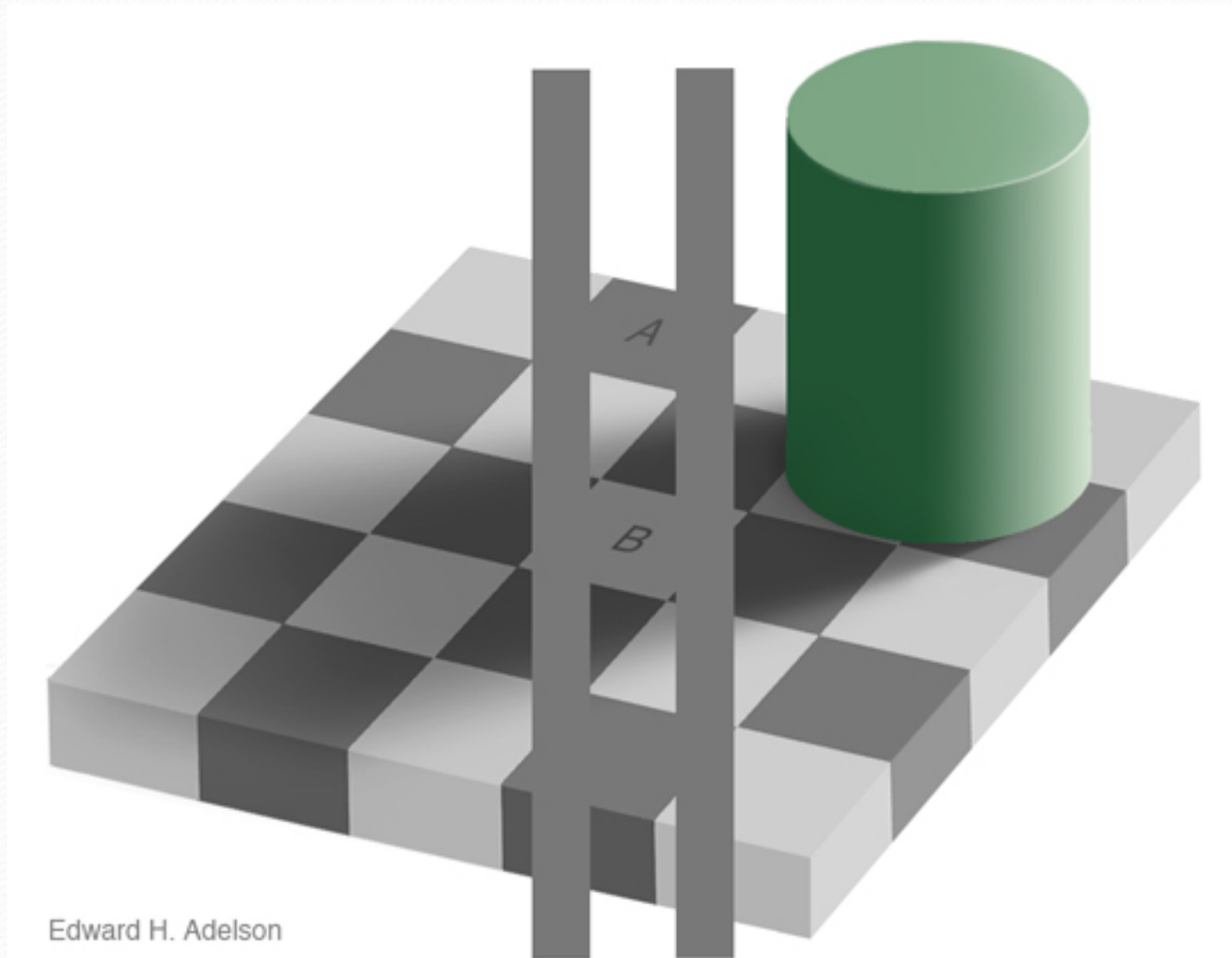
- Patterns of subjective judgment.
- Simplified information processing strategies.
- Subconscious mental procedures for processing information.

Defining Cognitive Bias



‘Deduction’ of color / shade

Defining Cognitive Bias



‘Deduction’ of color / shade

Example Types of Cognitive Bias

Select Biases

Confirmation Bias

- Seek out evidence that confirms
- Self-fulfilling prophecies
- Avoid information supporting competing hypotheses.

Select Biases

Self-serving Bias

- Self-enhancement
- Self-preservation
- Self-esteem
- Social and/or Career Advancement



Select Biases

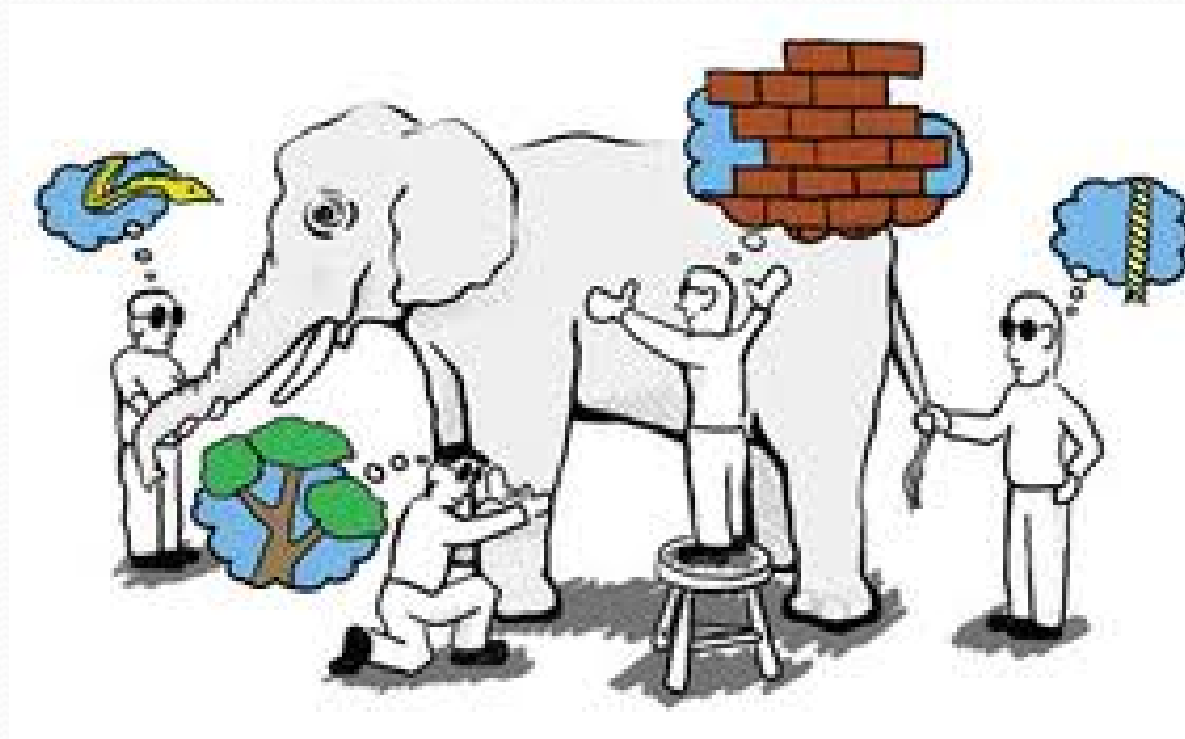
Echo Effect

- Information repeated by source after source.
- * Media telephone
- * Sources obscured
- * Bandwagon effect
- * Promotes group-think

Select Biases

Representativeness

- Focus on similarities / Neglect differences



Select Biases

Representativeness Cont.

- Base Rate Neglect

$$P(A | B) = \frac{P(B | A)P(A)}{P(B)}$$

Select Biases

- Base Rate Neglect Cont.

- * Deadly Disease 'X'
- * Afflicts .01% of Population
- * Cheap diagnostic test that finds the disease in 99.5% of those infected, false-positive rate of only 1.95%

*** Test = Positive (Oh God I'm Dying!
99.5%!!!)**

But Wait There's More

Select Biases

- Base Rate Neglect Cont.

99.5% likely to find it *if* you have it.

- 1.95% false-positive rate
- 1 mill people tested, 100 of which are infected (.01%)
- Test accurately identifies 99 of them as infected
- **BUT** 19,500 uninfected receive a false-positive (1.95%)

Select Biases

Availability Bias

- “Anecdotal” (first or second hand)
- Topic’s trend-power
- Censorship
- Language(s) of collector / analyst
- Маскировка (Maskirovka)

*** Dezinformatsiia**

Synthesis

Reddit vs. Boston Bombers

Reddit Detective Squad



**We're not right,
but we'll ruin your life anyway.**

Reddit vs. Boston Bombers

“Methodology”

- Marathon Photos and Videos
 - * ‘not looking at the race’
- Warped police scanner snippets
- Multiple ‘suspects’
 - * Social media harassment / cyberstalking
- **Media outlets ran bad info from Reddit**

Reddit vs. Boston Bombers



Reddit vs. Boston Bombers

Bias

- Bandwagon effect
- Echo effect
- Availability bias
- Self-serving bias
- Confirmation bias

Attack Attribution - APT

APT: Advanced Persistent Threat
=
OMFGWTFBBQ CHINA!!1one!!



Attack Attribution - APT

“Evidence”

- Type of RAT (Remote Administration Tool)
- Geo Loc of C2s (Command and Control)
- ‘Shared similarities’ with past APTs
- Tool author’s (not user’s) native language
- “We’re expert researchers, just trust us”
(Show me your methodology!)

Attack Attribution - APT

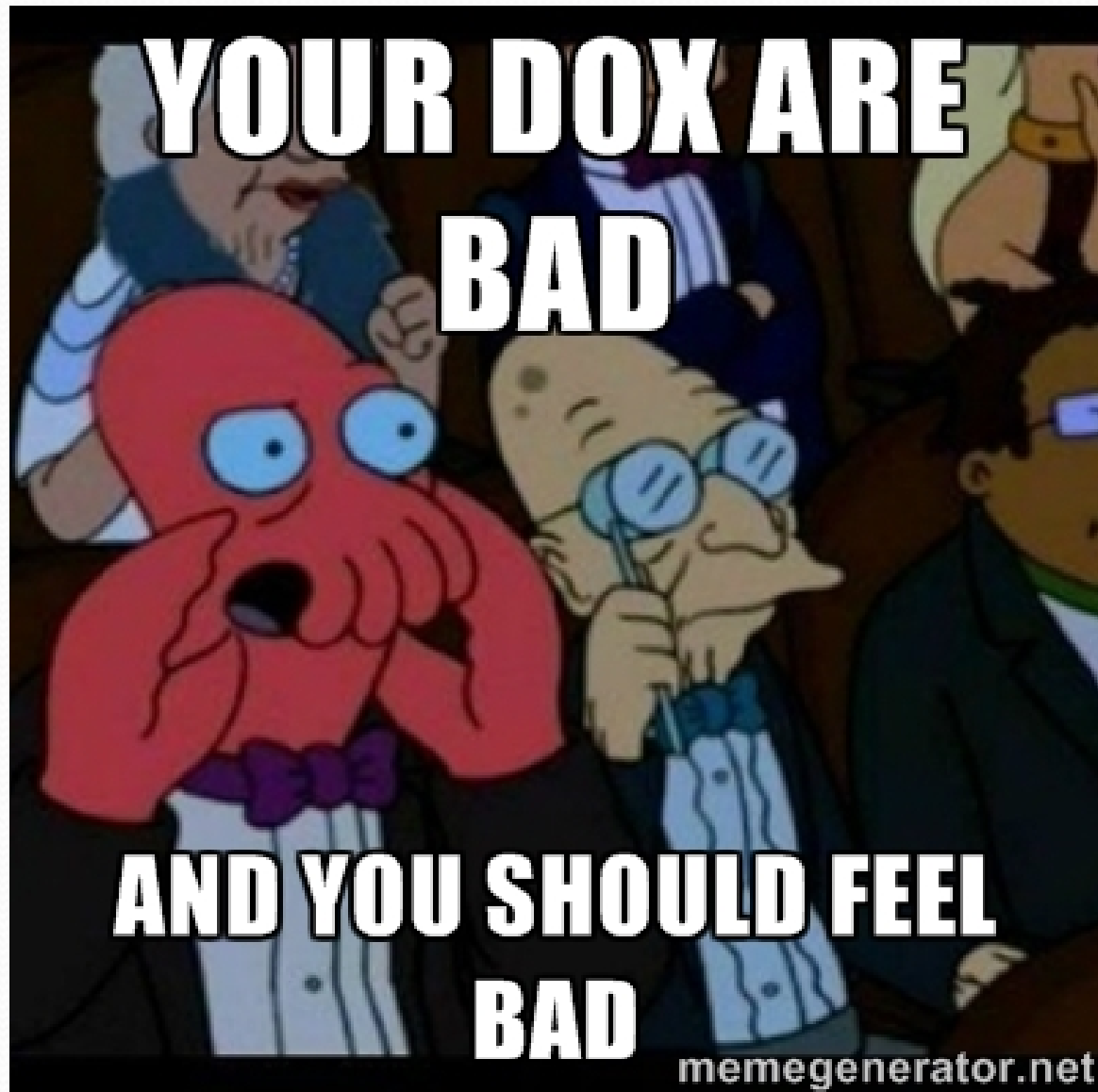
(Vendor) Bias

- Confirmation bias
- Self-serving bias
- Representativeness

* Base rate / Population

- Availability Bias

D0xing



White-Knight Syndrome

- Suspected Amanda Todd bully
- L337 Pro-Scientology hackers:
 - * 59 year-old couple
- LEO in Ferguson not involved
 - * Family info used for ID fraud

DDoS FUD



DDoS FUD

- Statistical methodology
 - * Sample size
 - * Length of collection time
- Availability bias
- Self-serving bias (vendors)

Newsweek vs The 'Creator of Bitcoin'



Malaysia Airways flight MH370 (Google Maps)



Groundwork For Remedy



Defining Metacognition

“Thinking about thinking”

Defining Critical Thinking

- **“What do I think I know?”**
- **“How do I think I know it?”**
- **“When would it not be true?”**

The More You Know

Know about cognitive biases.

- Difficult to affect that which you don't know you don't know.
- Everyone has them, you are not immune or invincible.



The More You Know

[META INTENSIFIES]

**Beware The Bias Bias /
Bias Blind Spot**

- Belief that your bias is actually insight

The More You Know

Dr. Emily Pronin

Princeton University - Dept of Psychology

Subjects:

- Report being less susceptible to bias
- Infer bias in others holding contrary opinions



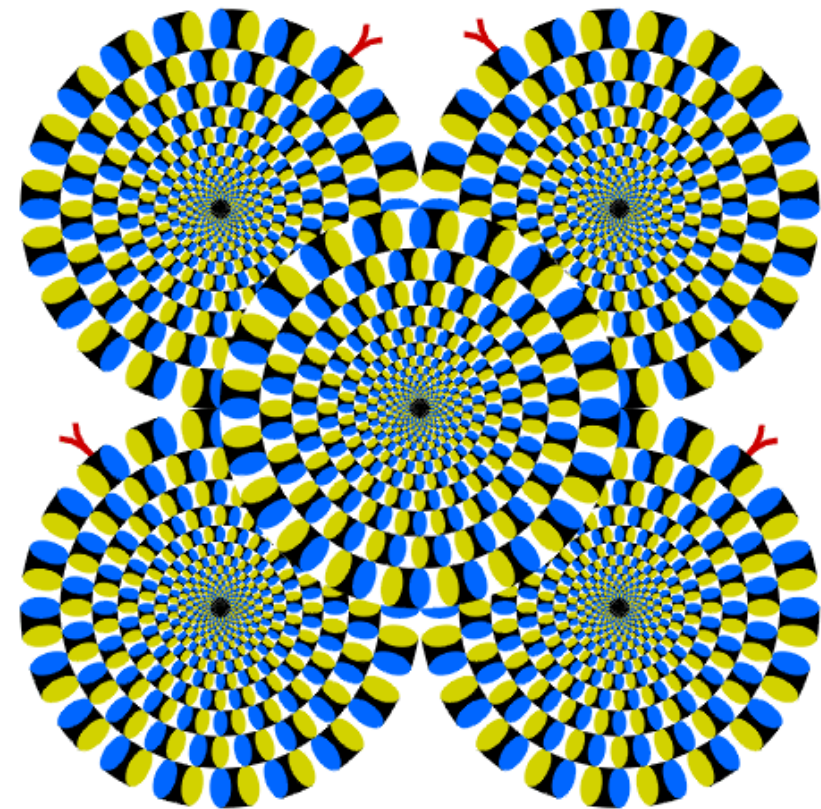
The More You Know

Actively seek out:

- Peer review
- Diverse, outside expertise
- Alternative mindsets

Defining Cognitive Bias

“Similar to optical illusions... [it] remains compelling even when one is fully aware of its nature.”



Two Frameworks

Structures and Frameworks

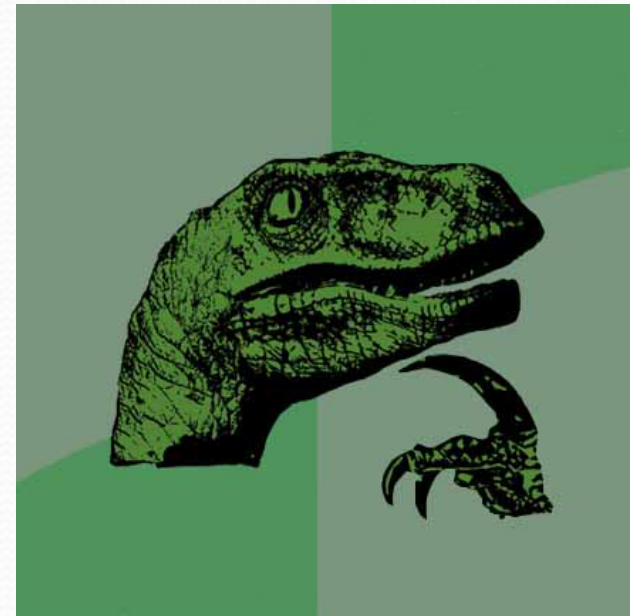
Checklists For Analysts

- Defining the problem
- Generating hypotheses
- Collecting information
- Evaluating hypotheses
- Selecting the most likely hypothesis
- Ongoing monitoring of new information

Structures and Frameworks

Defining The Problem

- Right question
- Framing
- Audience
- Specificity



Structures and Frameworks

Generating Hypotheses

- Identify all plausible hypothesis
- Consult peers and outside experts
- Do not yet screen out or reject
- Consider actor deception or denial

Structures and Frameworks

Collecting Information

- Don't just focus on likely hypothesis
- Suspend judgement
- Notice /note info gaps



Structures and Frameworks

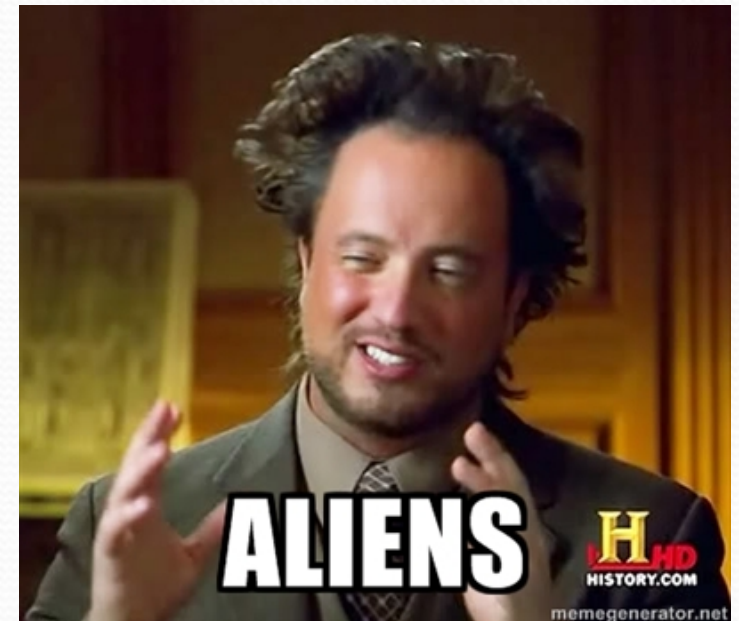
Evaluating Hypotheses

- Develop arguments *against* each hypothesis
- Check assumptions and their origins
- Implement ACH frameworks
(Analysis of Competing Hypothesis)

Structures and Frameworks

Selecting Most Likely Hypothesis

- **Least** evidence against
- **Reject** don't confirm
- Note alternate hypotheses



Structures and Frameworks

Ongoing Monitoring

- Add data sources
- Plug-in alternate hypotheses
- Keep conclusions tentative

Structured Analytic Techniques for Improving Intelligence Analysis

Structures and Frameworks

Structured Analytic Techniques for Improving Intelligence Analysis

- Diagnostic Techniques
- Contrarian Techniques
- Imaginative Thinking Techniques

Structures and Frameworks

Diagnostic Techniques

- Key Assumptions Check

 - *“What do we think we know? How do we think we know it?”

- Quality of Information Check

- Indicators or Signposts of Change

- Analysis of Competing Hypotheses

Structures and Frameworks

Contrarian Techniques

- Devil's Advocacy
- Team A / Team B
- High-Impact /
Low-Probability
- “What If?” Analysis



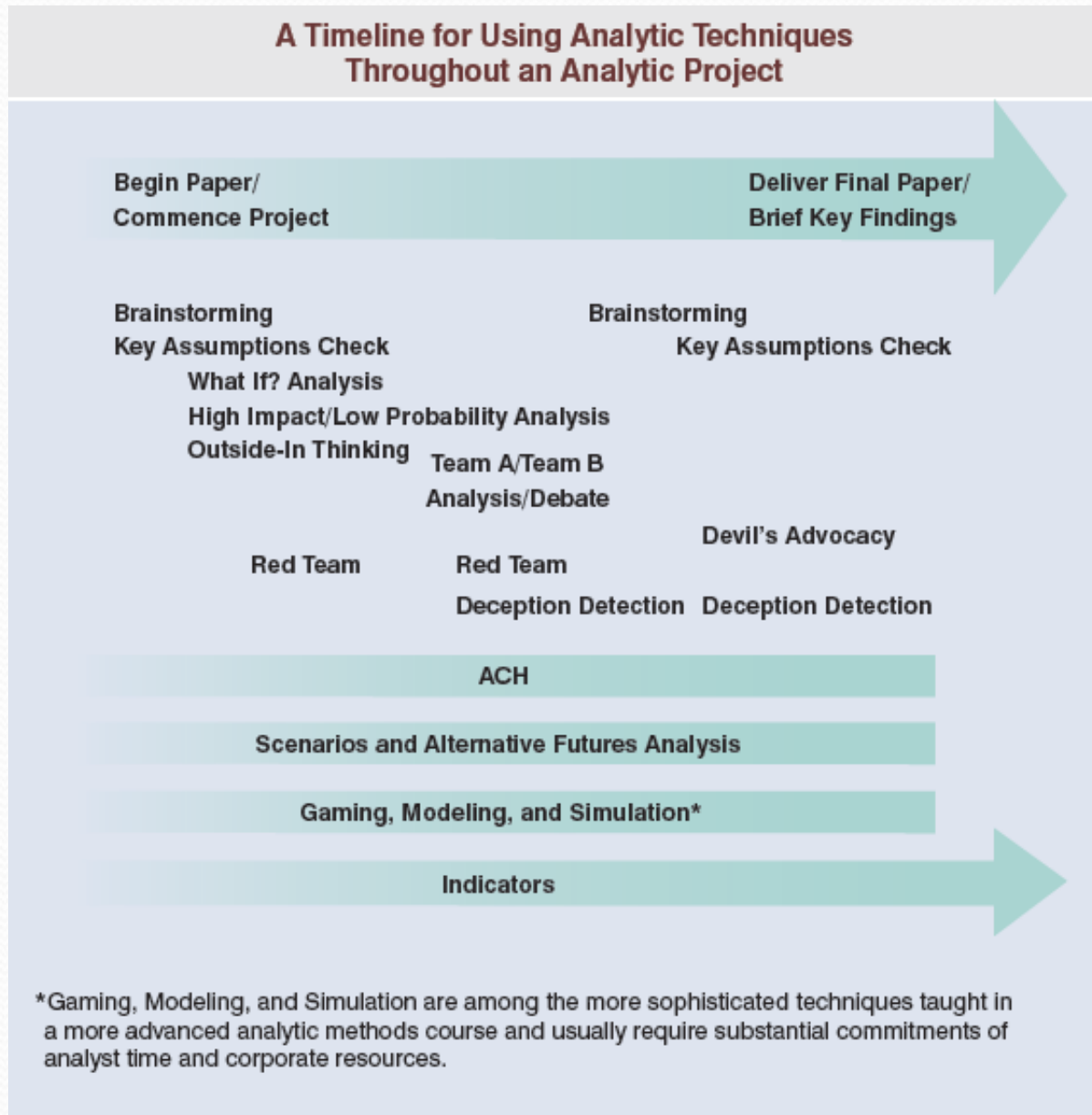
Structures and Frameworks

Imaginative Thinking Techniques

- Brainstorming
- Outside-In Thinking
- Red Team Analysis
- Alternative Futures Analysis



Structures and Frameworks



Application

Application - Report

- Clearly Define
 - * Goals
 - * Sources
 - * Audience
 - * Limitations & Assumptions
 - ...



Application

METHODOLOGY

Verizon, Trend Micro, Prolexic, Recorded Future

Further Research

Further Research

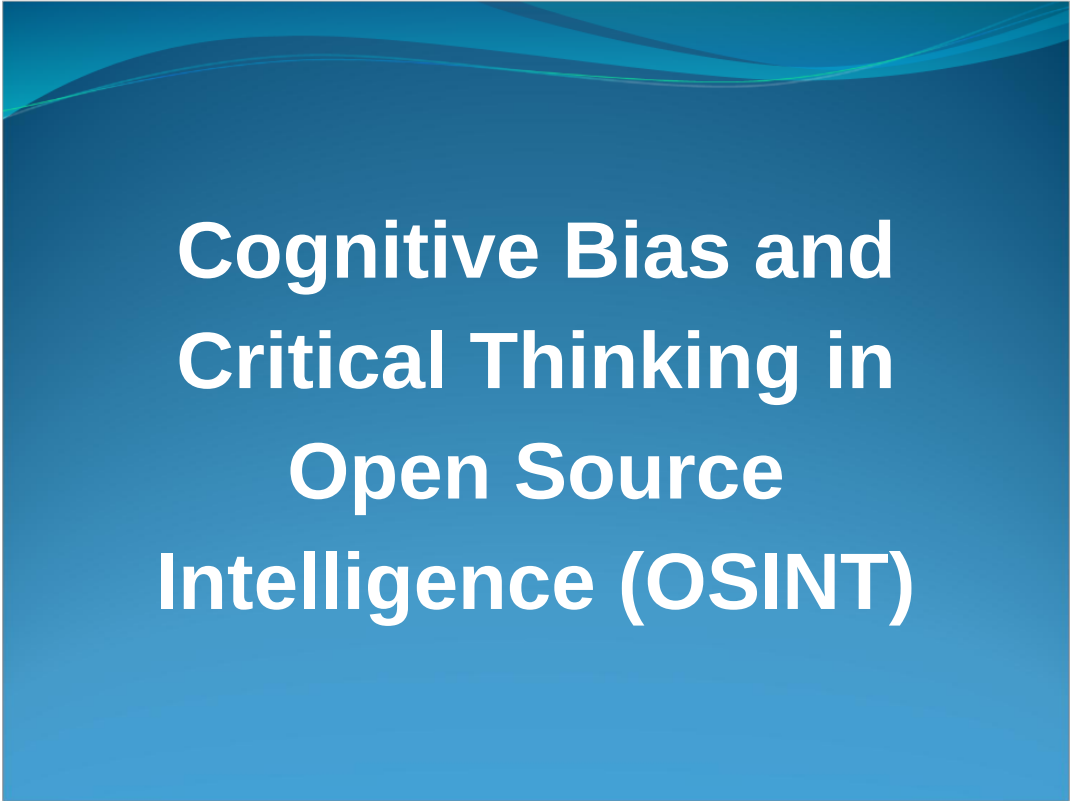
- Context
 - * Chrononarcissism and historical context
 - * Socio-cultural and economic context
- Unknown unknowns and blindspots
- Data originator biases /
data supply-chain pressures
- Baked-in Bias for OSINT automation tools
- Analysis of competing hypotheses (ACH)

Suggested Reading

- **“Psychology of Intelligence Analysis”**, Richards J. Heuer, Jr.
- **“A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis”**, US Government
- **“Judgement in Managerial Decision Making”**, Max H. Bazerman and Don Moore

Contact Me

bbrowntalks@gmail.com



Cognitive Bias and Critical Thinking in Open Source Intelligence (OSINT)

Benjamin Brown

Akamai Technologies

Security Architecture

- * Law Enforcement Engagement**
- * Systems Safety**
- * Threat Intelligence**
- * Security Research**
 - Novel Attack Vectors**
 - Multilayered Attacks**



Coming To Terms

- Cognitive Biases**
- Open Source Intelligence**
- Intelligence Analysis**
- Metacognition**
- Critical Thinking**
- Frameworks for Structured Analysis**



The terms may layout a 'So', but we also need a 'So What'

Why We Care

Actionable Intelligence

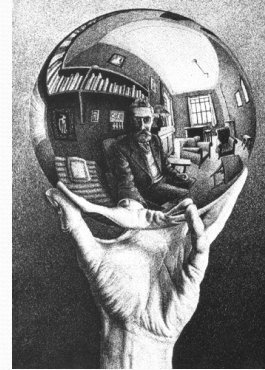
- Accurate conclusions
- Properly framed

Cognitive Biases (faulty heuristics)

- Can lead to inaccurate conclusions

Metacognition and Critical Thinking

- Recognize and correct for cognitive biases
- Arrive at more accurate solutions more often



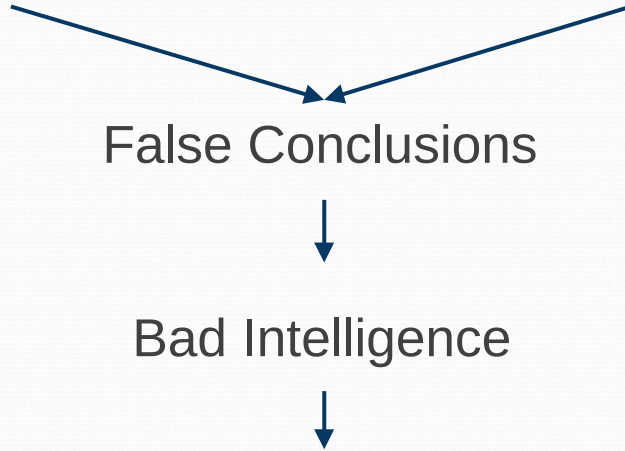
Why We Care

Bad Data

Biased Analysis

False Conclusions

Bad Intelligence



Why We Care



Think Bay of Pigs



Open Source Intelligence (OSINT)



Defining OSINT

"Intelligence produced
from publicly available
information"

Army Techniques Publication (ATP), "Open-Source Intelligence," 2-22.9 July 2012.

Defining OSINT

Typical Quality of Publicly Available Information:

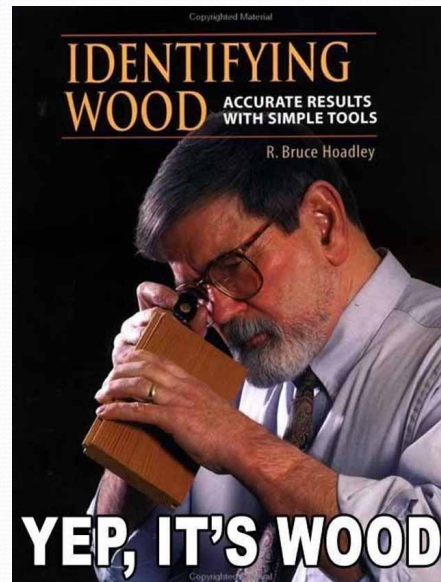


You are relying on public information of variable quality to draw important conclusions that you intend to act upon.
You damn well better be able to recognize bad information and bad analysis. Including you own!

Intelligence vs Information

- Timely
- Relevant
- Actionable

VS



Information may look interesting, but is it really useful?

OSINT Sources

- Search engines
- Social networks
- Communication services
- E-commerce site profiles
- Business / tax records
- Media



OSINT Tools

- Recon-ng
- ExifTool
- theHarvester
- Maltego
- Cree.py
- fierce.pl
- TAPIR
- DNSRecon



Defining Cognitive Bias

Defining Cognitive Bias

Note: Emotional, intrinsically cultural, spiritual, or faith-based biases are **out of scope.**

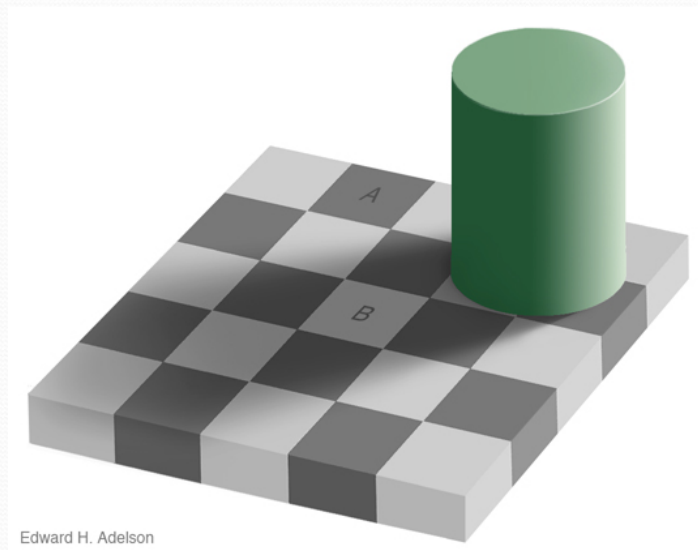




Defining Cognitive Bias

- Patterns of subjective judgment.
- Simplified information processing strategies.
- Subconscious mental procedures for processing information.

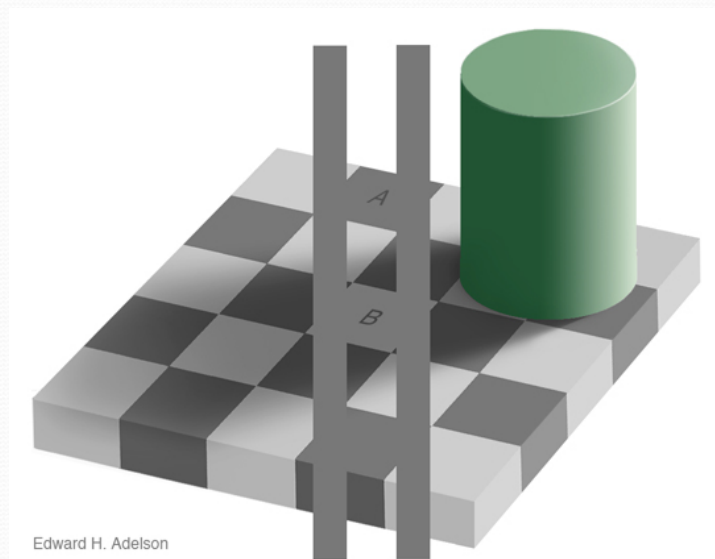
Defining Cognitive Bias



‘Deduction’ of color / shade

Human brain does not see the colors as they are, but ‘deduces’ the shade of grey from other information presented.

Defining Cognitive Bias



‘Deduction’ of color / shade

Human brain does not see the colors as they are, but ‘deduces’ the shade of grey from other information presented.



Example Types of Cognitive Bias



Select Biases

Confirmation Bias

- Seek out evidence that confirms
- Self-fulfilling prophecies
- Avoid information supporting competing hypotheses.

Select Biases

Self-serving Bias

- Self-enhancement
- Self-preservation
- Self-esteem
- Social and/or Career Advancement





Select Biases

Echo Effect

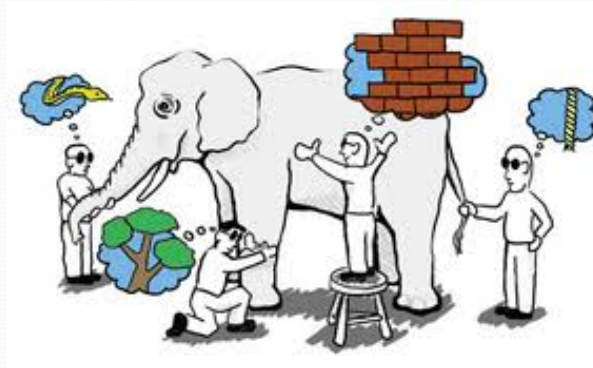
- Information repeated by source after source.

- * Media telephone
- * Sources obscured
- * Bandwagon effect
 - * Promotes group-think

Select Biases

Representativeness

- Focus on similarities / Neglect differences



Select Biases

Representativeness Cont.

- Base Rate Neglect

$$P(A | B) = \frac{P(B | A)P(A)}{P(B)}$$

Focusing on specific information and neglecting the importance of base rates

Select Biases

- Base Rate Neglect Cont.

- * Deadly Disease 'X'
- * Afflicts .01% of Population
- * Cheap diagnostic test that finds the disease in 99.5% of those infected, false-positive rate of only 1.95%

* **Test = Positive (Oh God I'm Dying! 99.5%!!!)**

But Wait There's More

Focusing on specific information and neglecting the importance of base rates

Select Biases

- Base Rate Neglect Cont.

99.5% likely to find it *if* you have it.

- 1.95% false-positive rate
- 1 mill people tested, 100 of which are infected (.01%)
- Test accurately identifies 99 of them as infected
- **BUT** 19,500 uninfected receive a false-positive (1.95%)

Focusing on specific information and neglecting the importance of base rates



Select Biases

Availability Bias

- **“Anecdotal” (first or second hand)**
- **Topic’s trend-power**
- **Censorship**
- **Language(s) of collector / analyst**
- **Маскировка (Maskirovka)**

*** Dezinformatsiia**



Synthesis

Reddit vs. Boston Bombers



We're not right,
but we'll ruin your life anyway.



Reddit vs. Boston Bombers

“Methodology”

- Marathon Photos and Videos
 - * ‘not looking at the race’
- Warped police scanner snippets
- Multiple ‘suspects’
 - * Social media harassment / cyberstalking
- **Media outlets ran bad info from Reddit**

Reddit vs. Boston Bombers





Reddit vs. Boston Bombers

Bias

- Bandwagon effect
- Echo effect
- Availability bias
- Self-serving bias
- Confirmation bias

Mad Internet points yo, rolling in the karma

Attack Attribution - APT

APT: Advanced Persistent Threat
=
OMFGWTFBBQ CHINA!!1one!!



Attack Attribution - APT

“Evidence”

- Type of RAT (Remote Administration Tool)
- Geo Loc of C2s (Command and Control)
- ‘Shared similarities’ with past APTs
- Tool author’s (not user’s) native language
- “We’re expert researchers, just trust us”
(Show me your methodology!)

RAT - freely available source and compiled binaries

Geo Loc services like Maxmind are notoriously unreliable

Show Me Your Methodology!!

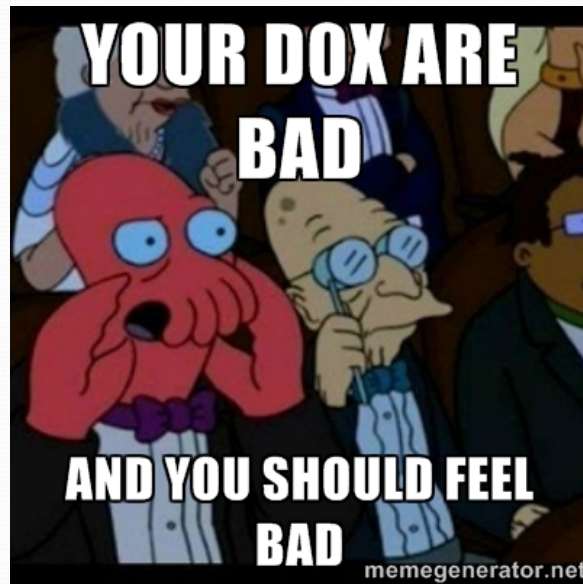
Attack Attribution - APT

(Vendor) Bias

- Confirmation bias
- Self-serving bias
- Representativeness
 - * Base rate / Population
- Availability Bias

Most reports come from Vendors offering anti-APT services

D0xing





White-Knight Syndrome

- Suspected Amanda Todd bully
- L337 Pro-Scientology hackers:
 - * 59 year-old couple
- LEO in Ferguson not involved
 - * Family info used for ID fraud

DDoS FUD





DDoS FUD

- Statistical methodology
 - * Sample size
 - * Length of collection time
- Availability bias
- Self-serving bias (vendors)

Newsweek vs The 'Creator of Bitcoin'



Malaysia Airways flight MH370 (Google Maps)





Groundwork For Remedy



Defining Metacognition

“Thinking about thinking”



Defining Critical Thinking

- **“What do I think I know?”**
- **“How do I think I know it?”**
- **“When would it not be true?”**



The More You Know

Know about cognitive biases.

- Difficult to affect that which you don't know you don't know.
- Everyone has them, you are not immune or invincible.

If you are familiar with them you are more likely to recognize them in yourself, your data, and others



The More You Know

[META INTENSIFIES]

**Beware The Bias Bias /
Bias Blind Spot**

- Belief that your bias is actually insight

The More You Know

Dr. Emily Pronin

Princeton University - Dept of Psychology

Subjects:

- Report being less susceptible to bias
- Infer bias in others holding contrary opinions



Pronin, Emily, et al. PSPB, Vol. 2 No 3, "The Bias Blind Spot: Perceptions of Bias in Self Versus Others," March 2002.



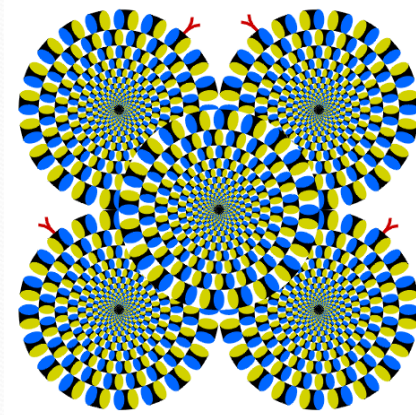
The More You Know

Actively seek out:

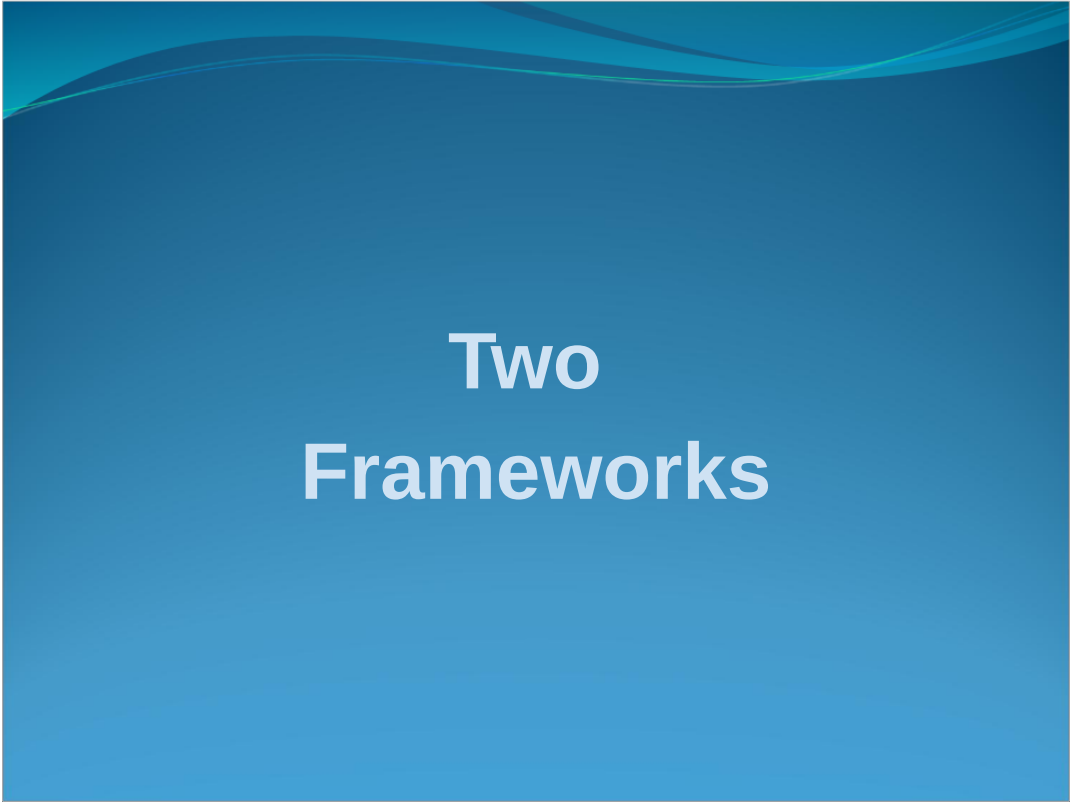
- Peer review
- Diverse, outside expertise
- Alternative mindsets

Defining Cognitive Bias

“Similar to optical illusions... [it] remains compelling even when one is fully aware of its nature.”



Heuer, Richards J., Jr. Psychology of Intelligence Analysis. Washington D.C.: CSI, 1999.



Two Frameworks

Structures and Frameworks

Checklists For Analysts

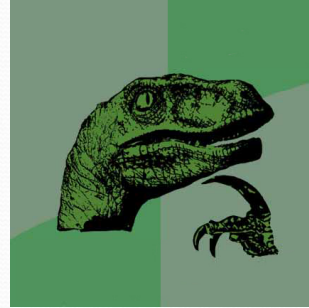
- Defining the problem
- Generating hypotheses
- Collecting information
- Evaluating hypotheses
- Selecting the most likely hypothesis
- Ongoing monitoring of new information

Heuer, Richard D., in "Psychology of Intelligence Analysis," Washington D.C.: CSI, 1999.

Structures and Frameworks

Defining The Problem

- Right question
- Framing
- Audience
- Specificity



Heuer, Richards J., Jr. "Psychology of Intelligence Analysis," Washington D.C.: CSI, 1999.



Structures and Frameworks

Generating Hypotheses

- Identify all plausible hypothesis
- Consult peers and outside experts
- Do not yet screen out or reject
- Consider actor deception or denial

Structures and Frameworks

Collecting Information

- Don't just focus on likely hypothesis

COLLECT ALL THE THINGS

- Suspend judgement

- Notice /note info gaps



Heuer, Richards J., Jr. "Psychology of Intelligence Analysis," Washington D.C.: CSI, 1999.

Structures and Frameworks

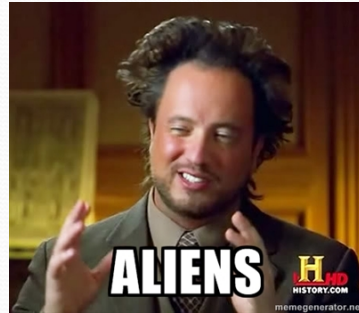
Evaluating Hypotheses

- Develop arguments ***against*** each hypothesis
- Check assumptions and their origins
- Implement ACH frameworks
(Analysis of Competing Hypothesis)

Structures and Frameworks

Selecting Most Likely Hypothesis

- **Least** evidence against
- **Reject** don't confirm
- Note alternate hypotheses



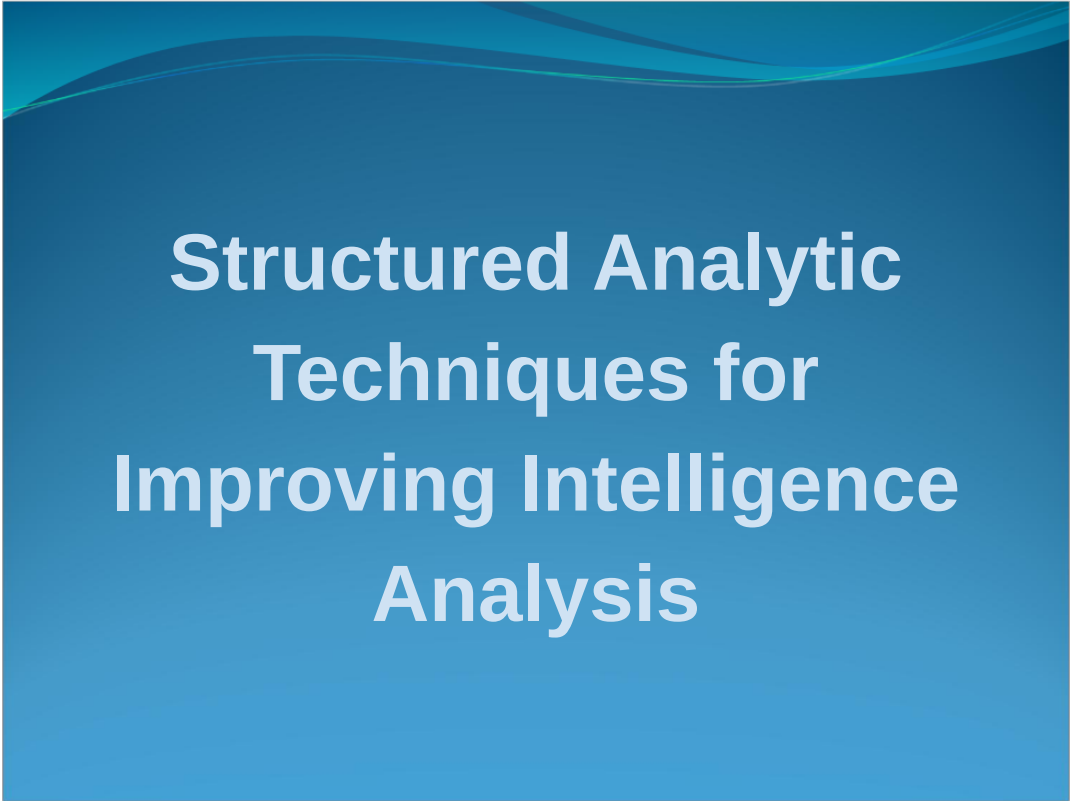
Heuer, Richards J., Jr. "Psychology of Intelligence Analysis," Washington D.C.: CSI, 1999.



Structures and Frameworks

Ongoing Monitoring

- Add data sources
- Plug-in alternate hypotheses
- Keep conclusions tentative



Structured Analytic Techniques for Improving Intelligence Analysis



Structures and Frameworks

Structured Analytic Techniques for Improving Intelligence Analysis

- Diagnostic Techniques
- Contrarian Techniques
- Imaginative Thinking Techniques

US Government, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009.



Structures and Frameworks

Diagnostic Techniques

- Key Assumptions Check

- *“What do we think we know? How do we think we know it?”

- Quality of Information Check

- Indicators or Signposts of Change

- Analysis of Competing Hypotheses

US Government, “A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis,” March 2009.

Key Assumptions Check - “What do we think we know? Why do we think we know it?”

Structures and Frameworks

Contrarian Techniques

- Devil's Advocacy
- Team A / Team B
- High-Impact /
Low-Probability
- "What If?" Analysis



US Government, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009.

Team A / Team B: Using separate analytic teams to contrast competing hypotheses

High-Impact / Low-Probability Analysis: Highlighting Black Swan Events

Structures and Frameworks

Imaginative Thinking Techniques

- Brainstorming
- Outside-In Thinking
- Red Team Analysis
- Alternative Futures Analysis

US Government, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2006

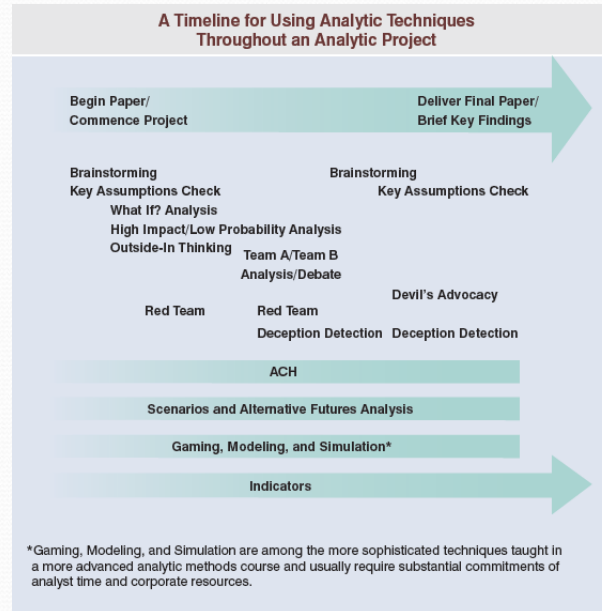
Outside-In Thinking: Identifying the full range of basic forces, factors, and trends that would indirectly shape an issue.

Red Team Analysis: Modeling adversaries

Alternative Futures Analysis: Systematically exploring multiple ways a situation can develop



Structures and Frameworks



US Government, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009.



Application



Application - Report

- Clearly Define
 - * Goals
 - * Sources
 - * Audience
 - * Limitations & Assumptions
 - ...



Application

METHODOLOGY

Verizon, Trend Micro, Prolexic, Recorded Future



Further Research



Further Research

- Context
 - * Chrononarcissism and historical context
 - * Socio-cultural and economic context
- Unknown unknowns and blindspots
- Data originator biases /
data supply-chain pressures
- Baked-in Bias for OSINT automation tools
- Analysis of competing hypotheses (ACH)



Suggested Reading

- **“Psychology of Intelligence Analysis”**, Richards J. Heuer, Jr.
- **“A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis”**, US Government
- **“Judgement in Managerial Decision Making”**, Max H. Bazerman and Don Moore



Contact Me

bbrowntalks@gmail.com