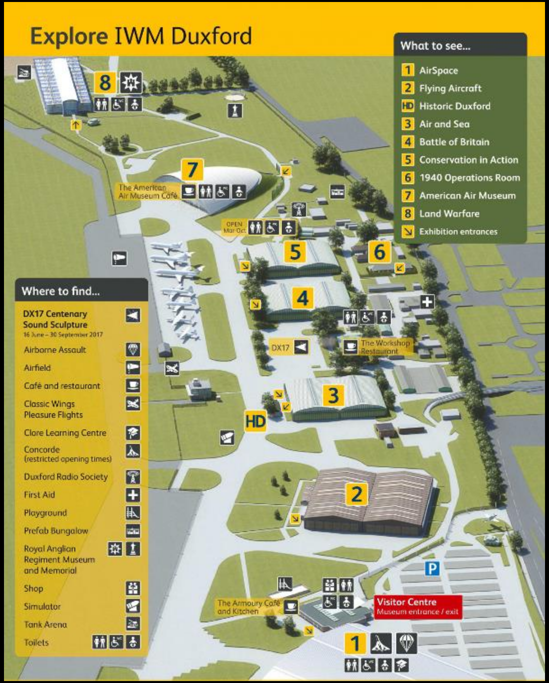
There Is MOAR To Structured Analytic Techniques Than Just ACH!

Rick Holland
CISO, Digital Shadows

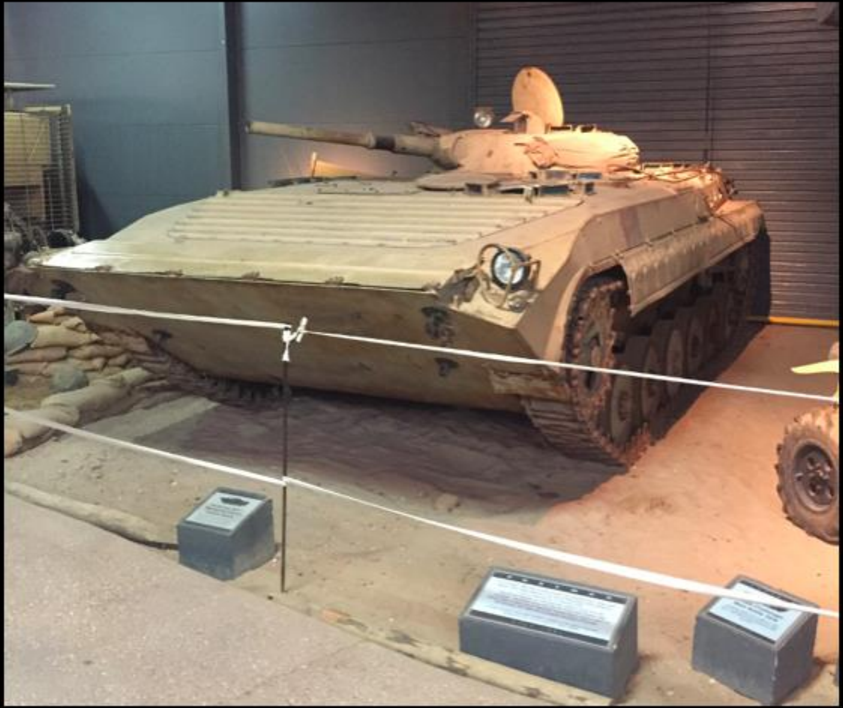
@rickhholland
#CTISummit

Welcome to
IWM Duxford
Schuhmacher
iwm.org.uk


Explore IWM Duxford
What to see...
1 AirSpace
2 Flying Aircraft
HD Historic Duxford
3 Air and Sea
4 Battle of Britain
5 Conservation in Action
6 1940 Operations Room
7 American Air Museum
8 Land Warfare
Exhibition entrances
Where to find...
DX17 Centenary Sound Sculpture
16 June – 30 September 2017
Airborne Assault
Airfield
Café and restaurant
Classic Wings Pleasure Flights
Clore Learning Centre
Concorde (restricted opening times)
Duxford Radio Society
First Aid
Playground
Prefab Bungalow
Royal Anglian Regiment Museum and Memorial
Shop
Simulator
Tank Arena
Toilets
The American Air Museum Café
OPEN Mar-Oct
DX17
The Workshop Restaurant
The Armoury Café and Kitchen
Visitor Centre
Museum entrance / exit
P

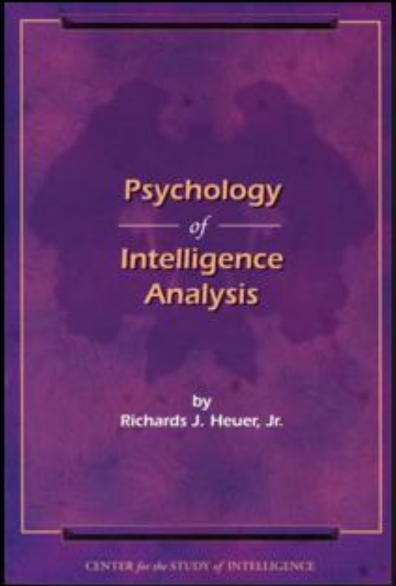
BT
020

BMP1 or BMP2?



FAIL

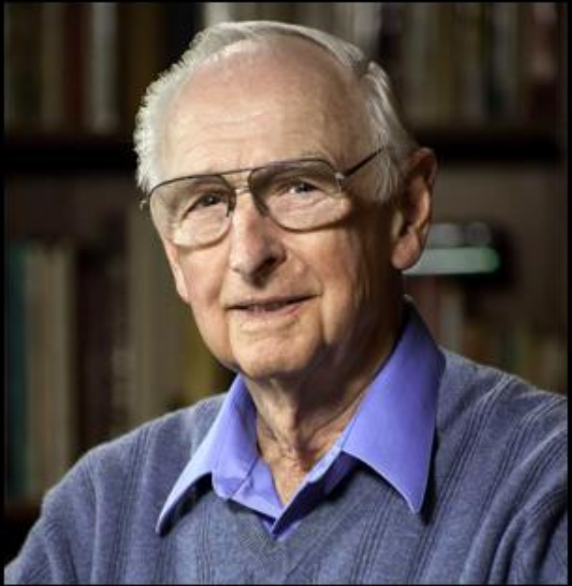
Dick Heuer Jr.



Psychology of Intelligence Analysis

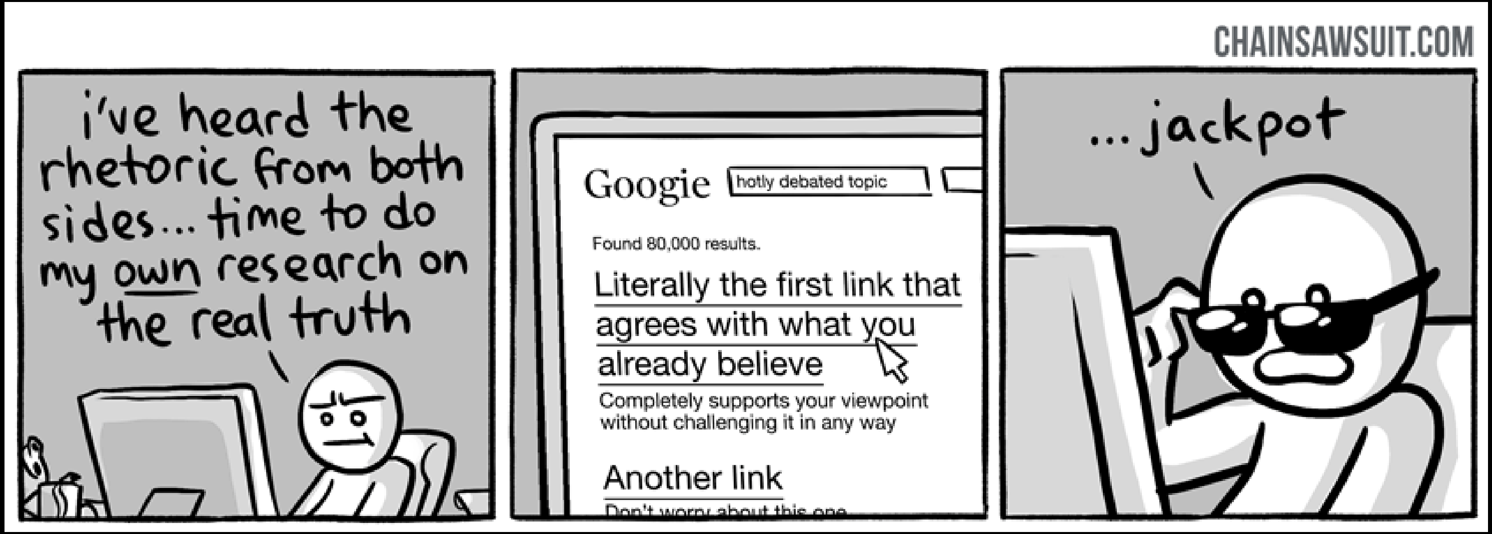
by
Richards J. Heuer, Jr.

CENTER *for the* STUDY *of* INTELLIGENCE



"Structured analysis uses structured techniques to mitigate the adverse impact on our analysis of known cognitive limitations and pitfalls. The most distinctive characteristic is that structured techniques externalize and decompose our thinking in a manner that enables it to be reviewed and critiqued piece by piece, or step by step, by other knowledgeable analysts."

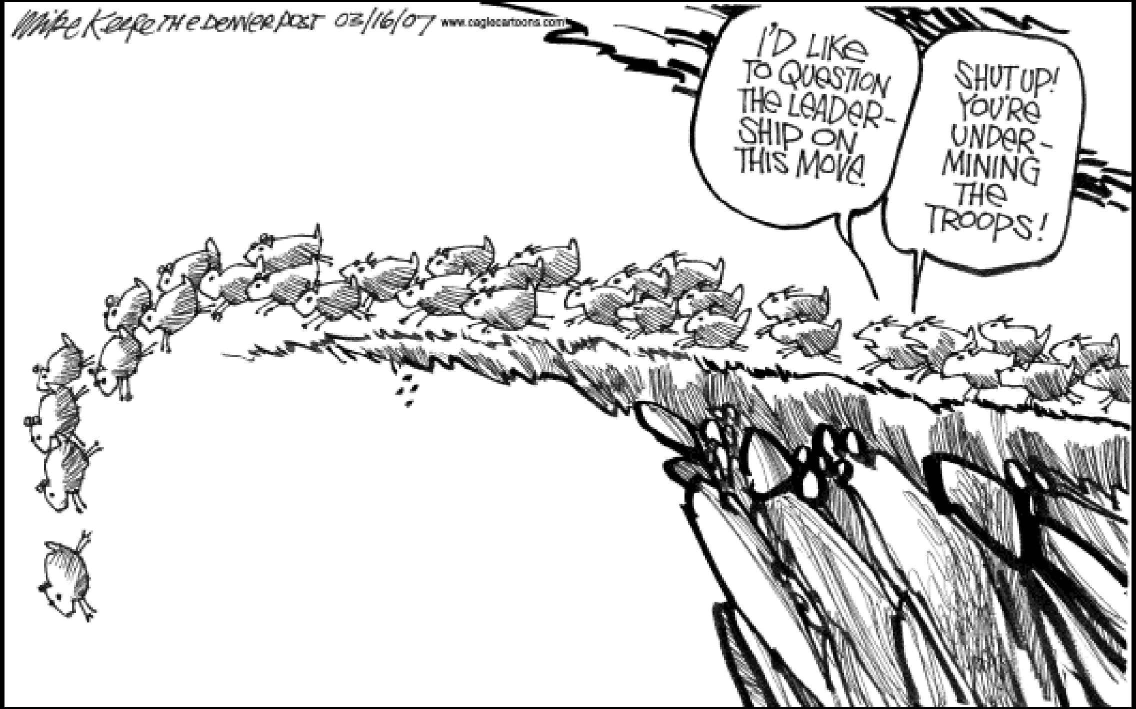
Confirmation bias

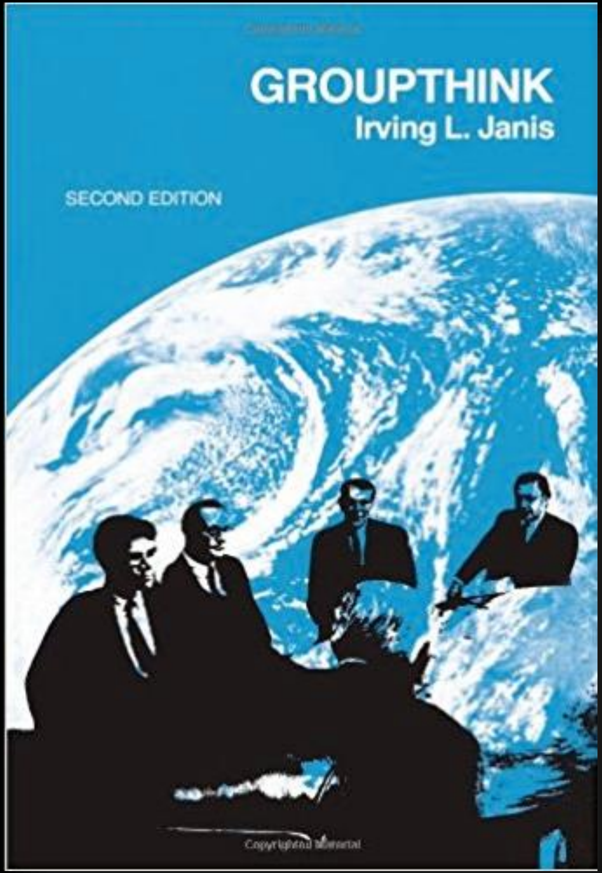

CHAINSAWSUIT.COM
i've heard the rhetoric from both sides... time to do my own research on the real truth
Googie
hotly debated topic
Found 80,000 results.
Literally the first link that agrees with what you already believe
Completely supports your viewpoint without challenging it in any way
Another link
Don't worry about this one
...jackpot

Mirror imaging

Anchoring

Groupthink


Mike Keefe THE DENVER POST 03/16/07 www.caglecartoons.com
I'D LIKE TO QUESTION THE LEADERSHIP ON THIS MOVE!
SHUT UP! YOU'RE UNDERMINING THE TROOPS!

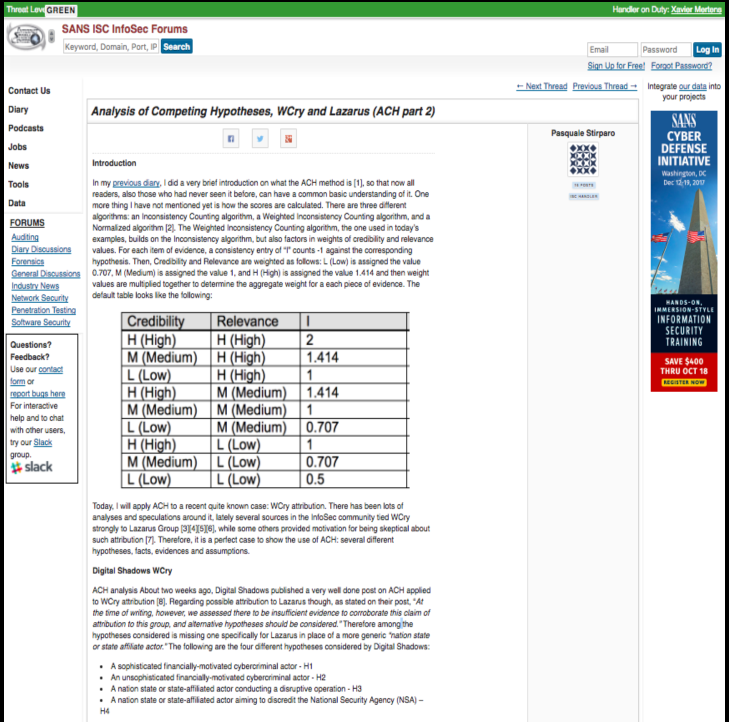


Groupthink contributors:

1. Cohesion	Lack of Methodological Procedure Lack of Critical Culture
2. Organizational Faults	Lack of Impartial leadership Lack of Diversity Lack of Methodological Procedures
3. Situational Factors	Fatigue Emotional Welfare

Familiar?

Analysis of Competing Hypothesis



Threat Leve GREEN | Handler on Duty: Xavier Mertens

SANS ISC InfoSec Forums

Keyword, Domain, Port, IP | Search

Email | Password | Log In

Sign Up for Free! Forgot Password?

Contact Us
Diary
Podcasts
Jobs
News
Tools
Data

FORUMS
Auditing
Diary Discussions
Forensics
General Discussions
Industry News
Network Security
Penetration Testing
Software Security

Questions? Feedback? Use our contact form or report bugs here For interactive help and to chat with other users, try our Slack group.

slack

← Next Thread Previous Thread →

Integrate our data into your projects

Analysis of Competing Hypotheses, WCry and Lazarus (ACH part 2)

Pasquale Stirparo

Introduction

In my previous diary, I did a very brief introduction on what the ACH method is [1], so that now all readers, also those who had never seen it before, can have a common basic understanding of it. One more thing I have not mentioned yet is how the scores are calculated. There are three different algorithms: an Inconsistency Counting algorithm, a Weighted Inconsistency Counting algorithm, and a Normalized algorithm [2]. The Weighted Inconsistency Counting algorithm, the one used in today's examples, builds on the Inconsistency algorithm, but also factors in weights of credibility and relevance values. For each item of evidence, a consistency entry of "I" counts -1 against the corresponding hypothesis. Then, Credibility and Relevance are weighted as follows: L (Low) is assigned the value 0.707, M (Medium) is assigned the value 1, and H (High) is assigned the value 1.414 and then weight values are multiplied together to determine the aggregate weight for a each piece of evidence. The default table looks like the following:

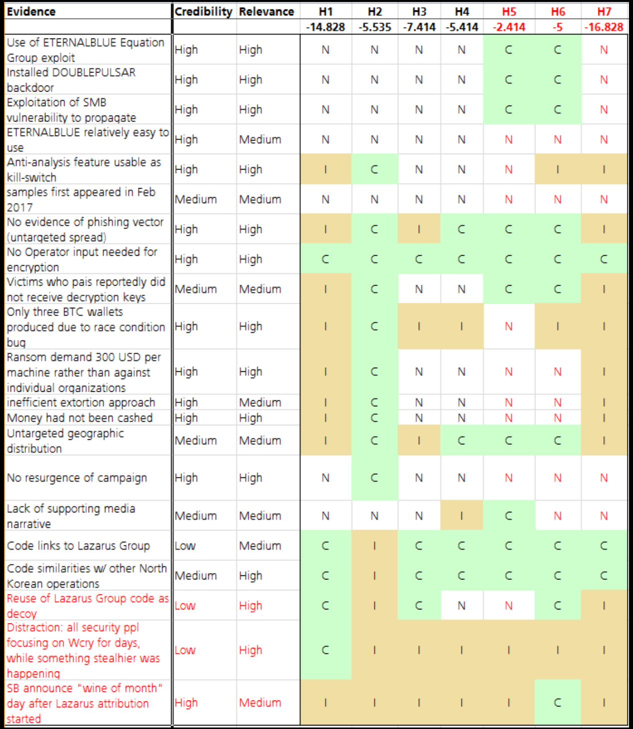
Credibility	Relevance	I
H (High)	H (High)	2
M (Medium)	H (High)	1.414
L (Low)	H (High)	1
H (High)	M (Medium)	1.414
M (Medium)	M (Medium)	1
L (Low)	M (Medium)	0.707
H (High)	L (Low)	1
M (Medium)	L (Low)	0.707
L (Low)	L (Low)	0.5

Today, I will apply ACH to a recent quite known case: WCry attribution. There has been lots of analyses and speculations around it, lately several sources in the InfoSec community tied WCry strongly to Lazarus Group [3][4][5][6], while some others provided motivation for being skeptical about such attribution [7]. Therefore, it is a perfect case to show the use of ACH: several different hypotheses, facts, evidences and assumptions.

Digital Shadows WCry

ACH analysis About two weeks ago, Digital Shadows published a very well done post on ACH applied to WCry attribution [8]. Regarding possible attribution to Lazarus though, as stated on their post, "*At the time of writing, however, we assessed there to be insufficient evidence to corroborate this claim of attribution to this group, and alternative hypotheses should be considered.*" Therefore among the hypotheses considered is missing one specifically for Lazarus in place of a more generic *"nation state or state affiliate actor."* The following are the four different hypotheses considered by Digital Shadows:

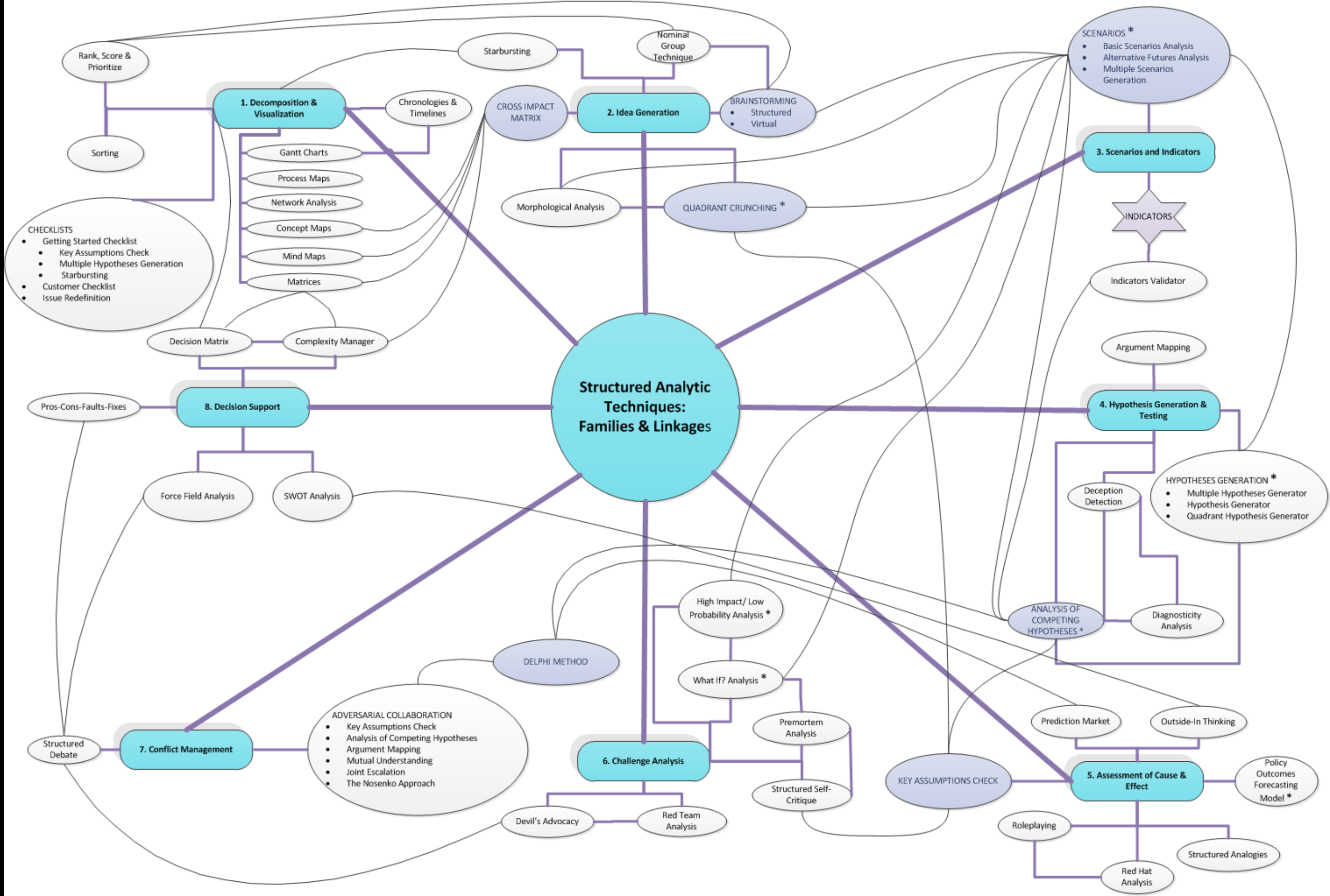
- A sophisticated financially-motivated cybercriminal actor - H1
- An unsophisticated financially-motivated cybercriminal actor - H2
- A nation state or state-affiliated actor conducting a disruptive operation - H3
- A nation state or state-affiliated actor aiming to discredit the National Security Agency (NSA) – H4



Evidence	Credibility	Relevance	H1	H2	H3	H4	H5	H6	H7
			-14.828	-5.535	-7.414	-5.414	-2.414	-5	-16.828
Use of ETERNALBLUE Equation Group exploit	High	High	N	N	N	N	C	C	N
Installed DOUBLEPULSAR backdoor	High	High	N	N	N	N	C	C	N
Exploitation of SMB vulnerability to propagate	High	High	N	N	N	N	C	C	N
ETERNALBLUE relatively easy to use	High	Medium	N	N	N	N	N	N	N
Anti-analysis feature usable as kill-switch	High	High	I	C	N	N	N	I	I
samples first appeared in Feb 2017	Medium	Medium	N	N	N	N	N	N	N
No evidence of phishing vector (untargeted spread)	High	High	I	C	I	C	C	C	I
No Operator input needed for encryption	High	High	C	C	C	C	C	C	C
Victims who pais reportedly did not receive decryption keys	Medium	Medium	I	C	N	N	C	C	I
Only three BTC wallets produced due to race condition bug	High	High	I	C	I	I	N	I	I
Ransom demand 300 USD per machine rather than against individual organizations	High	High	I	C	N	N	N	N	I
inefficient extortion approach	High	Medium	I	C	N	N	N	N	I
Money had not been cashed	High	High	I	C	N	N	N	N	I
Untargeted geographic distribution	Medium	Medium	I	C	I	C	C	C	I
No resurgence of campaign	High	High	N	C	N	N	N	N	N
Lack of supporting media narrative	Medium	Medium	N	N	N	I	C	N	N
Code links to Lazarus Group	Low	Medium	C	I	C	C	C	C	C
Code similarities w/ other North Korean operations	Medium	High	C	I	C	C	C	C	C
Reuse of Lazarus Group code as decoy	Low	High	C	I	C	N	N	C	I
Distraction: all security ppl focusing on Wcry for days, while something stealhier was happening	Low	High	C	I	I	I	I	I	I
SB announce "wine of month" day after Lazarus attribution started	High	Medium	I	I	I	I	I	C	I

BUT WAIT
THERE'S MORE
memes.com

BUT WAIT
THERE'S MORE
memegenerator.net



Structured Analytic Techniques: Families & Linkages

1. Decomposition & Visualization
- Rank, Score & Prioritize
- Sorting
- Chronologies & Timelines
- Gantt Charts
- Process Maps
- Network Analysis
- Concept Maps
- Mind Maps
- Matrices
- CHECKLISTS
  - Getting Started Checklist
    - Key Assumptions Check
    - Multiple Hypotheses Generation
    - Starbursting
  - Customer Checklist
  - Issue Redefinition

2. Idea Generation
- Starbursting
- Nominal Group Technique
- CROSS IMPACT MATRIX
- BRAINSTORMING
  - Structured
  - Virtual
- Morphological Analysis
- QUADRANT CRUNCHING *

3. Scenarios and Indicators
- SCENARIOS *
  - Basic Scenarios Analysis
  - Alternative Futures Analysis
  - Multiple Scenarios Generation
- INDICATORS
- Indicators Validator

4. Hypothesis Generation & Testing
- Argument Mapping
- Deception Detection
- HYPOTHESES GENERATION *
  - Multiple Hypotheses Generator
  - Hypothesis Generator
  - Quadrant Hypothesis Generator
- ANALYSIS OF COMPETING HYPOTHESES *
- Diagnosticity Analysis

5. Assessment of Cause & Effect
- Prediction Market
- Outside-In Thinking
- KEY ASSUMPTIONS CHECK
- Policy Outcomes Forecasting Model *
- Roleplaying
- Structured Analogies
- Red Hat Analysis

6. Challenge Analysis
- High Impact/ Low Probability Analysis *
- What If? Analysis *
- Premortem Analysis
- Structured Self-Critique
- Devil's Advocacy
- Red Team Analysis
- DELPHI METHOD

7. Conflict Management
- Structured Debate
- ADVERSARIAL COLLABORATION
  - Key Assumptions Check
  - Analysis of Competing Hypotheses
  - Argument Mapping
  - Mutual Understanding
  - Joint Escalation
  - The Nosenko Approach

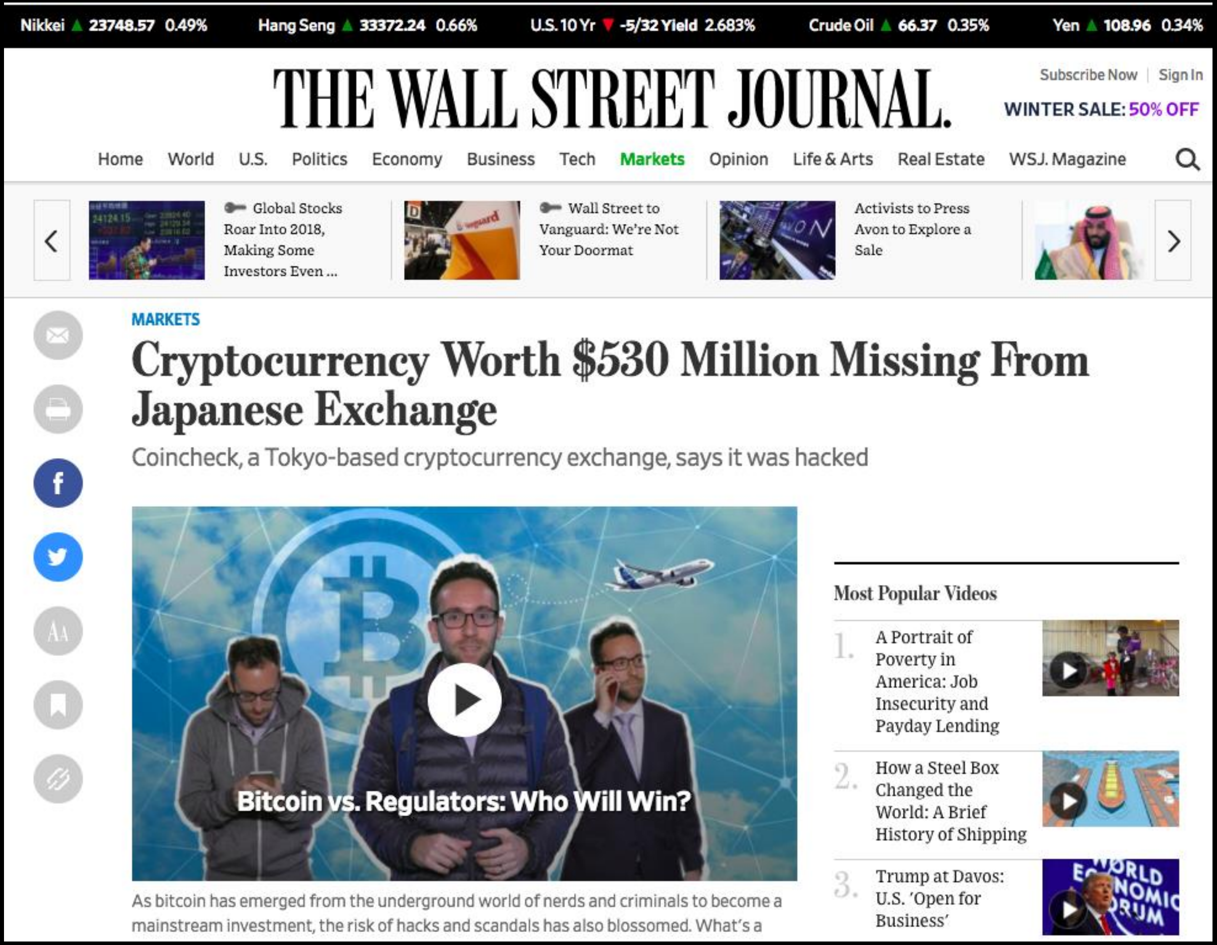
8. Decision Support
- Decision Matrix
- Complexity Manager
- Pros-Cons-Faults-Fixes
- Force Field Analysis
- SWOT Analysis

Source: Structured Analytic Techniques for Intelligence Analysis

Different techniques for different scenarios

Tactical	Structured Brainstorming	ACH
Operational	SWOT	Red Hat Analysis
Strategic	Scenario Planning / Horizon Scanning	Cone of Plausibility

Ain’t nobody got time for that!!!



Nikkei ▲ 23748.57 0.49% Hang Seng ▲ 33372.24 0.66% U.S. 10 Yr ▼ -5/32 Yield 2.683% Crude Oil ▲ 66.37 0.35% Yen ▲ 108.96 0.34%

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

Global Stocks Roar Into 2018, Making Some Investors Even ...

Wall Street to Vanguard: We're Not Your Doormat

Activists to Press Avon to Explore a Sale

MARKETS

Cryptocurrency Worth $530 Million Missing From Japanese Exchange

Coincheck, a Tokyo-based cryptocurrency exchange, says it was hacked

As bitcoin has emerged from the underground world of nerds and criminals to become a mainstream investment, the risk of hacks and scandals has also blossomed. What's a

Most Popular Videos

1. A Portrait of Poverty in America: Job Insecurity and Payday Lending
2. How a Steel Box Changed the World: A Brief History of Shipping
3. Trump at Davos: U.S. 'Open for Business'

New CISO says: “ZOMG tell me about BITCOIN fraud!”

Key Assumptions Check

“Systematic effort to make explicit and question the assumptions that guide an analyst’s interpretation of evidence and reasoning about any particular problem."

Cryptocurrency fraud key assumptions

- Cybercriminals will always seek opportunities for financial gain and will continue developing tools
- Technological advances will increase anonymity offered by new cryptocurrencies
- New cryptocurrencies will remain volatile, subject to speculation and price bubbles
- Cryptocurrencies will eventually be adopted by major retailers and financial institutions
- New alt coins and exchanges will emerge
- Regulation inevitable as cryptocurrencies are integrated into everyday society
- Security failures and poor practices will continue

ICE BOX
EMERGENCY
IN PROGRESS
TESTING
COMPLETE
CLOUD
INGESTION ENGINE
COMPRESSION ENGINE
FILE STORAGE SERVICES
PUBLISHING SERVICES
CDN DISTRIBUTION SERVICES
CONSUMPTION SERVICES
CONSUMPTION EDGE
OPERATIONS BILLING AND USER MANAGEMENT

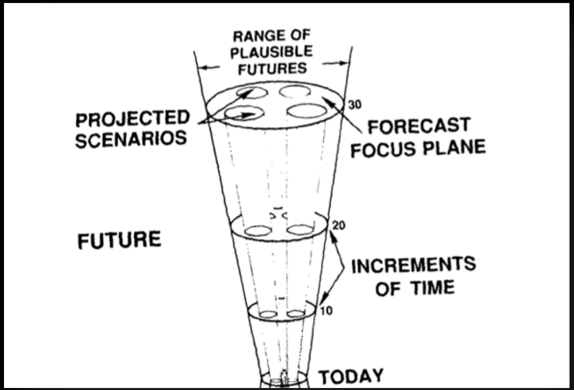
- Which circumstances would make the assumption untrue?
- Was the assumption true in the past but no longer?
- Assign a confidence level.
- Rate each as: Solid/Caveated/Unsupported

Forecast, don’t predict with the Cone of Plausibility

@rickhholland
#CTISummit

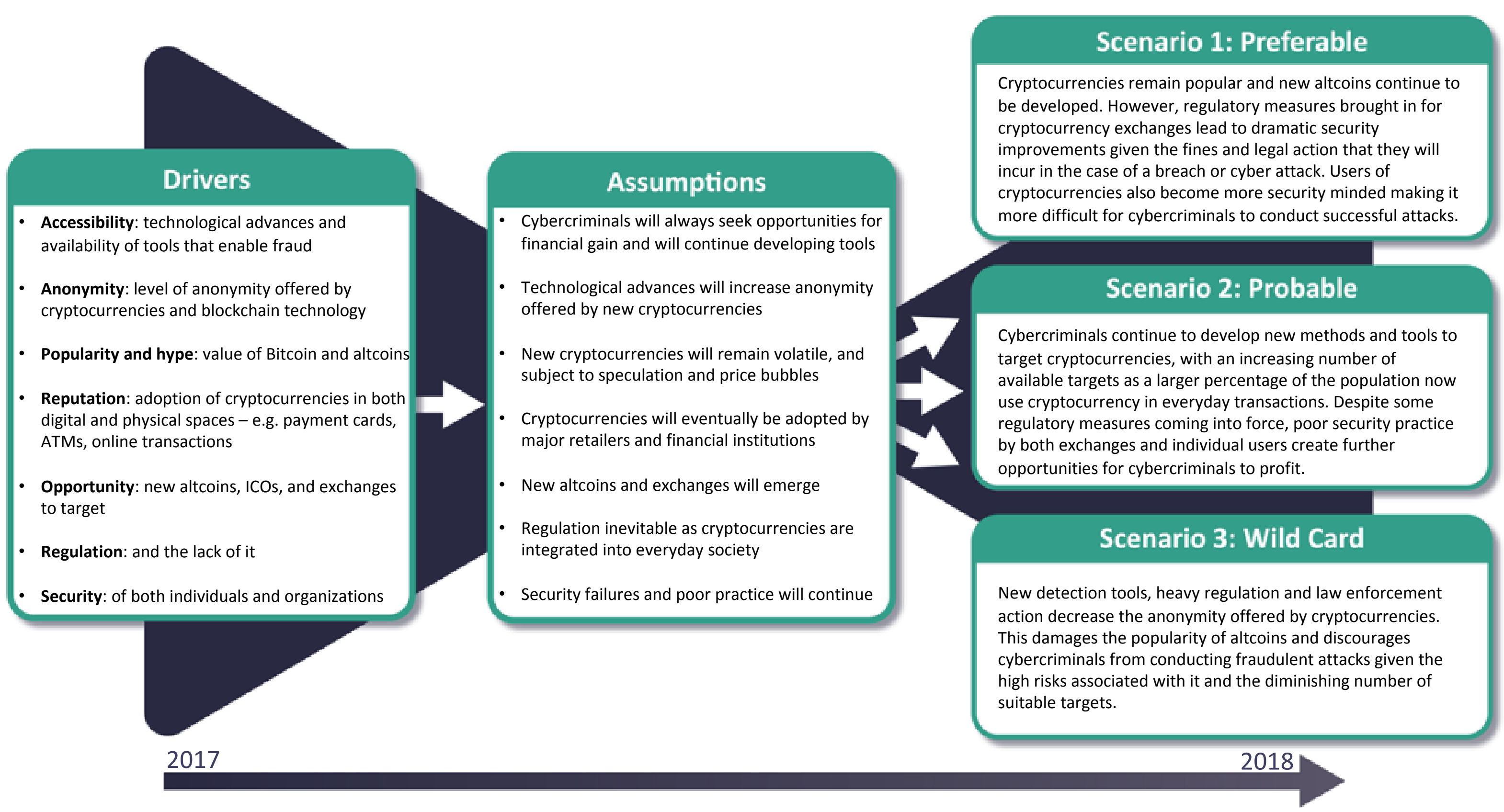
The methodology

- Project trends, events and their consequences holistically into the future.
- Permits a logical progression into time and the creation of alternative scenarios at preselected points or intervals called forecasts.



The methodology

1. Understand the current conditions
2. Cleary state
    1. Drivers
    2. Assumptions
3. Scenarios
    1. Preferred
    2. Probable
    3. Wildcard
4. Map controls against scenarios
5. Monitor for scenarios' emergence



Drivers

- **Accessibility**: technological advances and availability of tools that enable fraud
- **Anonymity**: level of anonymity offered by cryptocurrencies and blockchain technology
- **Popularity and hype**: value of Bitcoin and altcoins
- **Reputation**: adoption of cryptocurrencies in both digital and physical spaces – e.g. payment cards, ATMs, online transactions
- **Opportunity**: new altcoins, ICOs, and exchanges to target
- **Regulation**: and the lack of it
- **Security**: of both individuals and organizations

Assumptions

- Cybercriminals will always seek opportunities for financial gain and will continue developing tools
- Technological advances will increase anonymity offered by new cryptocurrencies
- New cryptocurrencies will remain volatile, and subject to speculation and price bubbles
- Cryptocurrencies will eventually be adopted by major retailers and financial institutions
- New altcoins and exchanges will emerge
- Regulation inevitable as cryptocurrencies are integrated into everyday society
- Security failures and poor practice will continue

Scenario 1: Preferable

Cryptocurrencies remain popular and new altcoins continue to be developed. However, regulatory measures brought in for cryptocurrency exchanges lead to dramatic security improvements given the fines and legal action that they will incur in the case of a breach or cyber attack. Users of cryptocurrencies also become more security minded making it more difficult for cybercriminals to conduct successful attacks.

Scenario 2: Probable

Cybercriminals continue to develop new methods and tools to target cryptocurrencies, with an increasing number of available targets as a larger percentage of the population now use cryptocurrency in everyday transactions. Despite some regulatory measures coming into force, poor security practice by both exchanges and individual users create further opportunities for cybercriminals to profit.

Scenario 3: Wild Card

New detection tools, heavy regulation and law enforcement action decrease the anonymity offered by cryptocurrencies. This damages the popularity of altcoins and discourages cybercriminals from conducting fraudulent attacks given the high risks associated with it and the diminishing number of suitable targets.

Probable scenario

Cybercriminals continue to develop new methods and tools to target cryptocurrencies, with an increasing number of available targets as a larger percentage of the population now use cryptocurrency in everyday transactions. Despite some regulatory measures coming into force, poor security practice by both exchanges and individual users create further opportunities for cybercriminals to profit.

Develop courses of action

@rickhholland
#CTISummit

Monitor GitHub and similar services for Amazon credentials that could be leveraged for crypto mining using your compute

GitHub

amazon
web services

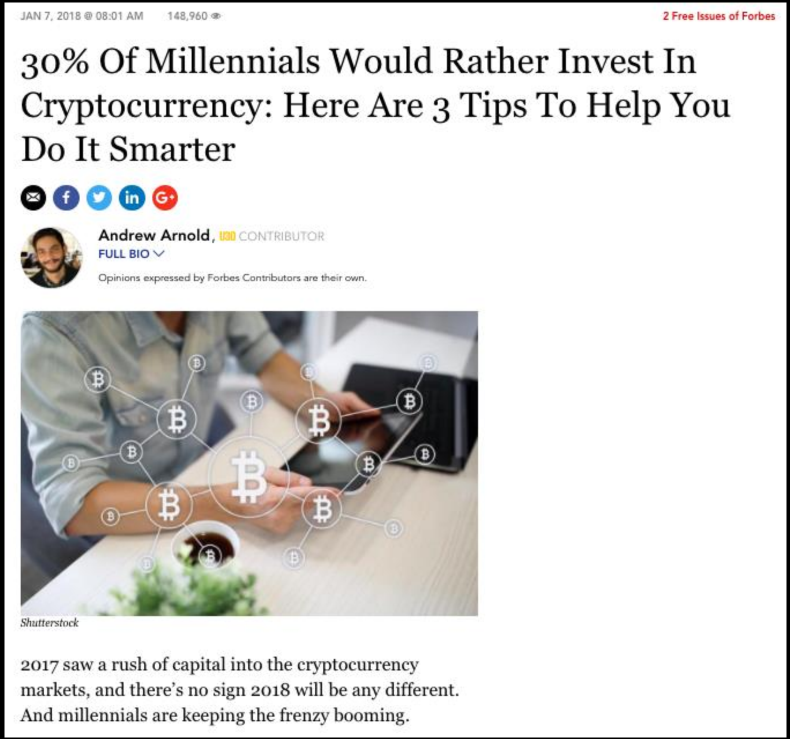
Validate web browser security controls are in place and account for 3rd party extensions

Use haveibeenpwned to monitor for employee credentials that could be exposed in cryptocurrency exchange compromises

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Provide Security Awareness training for staff that are likely to invest in cryptocurrencies



JAN 7, 2018 @ 08:01 AM 148,960

2 Free Issues of Forbes

30% Of Millennials Would Rather Invest In Cryptocurrency: Here Are 3 Tips To Help You Do It Smarter

Andrew Arnold, U30 CONTRIBUTOR

FULL BIO

Opinions expressed by Forbes Contributors are their own.

Shutterstock

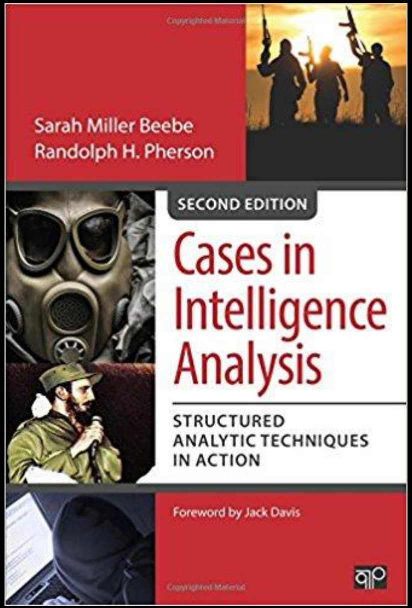
2017 saw a rush of capital into the cryptocurrency markets, and there's no sign 2018 will be any different. And millennials are keeping the frenzy booming.

What you can do

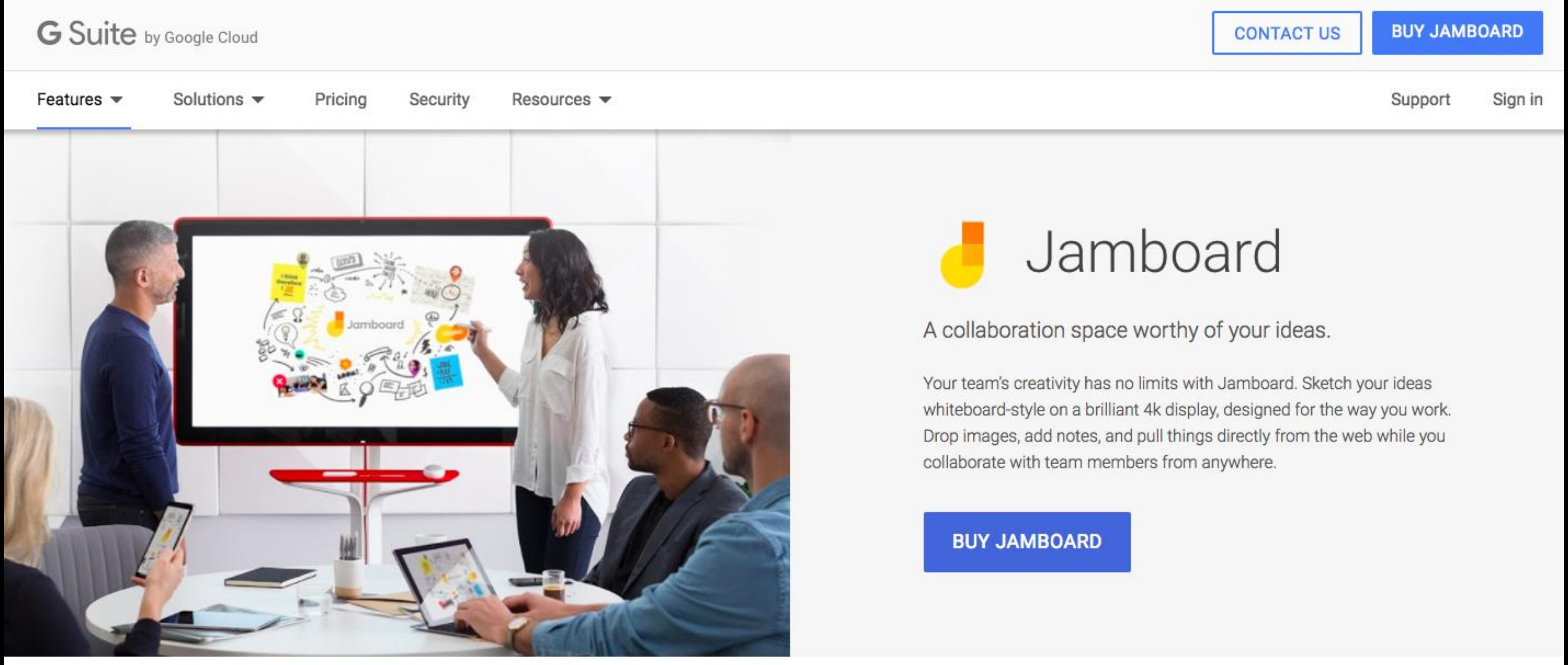
@rickhholland
#CTISummit

Recommended team activity

- Inspired by “Cases in Intelligence Analysis”
- Run periodic SAT exercises with your team
- Use historical examples from this book, or use previous assessments your team has produced



Google Docs

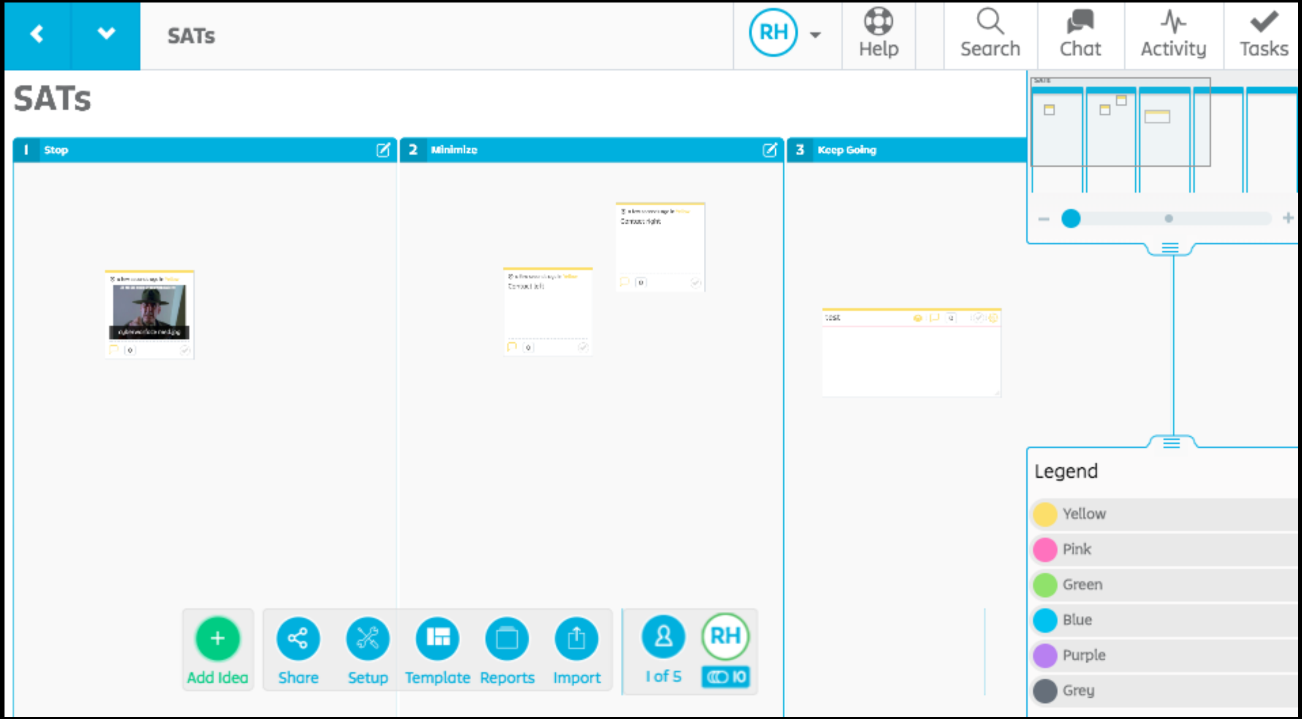


Jamboard

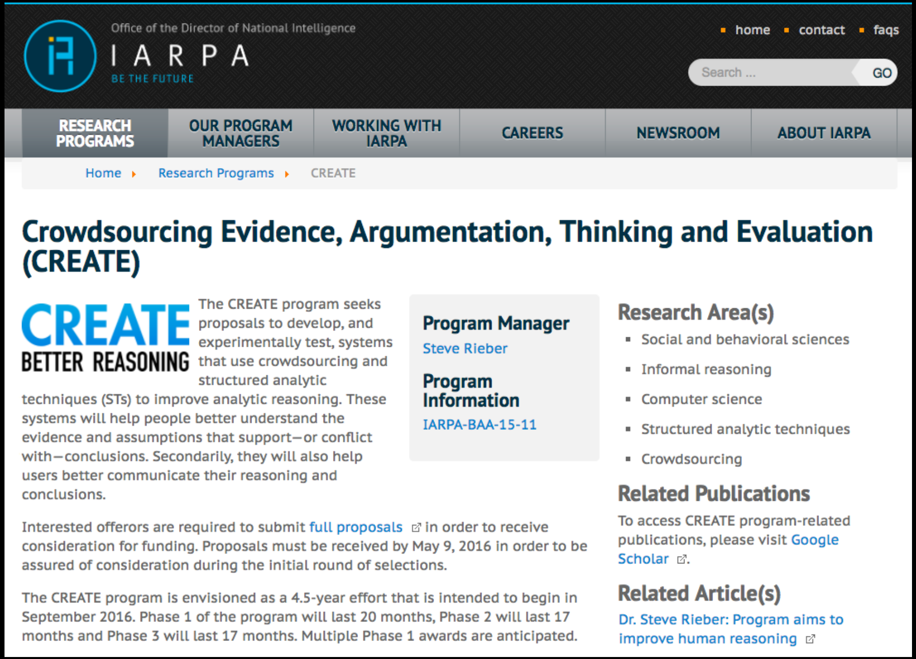
A collaboration space worthy of your ideas.

Your team's creativity has no limits with Jamboard. Sketch your ideas whiteboard-style on a brilliant 4k display, designed for the way you work. Drop images, add notes, and pull things directly from the web while you collaborate with team members from anywhere.

Use tools like Google Jamboard



Use tools like Stormboard



Crowdsourcing Evidence, Argumentation, Thinking and Evaluation (CREATE)

The CREATE program seeks proposals to develop, and experimentally test, systems that use crowdsourcing and structured analytic techniques (STs) to improve analytic reasoning. These systems will help people better understand the evidence and assumptions that support—or conflict with—conclusions. Secondarily, they will also help users better communicate their reasoning and conclusions.

Interested offerors are required to submit full proposals in order to receive consideration for funding. Proposals must be received by May 9, 2016 in order to be assured of consideration during the initial round of selections.

The CREATE program is envisioned as a 4.5-year effort that is intended to begin in September 2016. Phase 1 of the program will last 20 months, Phase 2 will last 17 months and Phase 3 will last 17 months. Multiple Phase 1 awards are anticipated.

Program Manager
Steve Rieber

Program Information
IARPA-BAA-15-11

Research Area(s)

- Social and behavioral sciences
- Informal reasoning
- Computer science
- Structured analytic techniques
- Crowdsourcing

Related Publications

To access CREATE program-related publications, please visit Google Scholar.

Related Article(s)

Dr. Steve Rieber: Program aims to improve human reasoning

Intelligence Advanced Research Projects Activity

Track CREATE projects

- Co-Arg - Cogent Argumentation System with Crowd Elicitation
- SWARM - Smartly-assembled Wiki-style Argument Marshalling
- TRACE - Trackable Reasoning and Analysis for Collaboration and Evaluation

GEORGE MASON UNIVERSITY

POSTERA CRESCAM LAUDE
THE UNIVERSITY OF MELBOURNE

SYRACUSE UNIVERSITY

SATs aren’t silver bullets

“Tell me what you know. Tell me what you don’t know. And then, based on what you really know and what you really don’t know, tell me what you think is most likely to happen.”

Thank you!

@rickhholland

For more information:

- Richards J. Heuer Jr., Randolph H. Pherson, Structured Analytic Techniques for Intelligence Analysis: https://www.amazon.com/Structured-Analytic-Techniques-Intelligence-Analysis/dp/1608710181
- UK Government Office for Science, Horizon Scanning: http://webarchive.nationalarchives.gov.uk/20140108141323/http://www.bis.gov.uk/assets/foresight/docs/horizon-scanning-centre/foresight_scenario_planning.pdf
- RAND, Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1408/RAND_RR1408.pdf
- PARC ACH Software: http://www2.parc.com/istl/projects/ach/ach.html
- Creating Strategic Visions. US National Intelligence Strategy, 2014: https://www.dni.gov/files/2014_NIS_Publication.pdf