2022 INSIDER THREAT VIRTUAL CONFERENCE

Defense Counterintelligence and Security Agency,
Center for Development of Security Excellence,
Insider Threat Division

Office of the Under Secretary of Defense (Intelligence & Security),

Counter Insider Threat Program

September 1, 2022

WELCOME

CDSE

Center for Development
of Security Excellence

Amber Jackson

Curriculum Manager
CDSE Insider Threat Division

NITAM

National Insider Threat Awareness Month

AGENDA

10:00 Conference Welcome

10:05 **KEYNOTE ADDRESS**
National Counterintelligence and Security Center (NCSC) and
Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S))

10:15 **FIVE HABITS OF THE MASTER THINKER:** Thinking Skills for Security Professionals

11:15 Break

11:30 **THE PSYCHOLOGY OF PHISHING**

12:15 Break

12:45 **MENTAL HEALTH RESOURCES PANEL DISCUSSION**

13:45 Break

14:00 **HOW COUNTERING THE INSIDER THREAT RESULTED IN GOOD MENTAL HEALTH**

15:15 Conference Wrap Up

ATTENDEE PARTICIPATION

Screen tools

FILE SHARING

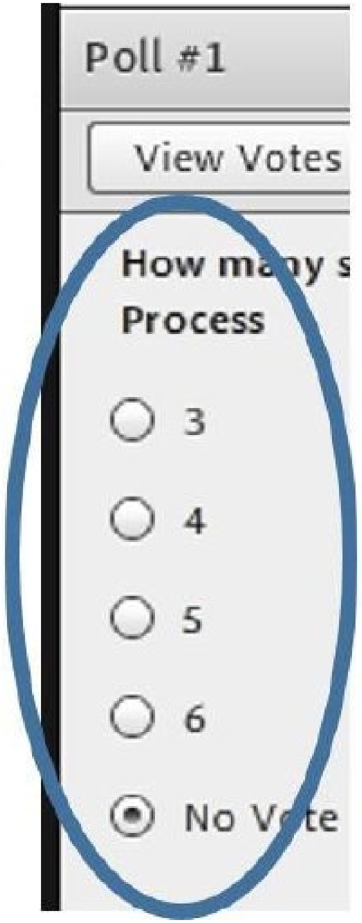
CLOSED CAPTIONING

ENLARGE WINDOW

Q&A

ATTENDEE PARTICIPATION

Polls, Chats, Feedback


Poll #1

View Votes

How many s
Process

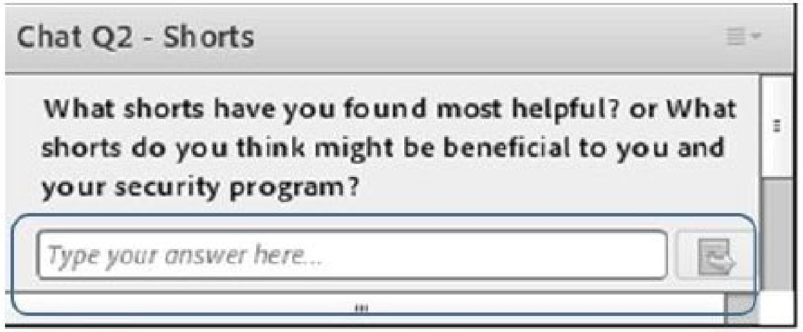
○ 3

○ 4

○ 5

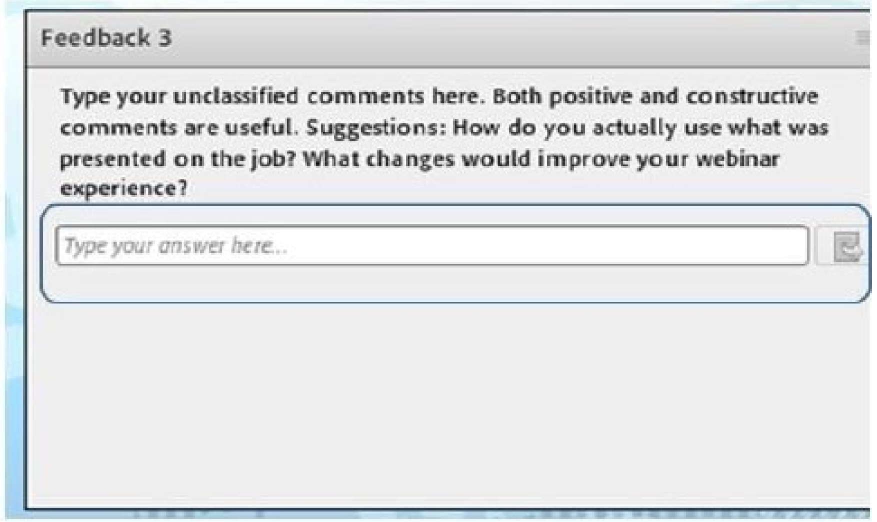
○ 6

● No Vote


Chat Q2 - Shorts

What shorts have you found most helpful? or What shorts do you think might be beneficial to you and your security program?

Type your answer here...


Feedback 3

Type your unclassified comments here. Both positive and constructive comments are useful. Suggestions: How do you actually use what was presented on the job? What changes would improve your webinar experience?

Type your answer here...

AUDIENCE POLL QUESTION #1

What time is it there?

a. 10:00 a.m.

b. 7:00 a.m.

c. 1:00 p.m.

d. Too early!

e. Too late!

KEYNOTE SPEAKER

Tara Jones

Deputy Director for Defense Intelligence (Counterintelligence, Law Enforcement & Security)
OUSD(I&S)

PRESENTATION

Five Habits of the Master Thinker

Thinking Skills for Security Professionals

Katherine Hibbs Pherson
CEO, Pherson Associates

Three Analytic Thinking Touchpoints

1. Fundamental **Concepts** of Analytic Thinking

2. Essential Tradecraft **Skills**
   - Mitigating Biases and Traps
   - Developing Conceptual Models
   - Understanding Probability
   - Questioning Misinformation and Flawed Argumentation

3. Five **Habits** of the Master Thinker

PHERSON

Fundamental Concepts of Analytic Thinking

PHERSON

Key Concepts to Understand Analytic Thinking

DATA: Greg Treverton -- ***Is our problem a puzzle or a mystery?***

- Can we simply collect and collate data, or do we need to engage in critical thinking?

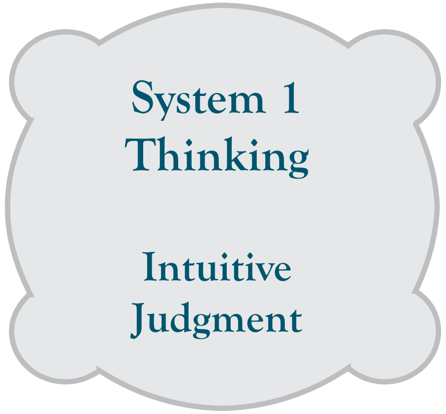
FRAMING: Gary Klein -- ***How do our brains help us with sensemaking?***

- Are we conscious of how our brains automatically fit data into a frame and fit the frame around the data?

REASONING: Daniel Kahneman -- ***Are we thinking fast and slow?***

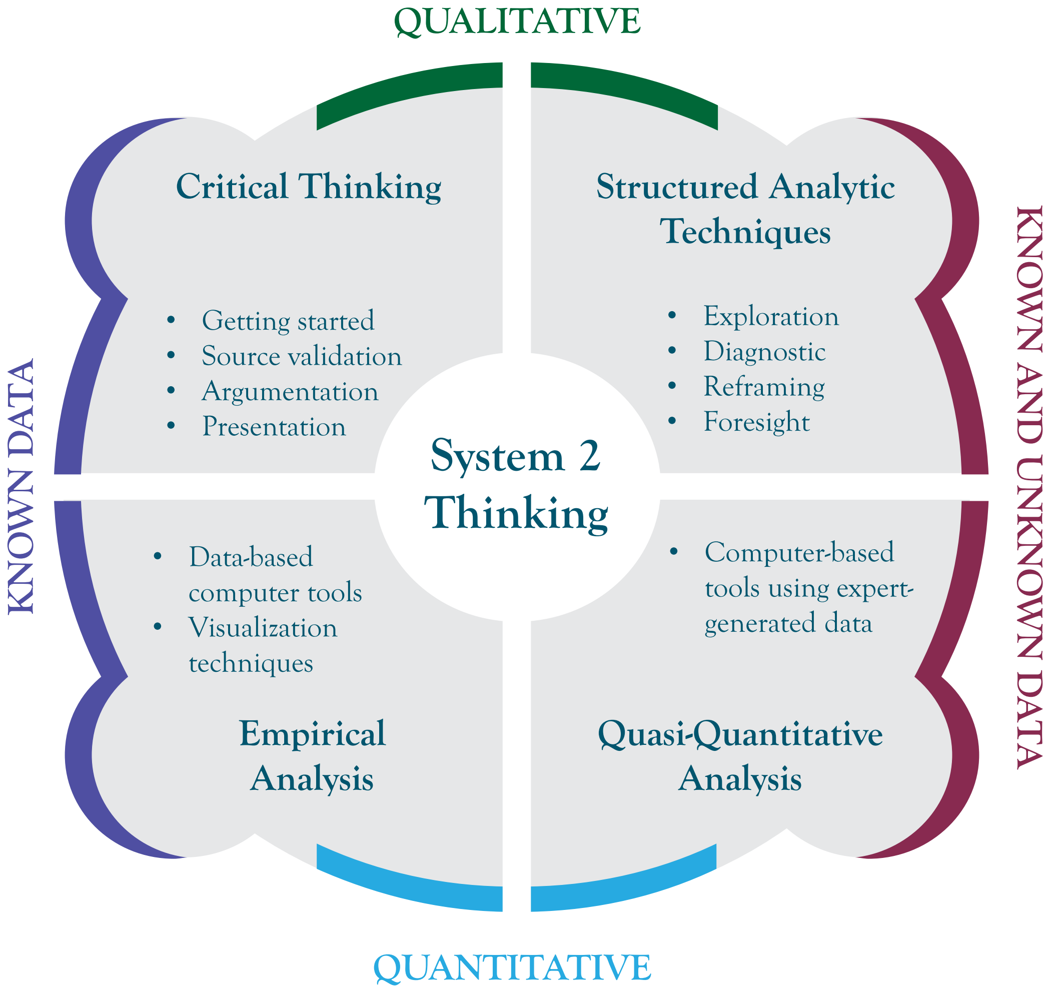
- How can we make the best use of **System 1 intuitive thinking** for efficiency and **System 2 deliberate reasoning** to mitigate bias and avoid errors?

Types of Analytic Approaches



System 1 Thinking

Intuitive Judgment



QUALITATIVE

KNOWN DATA

KNOWN AND UNKNOWN DATA

QUANTITATIVE

System 2 Thinking

Critical Thinking

- Getting started
- Source validation
- Argumentation
- Presentation

Structured Analytic Techniques

- Exploration
- Diagnostic
- Reframing
- Foresight

Empirical Analysis

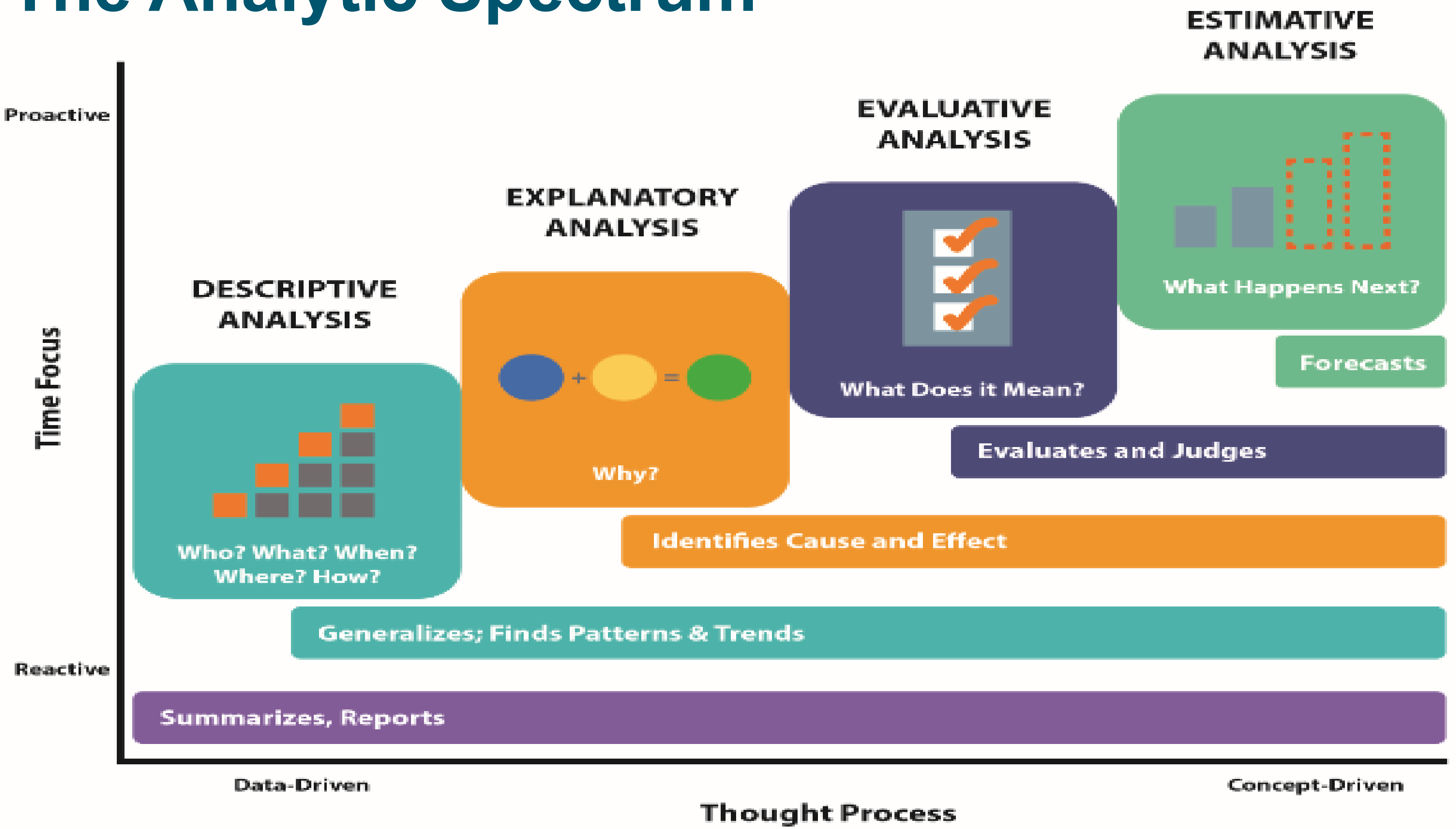
- Data-based computer tools
- Visualization techniques

Quasi-Quantitative Analysis

- Computer-based tools using expert-generated data

Source: Pherson, Katherine Hibbs and Randolph Pherson. *Critical Thinking for Strategic Intelligence, 3rd edition,* Thousand Oaks, CA: Sage Press, 2021.

The Analytic Spectrum

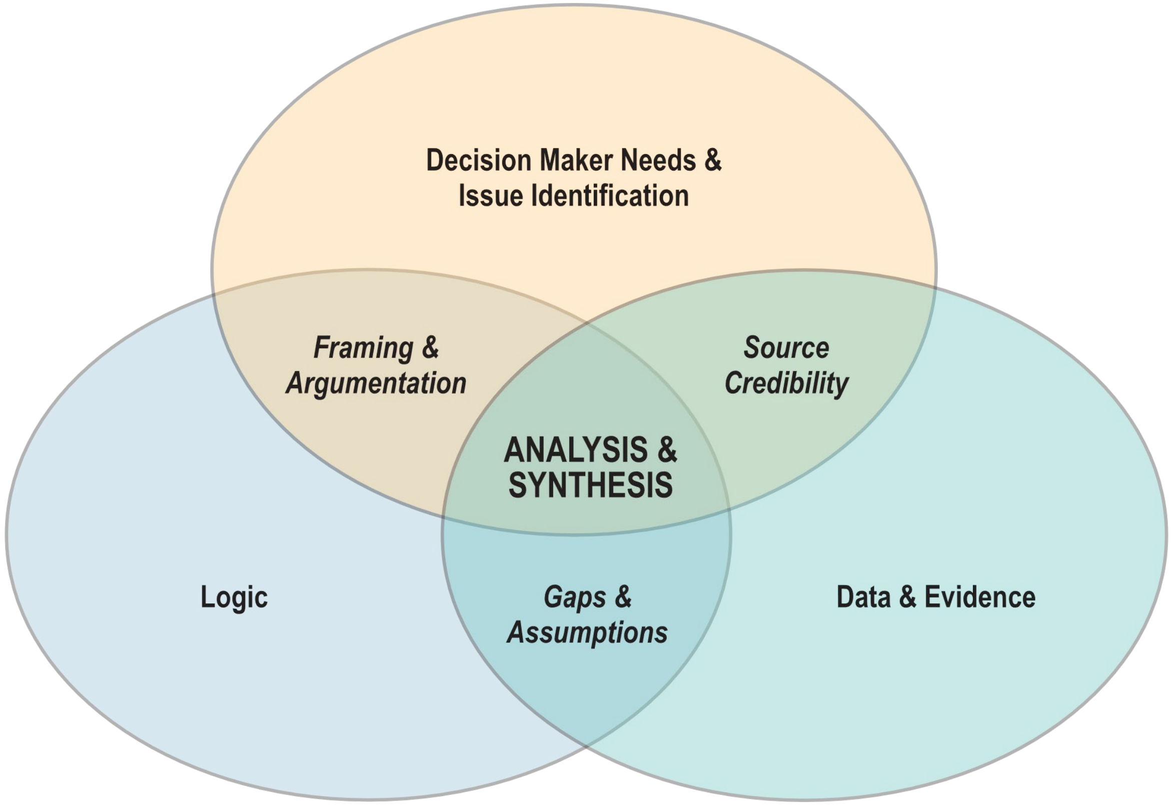


Source: Pherson, Katherine Hibbs and Randolph Pherson. *Critical Thinking for Strategic Intelligence, 3rd edition,* Thousand Oaks, CA: Sage Press, 2021.

How is Critical Thinking Defined?

Differing Definitions Can Guide Your Thinking

- Mental activity that is clear, precise, and purposeful.
- An ability to evaluate information and opinions in a systematic, purposeful, and efficient manner.
- The **adaptation of the processes and values of scientific inquiry** to the special circumstances of a world that is not scientific.



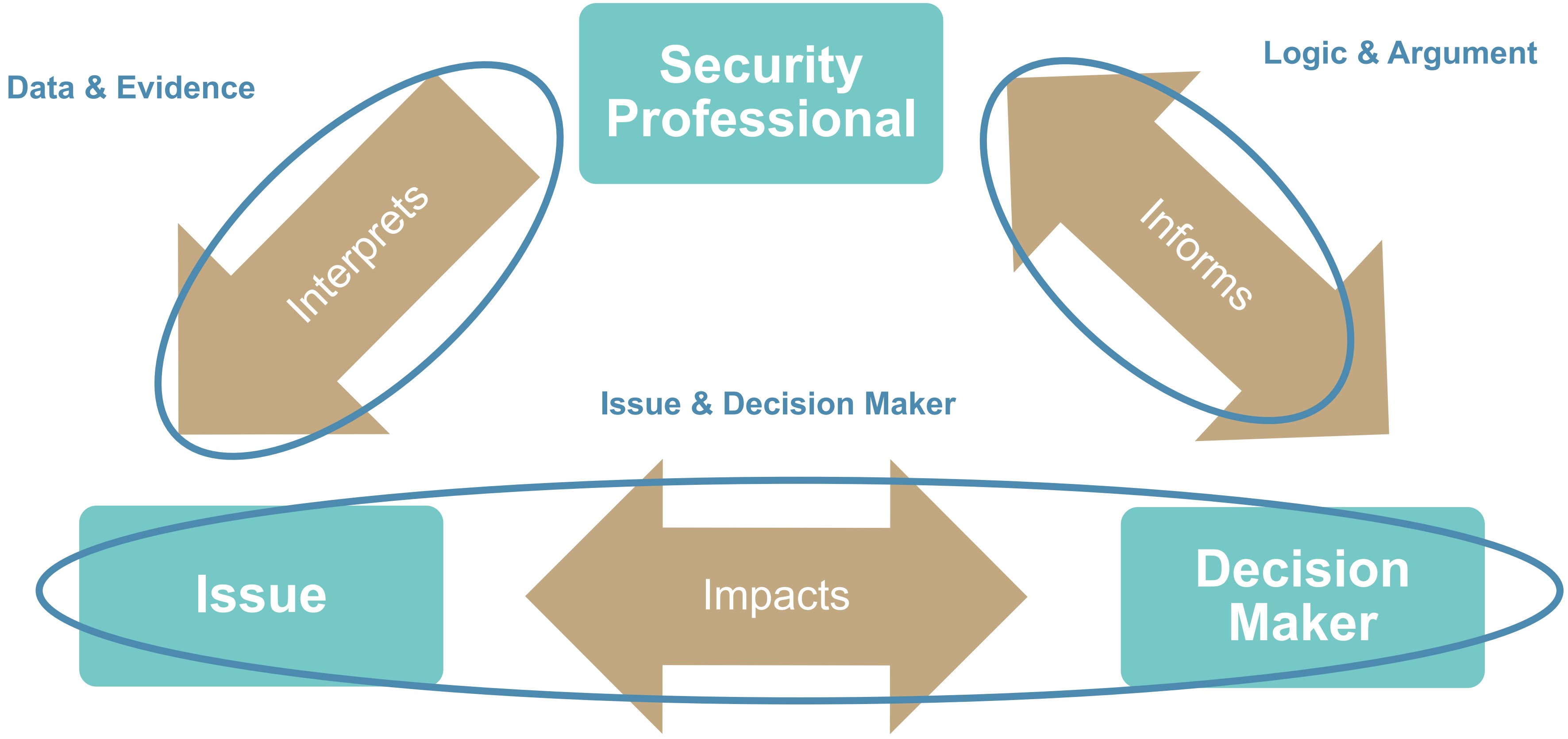
Source: Pherson, Katherine Hibbs and Randolph Pherson. *Critical Thinking for Strategic Intelligence, 3rd edition,* Thousand Oaks, CA: Sage Press, 2021.

The Eight Step Critical Thinking Process

- Ask the right **questions**
- Identify one's **assumptions**
- Reach out to **other sources**
- Evaluate the **data** for accuracy, relevance and completeness
- Assess the data and form **hypotheses**
- Evaluate the hypotheses; look for **conflicting data**
- Draw **conclusions**
- Present your **findings**

PHERSON

How Critical Thinking Fits into a Security Professional's Operating Environment



Source: Pherson, Katherine Hibbs and Randolph Pherson. *Critical Thinking for Strategic Intelligence, 3rd edition,* Thousand Oaks, CA: Sage Press, 2021.

Essential Tradecraft Skills

- Mitigating Biases and Intuitive Traps
- Developing Conceptual Models
- Understanding Probability
- Questioning Misinformation and Flawed Argumentation

PHERSON

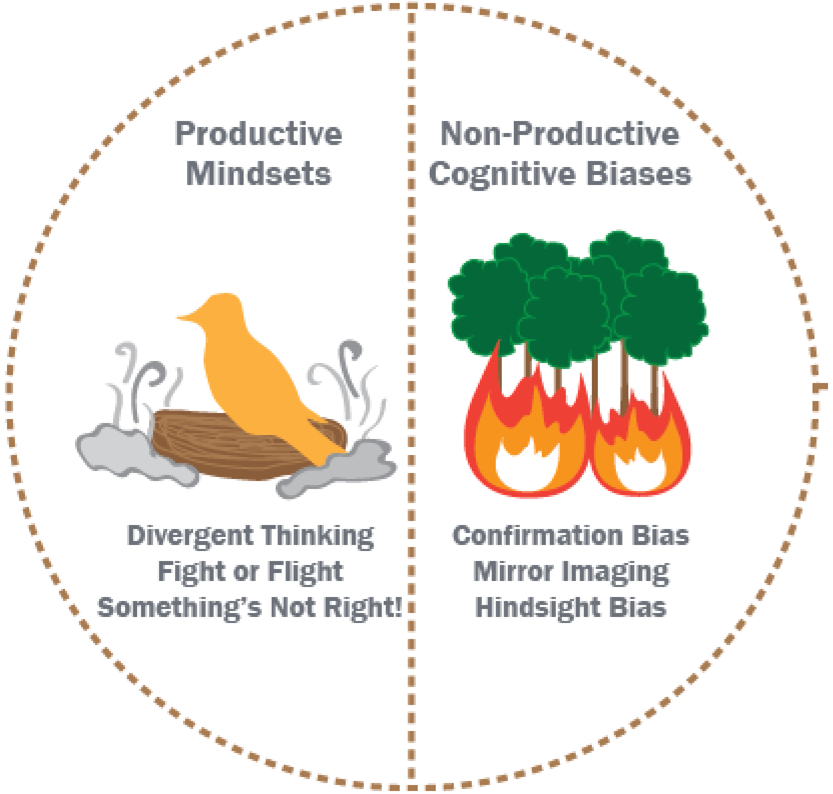
1. Mitigating Biases and Intuitive Traps

What is Cognitive Bias?

- Mental errors caused by our simplified information processing strategies
- Inherent thinking errors that people make in processing information

How you perceive data is strongly influenced by your:

- Past experiences
- Education
- Religion
- Nationality and cultural values
- Role requirements as a recipient of data



Cognitive biases prevent us from accurately understanding reality even when all the needed data and evidence that would form an accurate view is at hand.

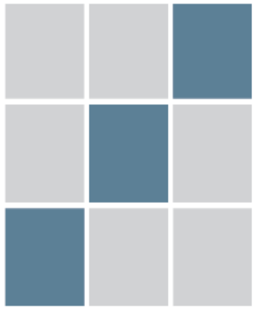
Cognitive Biases

KEY CHARACTERISTICS

Quick to form

Highly resistant to change

Information is made to fit into an existing conceptual framework



We don't see new patterns emerging

Initial, incorrect perceptions persist even after better information is available

We ignore or dismiss outlier data as noise

PHERSON

Misapplied Heuristics

Thinking Shortcuts Can Sometimes Cause Trouble!

Definition: Experience-based techniques or "rules of thumb" that can give a solution not guaranteed to be optimal

- The objective of a heuristic is to quickly produce a solution that is good enough to solve the problem at hand
- We can err by over-relying on or misapplying heuristics

These errors remain compelling even when one is fully aware of their nature. Awareness of the bias, by itself, does not produce a more accurate perception.

-- Richards J. Heuer Jr.

Inappropriately Used Heuristics

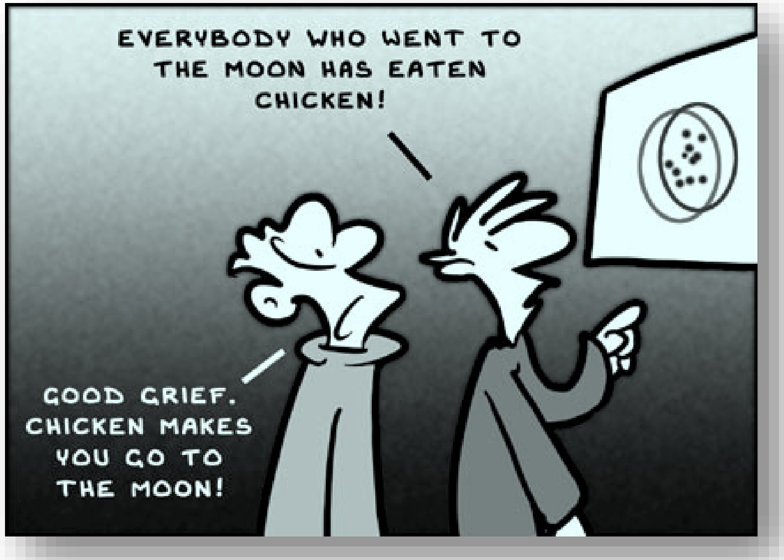
- Anchoring Effect
- Associative Memory
- Availability Heuristic
- Desire for Coherence and Uncertainty Reduction
- Groupthink
- Mental Shotgun
- Premature Closure
- Satisficing

PHERSON

Intuitive Traps

A New Category of Potential Pitfalls

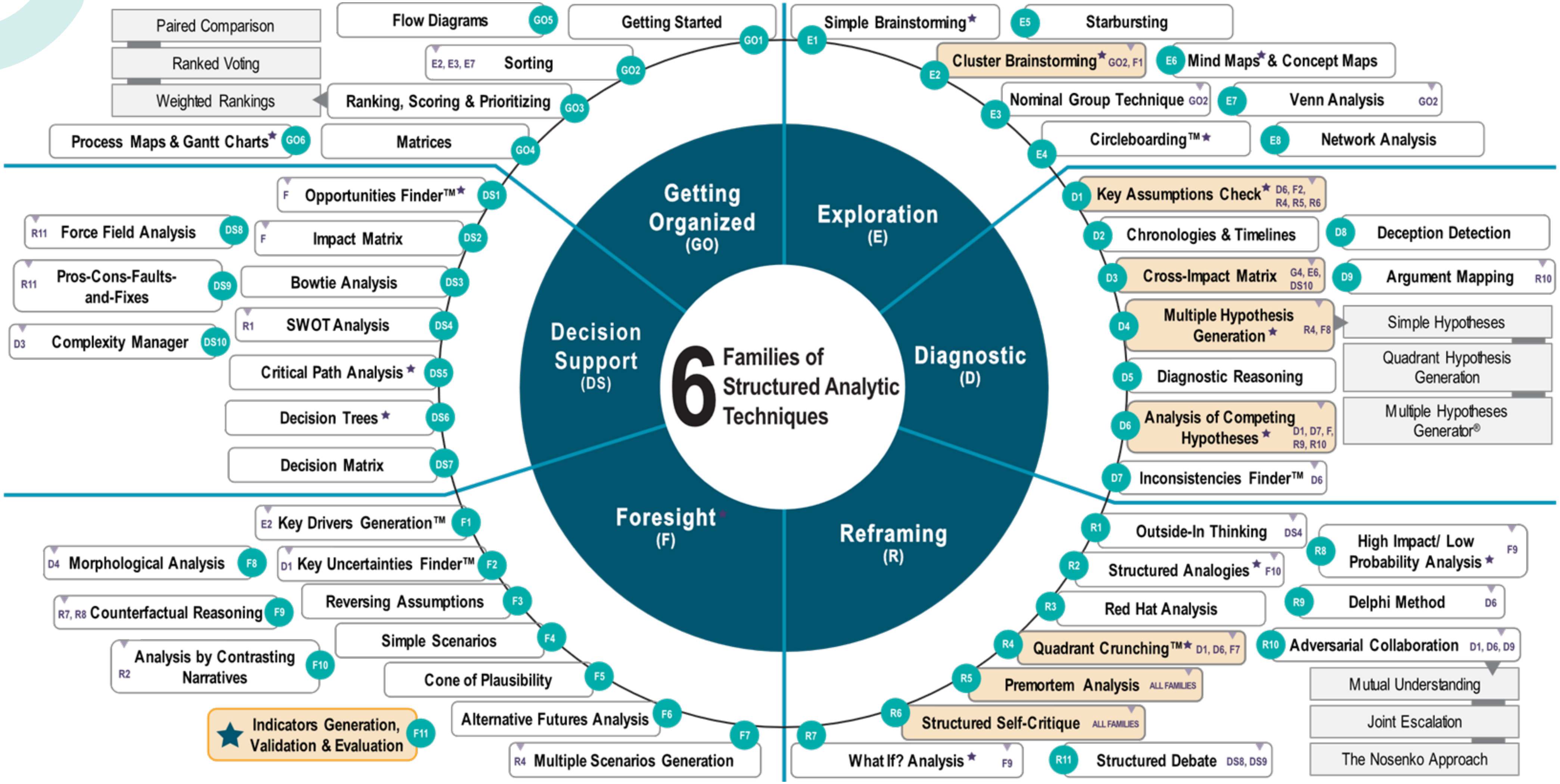
- Intuitive Traps are thinking errors that are manifestations of commonly recognized cognitive biases
- We often fall victim to these as we go about our daily lives, both personally and professionally
- Academics and theorists strenuously take steps to avoid these through systematic methods and peer reviews


EVERYBODY WHO WENT TO THE MOON HAS EATEN CHICKEN!
GOOD GRIEF. CHICKEN MAKES YOU GO TO THE MOON!

Most Common Intuitive Traps

- Favoring Firsthand Information
- Ignoring Inconsistent Evidence
- Ignoring the Absence of Information
- Projecting Past Experience
- Presuming Patterns
- Lacking Sufficient “Bins”
- Over-interpreting Small Samples
- Confusing Correlation with Causality
- Expecting Marginal Change

Taxonomy of Structured Analytic Techniques



6 Families of Structured Analytic Techniques

Getting Organized (GO)

- Paired Comparison
- Ranked Voting
- Weighted Rankings
- Flow Diagrams GO5
- Getting Started GO1
- E2, E3, E7 Sorting GO2
- Ranking, Scoring & Prioritizing GO3
- Process Maps & Gantt Charts★ GO6
- Matrices GO4

Exploration (E)

- E1 Simple Brainstorming★
- E5 Starbursting
- E2 Cluster Brainstorming★ GO2, F1
- E6 Mind Maps★ & Concept Maps
- E3 Nominal Group Technique GO2
- E7 Venn Analysis GO2
- E4 Circleboarding™★
- E8 Network Analysis

Diagnostic (D)

- D1 Key Assumptions Check★ D6, F2, R4, R5, R6
- D2 Chronologies & Timelines
- D8 Deception Detection
- D3 Cross-Impact Matrix G4, E6, DS10
- D9 Argument Mapping R10
- D4 Multiple Hypothesis Generation★ R4, F8
  - Simple Hypotheses
  - Quadrant Hypothesis Generation
  - Multiple Hypotheses Generator®
- D5 Diagnostic Reasoning
- D6 Analysis of Competing Hypotheses★ D1, D7, F, R9, R10
- D7 Inconsistencies Finder™ D6

Reframing (R)

- R1 Outside-In Thinking DS4
- R8 High Impact/ Low Probability Analysis★ F9
- R2 Structured Analogies★ F10
- R3 Red Hat Analysis
- R9 Delphi Method D6
- R4 Quadrant Crunching™★ D1, D6, F7
- R10 Adversarial Collaboration D1, D6, D9
  - Mutual Understanding
  - Joint Escalation
  - The Nosenko Approach
- R5 Premortem Analysis ALL FAMILIES
- R6 Structured Self-Critique ALL FAMILIES
- R7 What If? Analysis★ F9
- R11 Structured Debate DS8, DS9

Foresight★ (F)

- E2 Key Drivers Generation™ F1
- D4 Morphological Analysis F8
- D1 Key Uncertainties Finder™ F2
- Reversing Assumptions F3
- R7, R8 Counterfactual Reasoning F9
- Simple Scenarios F4
- R2 Analysis by Contrasting Narratives F10
- Cone of Plausibility F5
- ★ Indicators Generation, Validation & Evaluation F11
- Alternative Futures Analysis F6
- R4 Multiple Scenarios Generation F7

Decision Support (DS)

- F Opportunities Finder™★ DS1
- R11 Force Field Analysis DS8
- F Impact Matrix DS2
- R11 Pros-Cons-Faults-and-Fixes DS9
- Bowtie Analysis DS3
- R1 SWOT Analysis DS4
- D3 Complexity Manager DS10
- Critical Path Analysis★ DS5
- Decision Trees★ DS6
- Decision Matrix DS7

PHERSON

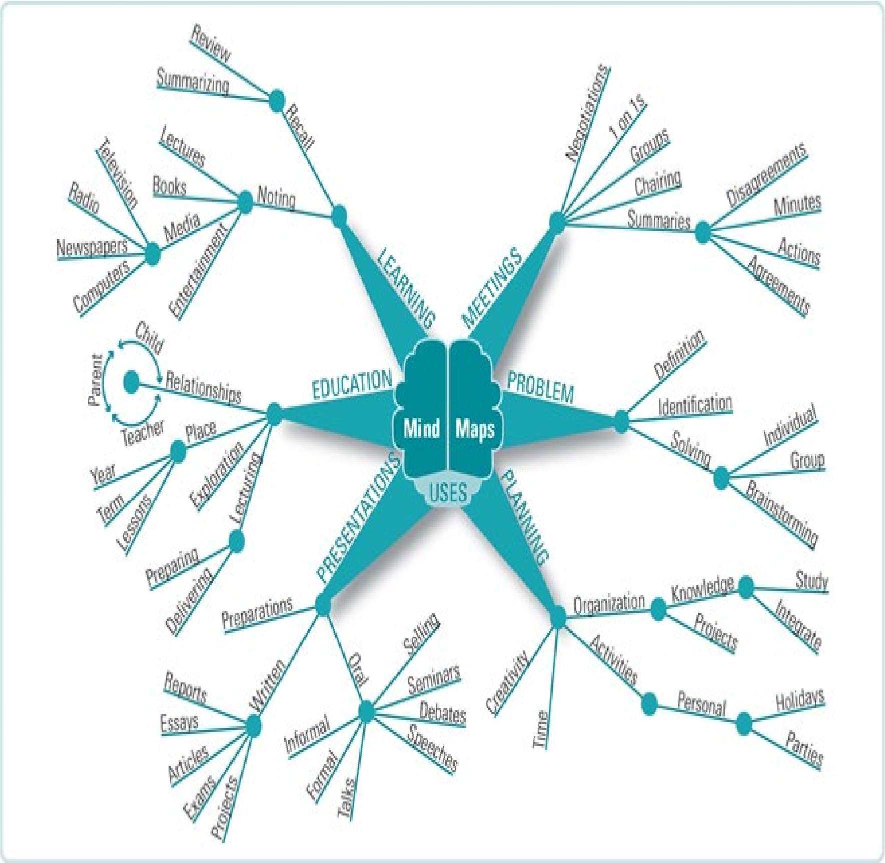
Use SATs for Strategy and Action

Structured Thinking enables awareness by avoiding Misapplied Heuristics and Intuitive Traps

- Provides some distance from your own intuitive reactions with System 2 thinking
- Facilitates explicit identification of your personal perspectives, separating your opinions and assumptions from the observables and facts at hand
- Forces you to consider multiple possibilities and explanations for what might be unknown or unfamiliar, including a “bin” for options you have not generated
- Enables you to think in terms of axes and combinations of variables
- Minimizes errors in judgment or action
- Promotes transparency and therefore collaboration
- Guides you with steps and processes when you might not be certain how to proceed

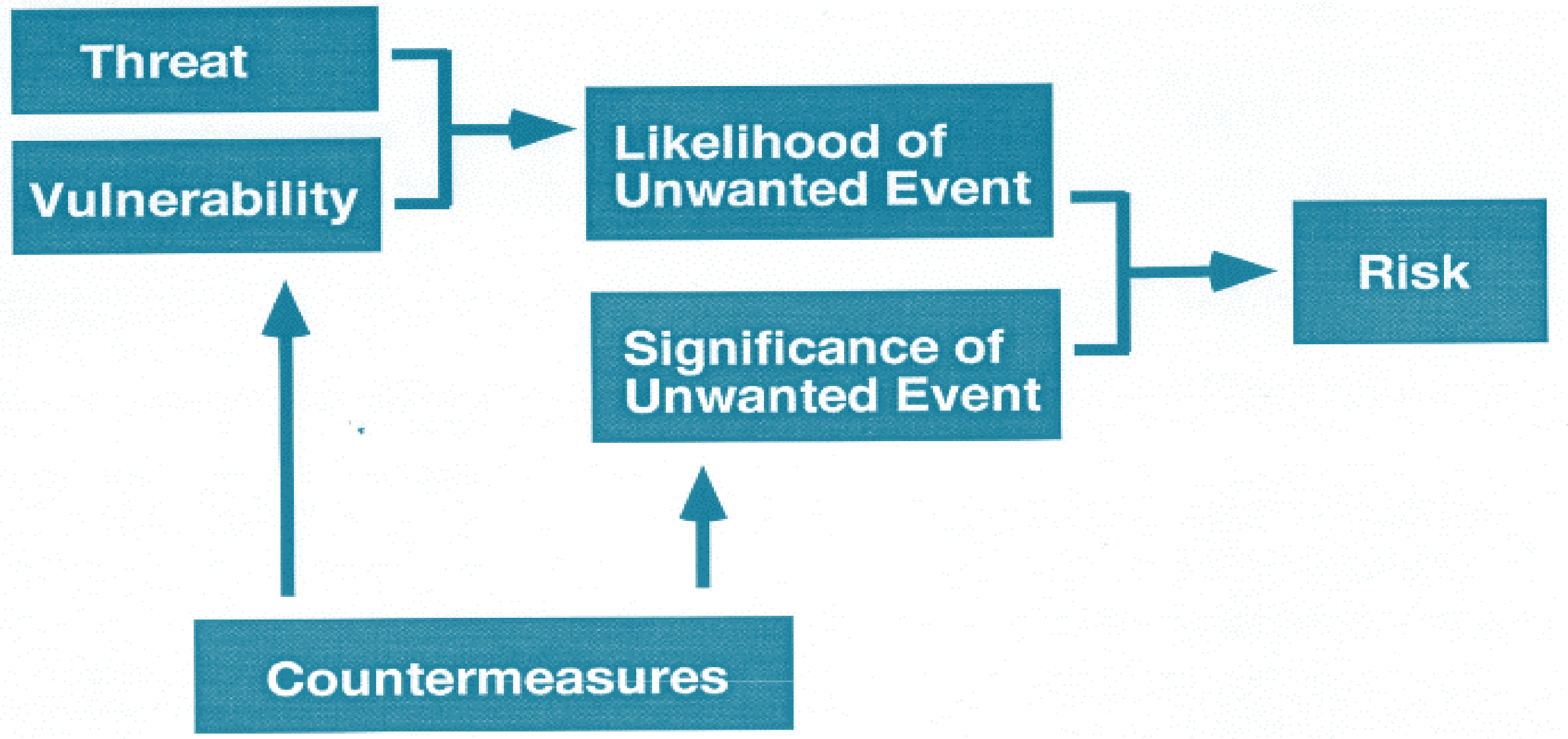
2. Leveraging Your Unconscious Framing Capability to Create Deliberate Models

- Define your problem or question using triggering aids such as the **5Ws and an H and STEMPLES+** to energize your **Brainstorming**
- Identify the **component parts** of your issue—this is the very definition of analysis—and make them as **Mutually Exclusive and Comprehensively Exhaustive (MECE)** as possible
- Examine your **assumptions**
- What are the **relationships and patterns** among the actors and factors? Which are **dynamic and changing**?
- Are there historical or substantive **analogies**? What are the **similarities or differences**?
- Can you **draw** your model or use a Mindmapping application?

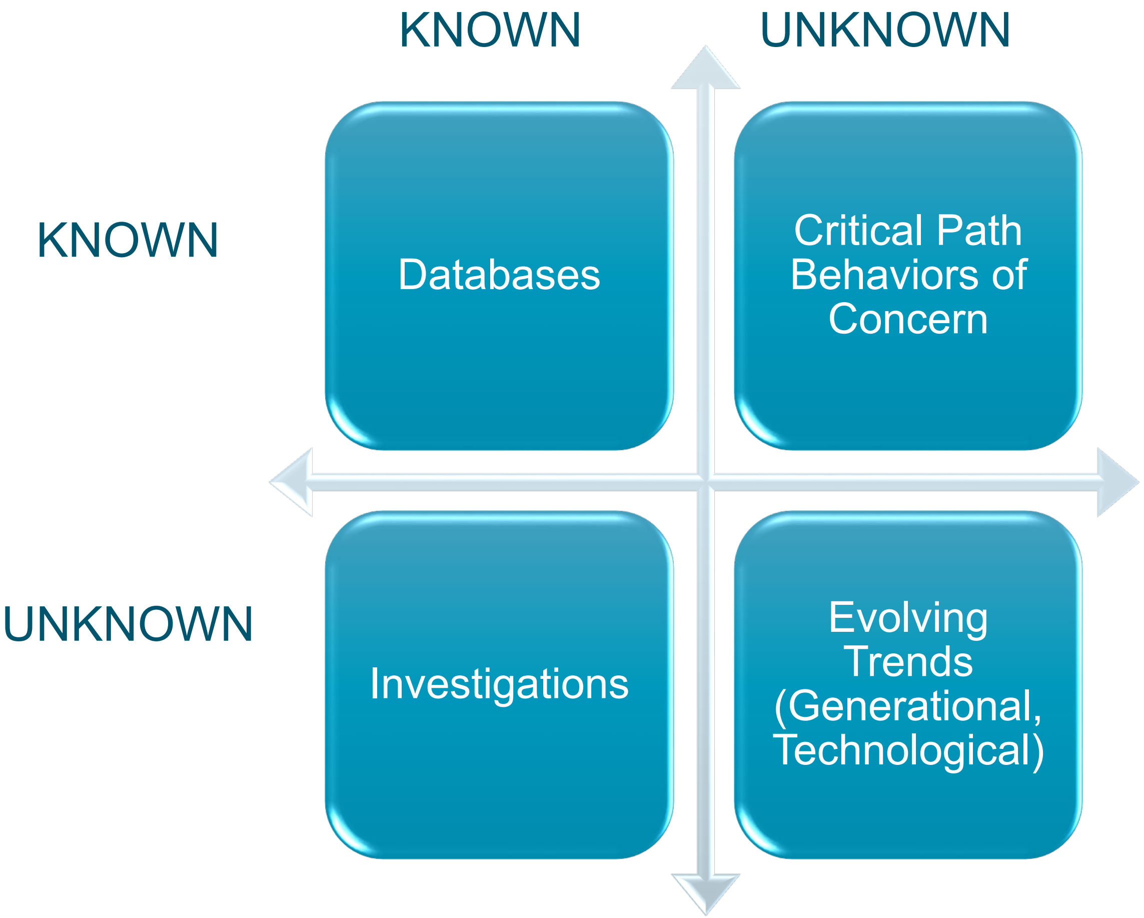


PHERSON

A Risk Management Model

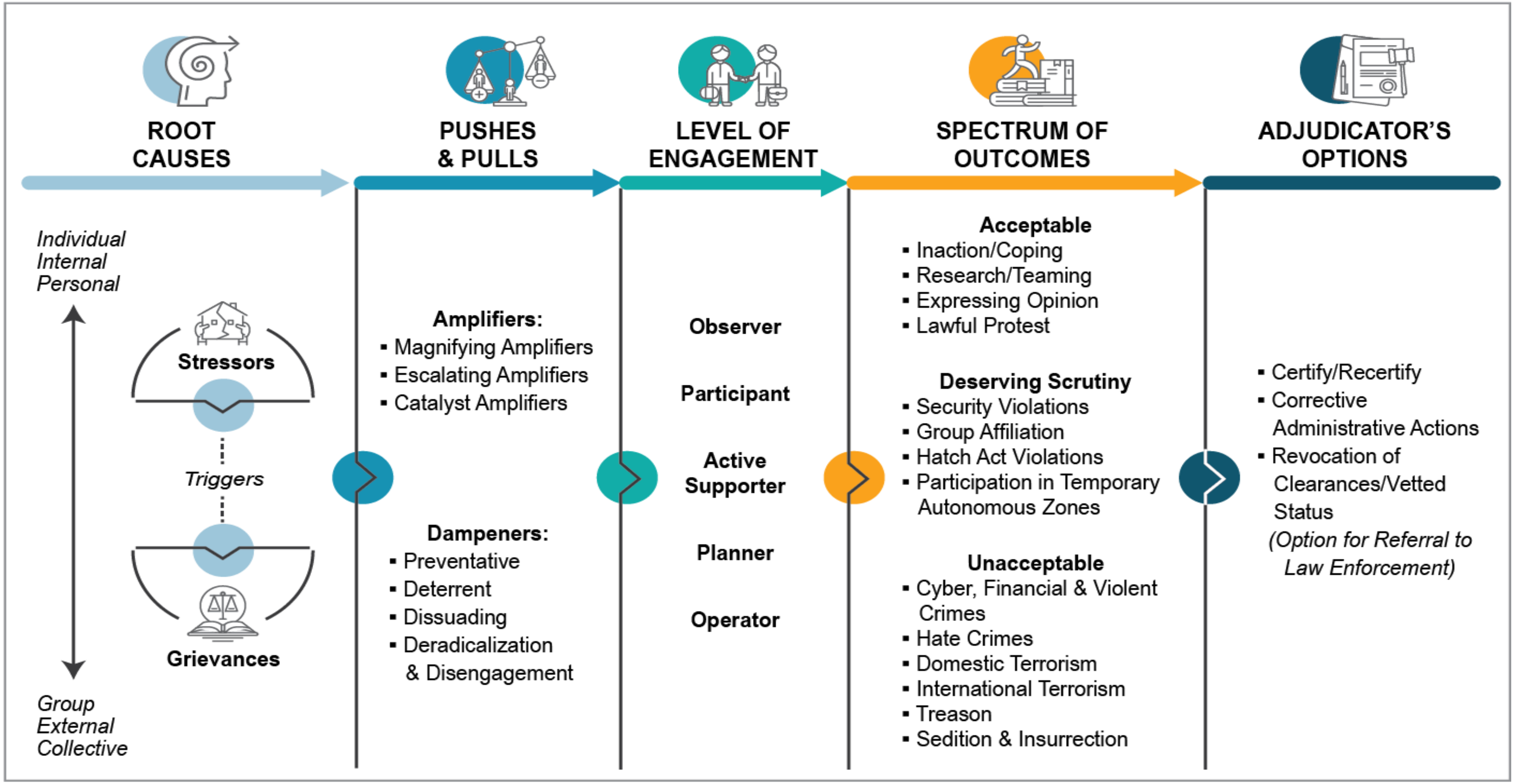


Categories of Personnel Vetting Information



	KNOWN	UNKNOWN
KNOWN	Databases	Critical Path Behaviors of Concern
UNKNOWN	Investigations	Evolving Trends (Generational, Technological)

Outside-In Personnel Vetting Model



ROOT CAUSES

Individual
Internal
Personal

Stressors

Triggers

Grievances

Group
External
Collective

PUSHES & PULLS

Amplifiers:

- Magnifying Amplifiers
- Escalating Amplifiers
- Catalyst Amplifiers

Dampeners:

- Preventative
- Deterrent
- Dissuading
- Deradicalization & Disengagement

LEVEL OF ENGAGEMENT

Observer

Participant

Active Supporter

Planner

Operator

SPECTRUM OF OUTCOMES

Acceptable

- Inaction/Coping
- Research/Teaming
- Expressing Opinion
- Lawful Protest

Deserving Scrutiny

- Security Violations
- Group Affiliation
- Hatch Act Violations
- Participation in Temporary Autonomous Zones

Unacceptable

- Cyber, Financial & Violent Crimes
- Hate Crimes
- Domestic Terrorism
- International Terrorism
- Treason
- Sedition & Insurrection

ADJUDICATOR'S OPTIONS

- Certify/Recertify
- Corrective Administrative Actions
- Revocation of Clearances/Vetted Status

(Option for Referral to Law Enforcement)

3. Understanding Probability

Humans Reason Poorly about Probability

- Intuitive and Complex Thinking are in different parts of the brain.
- **Intuition** is adept at matching and recognizing **patterns** but is quickly overwhelmed by uncertainty that requires assessing events in the context of all possible alternatives.
  - It falls back on **biased information** of what it already knows vs. what is really there.
  - **Vivid or incidental data** overrides crucial or knowable fact.
- **Probability** helps us calibrate our thinking about the unknown to best represent the world as it is and deal with the fact that our decisions will not always be right over the long term. It does this by:
  - Using **numeric values** to simulate order and what we do not know
  - Assuming we can discover regularity if we collate a **large enough sample of events over a long enough period of time.**
  - Helping **anticipate** outliers

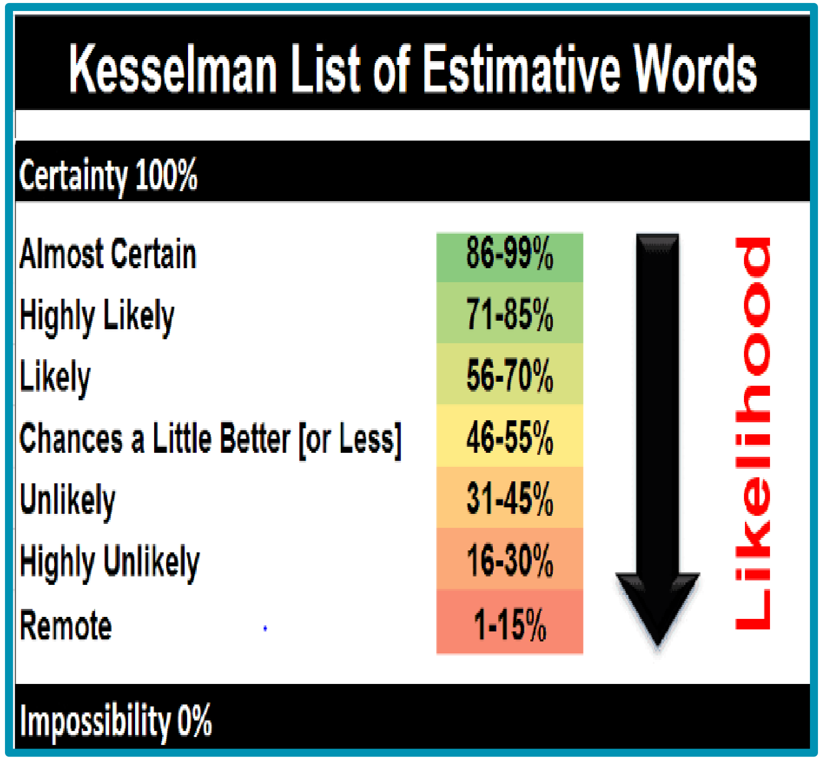
PHERSON

Common Traps in Expressing Probability

1. **Probabilistic Language** (likely, probably, we doubt)
   - Readers often interpret such language very differently
2. **Percentages** (1-100%)
   - Numbers usually imply a false sense of precision
3. **Percentage Range** (20-40%)
   - Analyst needs to establish reason for upper and lower limits
4. **Gamblers Scale** (1 in 3 chance)
   - Odds are effective in conveying risk to decisionmakers
5. **Defined Scale** (published spectrum for all products)
   - Readers must know the scale

Follow whatever approach you use with “**because**”!

> “We believe X is **highly likely** to occur **because** two necessary conditions are present, and a key driver is gaining strength.”



Kesselman List of Estimative Words

Certainty 100%	
Almost Certain	86-99%
Highly Likely	71-85%
Likely	56-70%
Chances a Little Better [or Less]	46-55%
Unlikely	31-45%
Highly Unlikely	16-30%
Remote	1-15%
Impossibility 0%	

Likelihood

Source: Rachel F. Kesselman, “Verbal Probability Expressions in NIEs,” (master’s thesis, Mercyhurst College, 2008).

Strategies that Enable Probability

1. Consciously employing **Structured Analytic Techniques** to mitigate cognitive weaknesses
   - Key Assumptions Check
   - Inconsistencies Finder™
   - Outside-In Thinking
   - Premortem Analysis
   - Red Hat Analysis
2. Incorporating **probability principles** into thinking processes
   - Law of Addition
   - Law of Multiplication
   - Multiple Factors
3. Practice **Calibration**
4. Establish **Base Rates** and monitor change

> “Probability is not about the odds, but about the belief in the existence of an alternative outcome, cause, or motive.”
>
> -- Nassim Nicholas Taleb
> *Fooled by Randomness* (2005)

4. Questioning Misinformation and Flawed Argumentation

Logical fallacies involve a faulty relationship between an argument's claim and its supporting facts or logic

- ***Circular Argument (Tautology):*** The claim or conclusion is part of the supporting argument
- ***Inadequate Sampling:*** The sample used as a measure is too small
- ***Hasty Generalization:*** General claims based on insufficient or unrepresentative evidence
- ***False Analogy:*** Argument supported with evidence that is not similar
- ***False Dichotomy:*** Set of possibilities is reduced to only two, misrepresenting the complexity
- ***Non Sequitur:*** Conclusion does not follow the premise
- ***Post Hoc, Ergo Propter Hoc ("after this because of this"):*** If one event preceded another, it much have caused the subsequent event to occur
- ***Slippery Slope:*** Relates first and last steps when intervening ones have not occurred
- ***Distraction (Red Herring):*** Brings irrelevant points to distract attention from the issue being argued
- ***Ad Hominem Argument:*** Targets the person making the argument rather than the argument
- ***Appeal to Authority:*** The opinion of a recognized expert is automatically seen as valid

Constructing Logical Arguments

Argument: A set of statements—one of which is the conclusion or claim—that are supported logically by other statements

- **Claim:** The assertion or point you are making
  - Based on reasonable evidence
  - Connected to observable facts
  - Characterized by clear, traceable, and fair thinking.
- **Reason:** How the evidence relates to the claim
- **Evidence:** Facts, data, and observations that support your reasons and claim
- **Assumption:** A belief that guides an analyst's interpretation of the evidence and underpins the reasoning and logic behind the argument

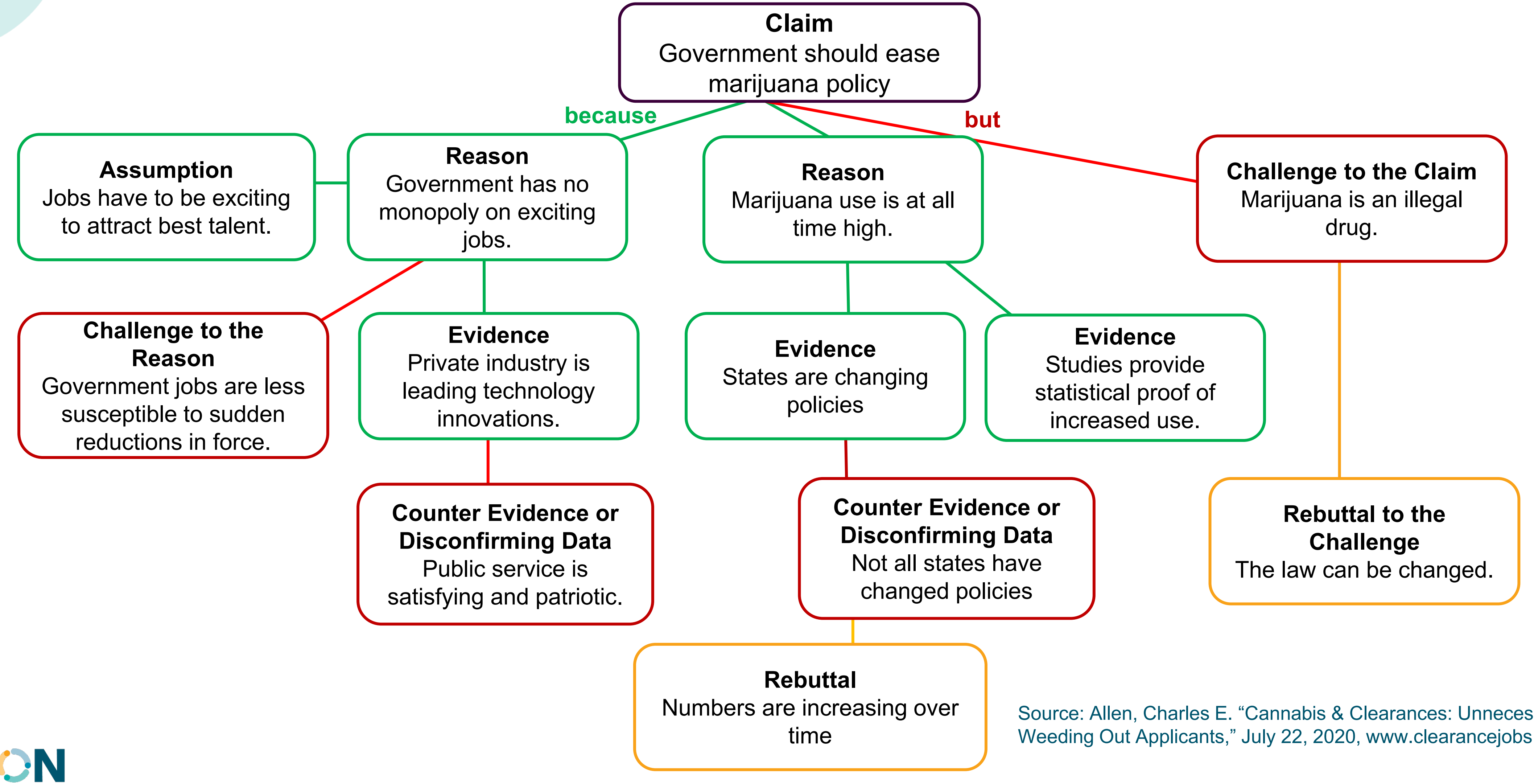
PHERSON

Building A Solid Analytic Argument

A good argument accounts in its reasoning for other views and differences

- Identify other lines of reasoning or **Alternative Hypotheses**
- Formulate an explanation – **Rebuttal** – why your argument with its claims, reasons, and evidence is stronger
- Revisit your claim, reasons, evidence, and assumptions, including alternate views or interpretations and, if possible, **indicators** of both your views and those of others
- Remove **emotionally laden terms** from your arguments and disregard them when evaluating those of others

Simplified Argument Map on Marijuana Policy

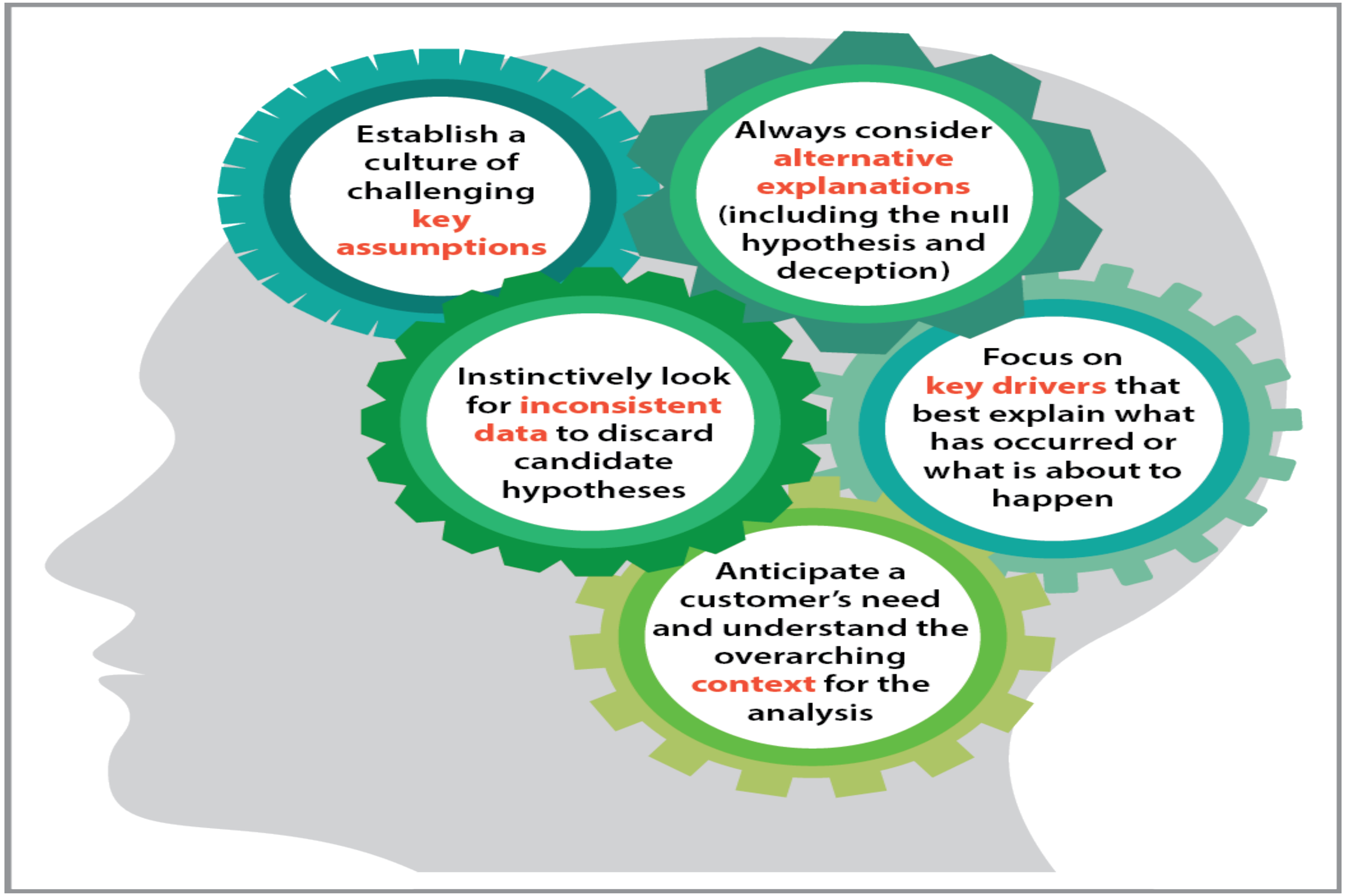

Claim
Government should ease marijuana policy
because
but
Assumption
Jobs have to be exciting to attract best talent.
Reason
Government has no monopoly on exciting jobs.
Reason
Marijuana use is at all time high.
Challenge to the Claim
Marijuana is an illegal drug.
Challenge to the Reason
Government jobs are less susceptible to sudden reductions in force.
Evidence
Private industry is leading technology innovations.
Evidence
States are changing policies
Evidence
Studies provide statistical proof of increased use.
Counter Evidence or Disconfirming Data
Public service is satisfying and patriotic.
Counter Evidence or Disconfirming Data
Not all states have changed policies
Rebuttal to the Challenge
The law can be changed.
Rebuttal
Numbers are increasing over time

Source: Allen, Charles E. “Cannabis & Clearances: Unnecessarily Weeding Out Applicants,” July 22, 2020, www.clearancejobs.com.

The Five Habits of the Master Thinker

PHERSON

Five Habits of the Master Thinker



Establish a culture of challenging **key assumptions**

Always consider **alternative explanations** (including the null hypothesis and deception)

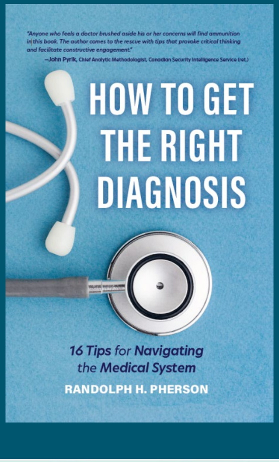
Instinctively look for **inconsistent data** to discard candidate hypotheses

Focus on **key drivers** that best explain what has occurred or what is about to happen

Anticipate a customer's need and understand the overarching **context** for the analysis

Source: Pherson, Randolph H., *"Five Habits of the Master Thinker,"* Journal of Strategic Security, Vol. 6, No. 3, Fall 2013.

Thank You!



"Anyone who feels a doctor brushed aside his or her concerns will find ammunition in this book. The author comes to the rescue with tips that provoke critical thinking and facilitate constructive engagement."
—John Pyrik, Chief Analytic Methodologist, Canadian Security Intelligence Service (ret.)

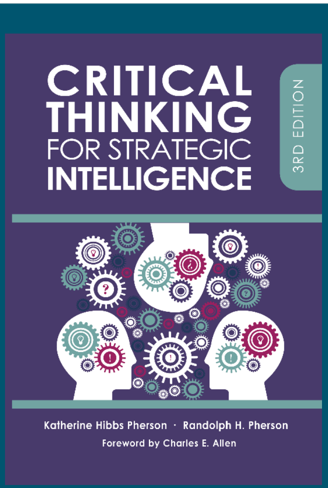
HOW TO GET THE RIGHT DIAGNOSIS

16 Tips for *Navigating the Medical System*

RANDOLPH H. PHERSON

STRUCTURED ANALYTIC TECHNIQUES
FOR INTELLIGENCE ANALYSIS

RICHARDS J. HEUER JR.
RANDOLPH H. PHERSON
FOREWORD BY JOHN McLAUGHLIN

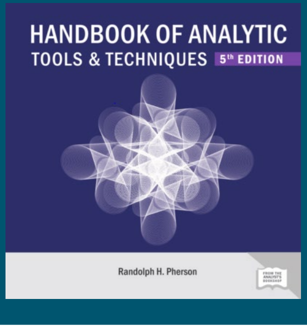


CRITICAL THINKING FOR STRATEGIC INTELLIGENCE

3RD EDITION

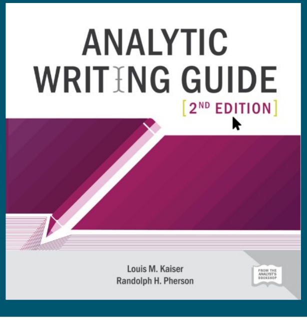
Katherine Hibbs Pherson · Randolph H. Pherson
Foreword by Charles E. Allen

ANALYST'S GUIDE TO INDICATORS



HANDBOOK OF ANALYTIC TOOLS & TECHNIQUES 5th EDITION

Randolph H. Pherson



ANALYTIC WRITING GUIDE
[2ND EDITION]

Louis M. Kaiser
Randolph H. Pherson

PHERSON

12110 Sunset Hills Road, #600
Reston, VA 20190

www.pherson.org
shop.globalytica.com

Katherine Hibbs Pherson, CEO
kpherson@pherson.org | 703.855.5540

BREAK

BREAK TIME

Please rejoin us at 11:30 a.m. ET

AUDIENCE POLL QUESTION #2

According to one industry threat report, what percentage of organizations experienced a successful email-based phishing attack in 2021?

a. 17%

b. 49%

c. 62%

d. 83%

PRESENTATION

The Psychology of Phishing

Ray Letteer

Deputy Director, Risk Management & Operational Integration Directorate, Department of Defense, Chief Information Officer, Cybersecurity

Background

- **Threat**: a circumstance or event with **potential to cause harm** to an information system in the form of **destruction, disclosure, and adverse modification of data and/or denial of service**.
  - **Natural/Environmental,** such as lightening, fire, hurricanes, tornadoes, or floods; poor building wiring or insufficient cooling for the systems
  - **Human**
    - **Unintentional,** such as human accident, bad habit, carelessness, or misinformation
    - **Intentional,** such as a human insider or outsider - a spy, hacker, criminal, cooperate raider, or disgruntled employee.
  - **Internal/External**
    - Attack vector is from either the inside or outside of the workforce and environment
    - External actors often take advantage of insiders’ mistakes, so an insider threat is frequently **the first part** of an outside attack.

From eavesdropping to mail tampering, criminals have always sought to **steal information** as a precursor to launching other exploits.

Situation: Genie out of the Bottle

Cyber Attacks

Ransomware

Information leaks from military, civilian, contractors and families affect mission readiness

"Loose lips sink ships;
Loose tweets sink fleets

Malicious/misguided efforts by military/civilian employees/ contractors

Improper Handling of Personally Identifiable Information(PII)/Controlled Unclassified Information (CUI)

Rogue Actors (Role Players/Interpreters)

Classified spillages/compromise

Internet predators

Lexicon

- **Cyber:** Connections, Communications, and Cognizance
- **Phishing**: using a “lure,” a more-or-less authentic-looking email or other form of communication, to catch or trick an unsuspecting user
- **Spear Phishing**: targeted to select group of people or a single individual
- **Whaling**: targeted at Senior Executives, CEOs, and other high-profile targets
- **Smishing**: derives from “SMS phishing.” Involves a deceptive text message rather than email.
- **Vishing**: short for "voice phishing," is when someone uses the phone to try to steal information.
- **Pharming**: a blend of “farming” and “phishing,” is when a victim gets malicious code installed on their computer, which sends the victim to a fake website designed to gather their login credentials.
- **Social Media Phishing**: attack executed through platforms like Instagram, LinkedIn, Facebook, or Twitter. The purpose of such an attack is to steal personal data or gain control of your social media account.

A **modern** twist to any number of age-old ploys to **trick people** into **giving up information** that can be used against them.

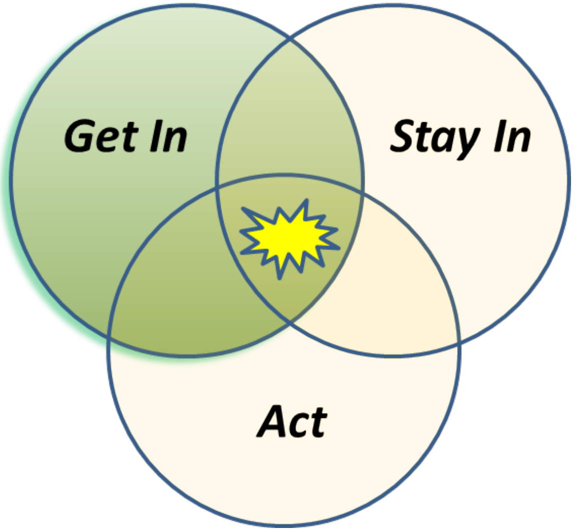
Understanding Phishing

- **Phishing** first used in 1996 to mean "…a scam by which an internet user is duped into revealing personal or confidential information which the scammer can use illicitly." The scammer can be **external** or **internal**.
  - Phishing is **deception through Cyber**.
  - Phishing emails use **emotional tactics** to get us to bypass logic—and **click the link**.
- Daniel Kahneman's model of two systems of thinking for humans.
  - **System 1** is fast, intuitive, and emotional…"automatic mode."
  - **System 2**, on the other hand, is slow and deliberate.
  - By appealing to our biases and emotions, **phishing tries to get us to stay in automatic mode: System 1**
- **External** actors often take advantage of **insiders**' mistakes, so an **insider threat** is frequently the **first part of an outside attack**.

Phishing emails frequently **manipulate** via mental shortcuts, also known as **heuristics**. Psychologist Robert Cialdini has identified seven "psychological principles of influence": authority, commitment, liking, perceptual contrast, reciprocation, scarcity, and social proof.

Strategy of the attack

- Attack components
  - **Obedience**: perceived Authority source, e.g., the Milgram experiment
  - **Urgency**: need to respond quickly, default to known or predictable pattern, e.g., System 1; make a decision under pressure
  - **Curiosity**: topic is of interest, e.g., “mistaken payroll email.”
- Adversary Objectives
  - **Get In**: Penetrate our networks
  - **Stay In**: Maintain a persistent presence
  - **Act**: Perform some form of attack (disrupt, deny, degrade, or destroy) or exploitation (data modification/exfiltration) based upon the **intent** of the adversary



By appealing to **biases and emotions**, phishing tries to get us to **stay in automatic mode**, aka System 1. Phishers want users to **make fast decisions, not a thoughtful ones**.

Way Ahead

- Many efforts to combat phishing involve deploying **technology-based** solutions and strategies; however, we need to understand **why** people fall for phishing and **how** to protect them from being duped.
- Interventions and anti-phishing solutions should **move from a one-size-fits-all** to a more **targeted approach.**
  - Training should be targeted to the **specific demographic**, to provide what is specifically need to know, then tied to **independent** assessments.
  - **Social Media** vectors should be included in training and awareness; "**evil twins.**"
  - Subsequent Red Team and Phishing assessments must have a **specific set of expected metrics** in mind to evaluate. Reduce the "gotcha" syndrome.
- Technology advances must be used, e.g., Zero Trust framework, to aid in reducing unverified accesses. However, in addition to technology, tap into the **expertise of psychology**, since the target is always the **human**.

While **technology** adapts and shifts quickly and frequently, **humans** don't

Usual reminders…

- For Government users, always **digitally sign** emails. Looks for the digital signature when receiving Government email.
- Have email sent and read in **Plain Text**. Rich Text Format (RTF) and HyperText Markup Language (HTML) may make signature look "fancy," but it hides the actual location of embedded hyper-links.
- Beware of emails or texts with "cut URLs"
- Beware of emails which ask for an urgent request or promise a reward for performing an action, even if it **appears legitimate** and from a **known address**. Approach it with **caution** and properly **vet the sender** before responding to it.
- It's human nature to **scan emails** when in "knee-jerk" **System 1 mode**. Counteract this tendency by prompting ourselves to **go into thoughtful, System 2 mode** with emails asking for important information (such as passwords or account numbers), request payments, or dangle freebies, especially downloads and say, "Wait a minute; let me double-check…"
- Beware of the "friends" and "social contacts" who reach out via **social media** with **no picture** or **inconsistent backgrounds**.

When in doubt…**don't click the link!!!**

LUNCH BREAK

LUNCH BREAK TIME

Please rejoin us at 12:45 p.m. ET

BREAK

Play During Lunch Break

Insider Threat Resilience Video:

https://www.dvidshub.net/video/811507/dcsa-cdse-insider-threat-awareness-resilience-psa

AUDIENCE POLL QUESTION #3

Did you catch the Resilience video during the lunch break?

a. No – I had to walk the dog

b. No – too hungry!

c. I wasn’t paying attention

d. Yes!

AUDIENCE POLL QUESTION #4

Mental Health includes which of the following?

a. Emotional well-being

b. Psychological well-being

c. Social well-being

d. All of the above

AUDIENCE POLL QUESTION #5

Does your organization have mental health resources available?

a. No

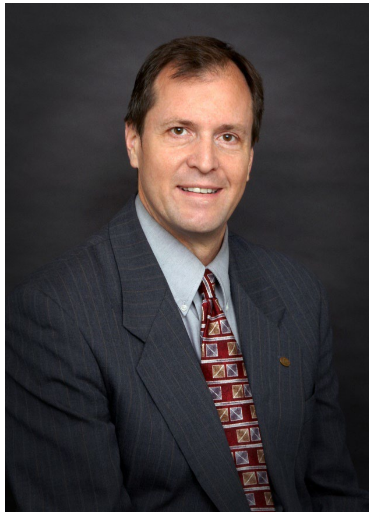
b. Maybe

c. Yes, but I don’t know much about them

d. Yes, but I wish there were more

e. Yes. I’ve utilized them

Mental Health Resources Panel Discussion

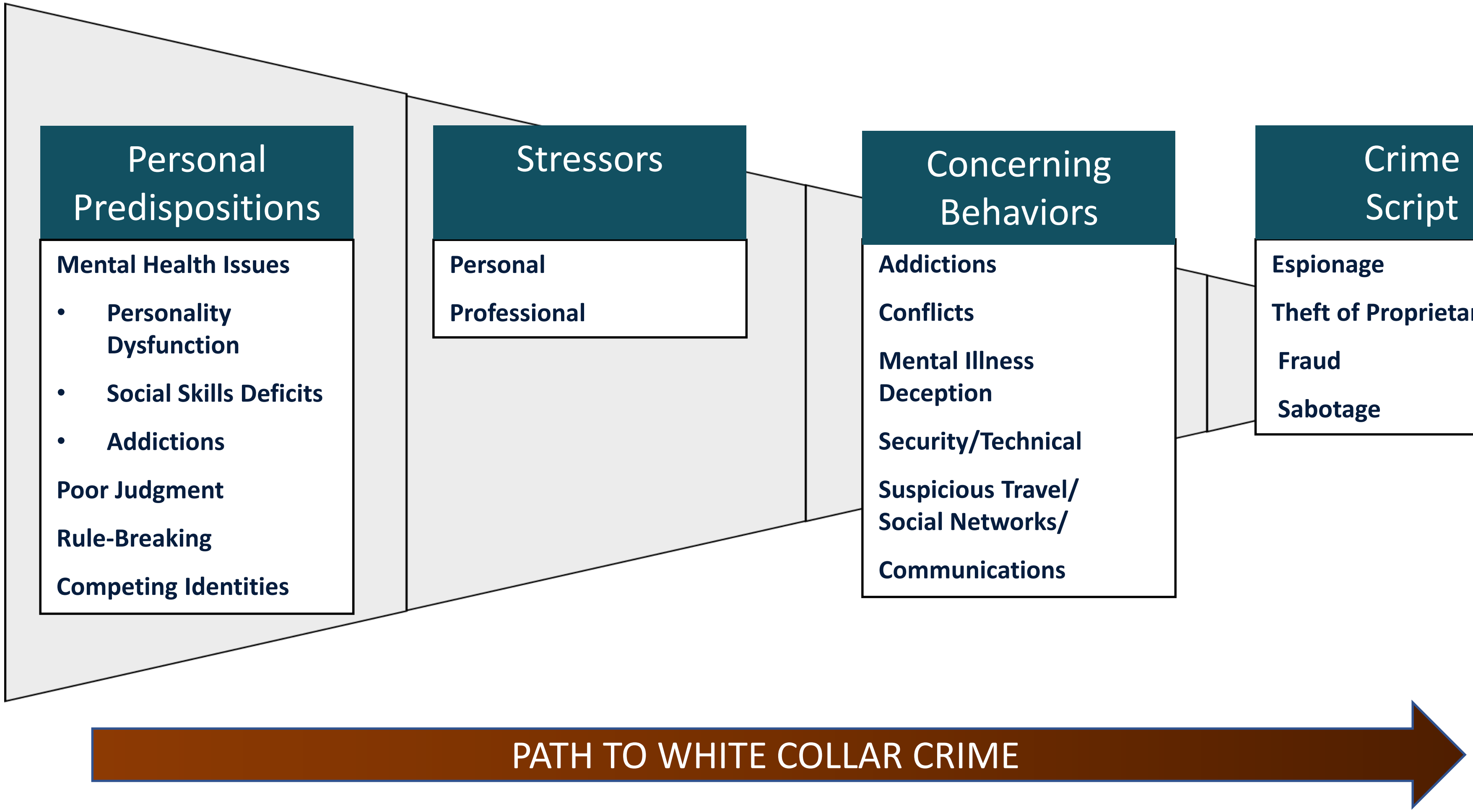


Dr. Kirk Kennedy
Clinical Psychologist, Peraton Inc.

Dr. Lindsay Braden
Senior Behavioral Advisor,
Defense Insider Threat Management Analysis Center

Michelle Aldana
Program Analyst,
Military Community and Family Policy, DOD

CRITICAL PATHWAY



Personal Predispositions

- Mental Health Issues
  - Personality Dysfunction
  - Social Skills Deficits
  - Addictions
- Poor Judgment
- Rule-Breaking
- Competing Identities

Stressors

- Personal
- Professional

Concerning Behaviors

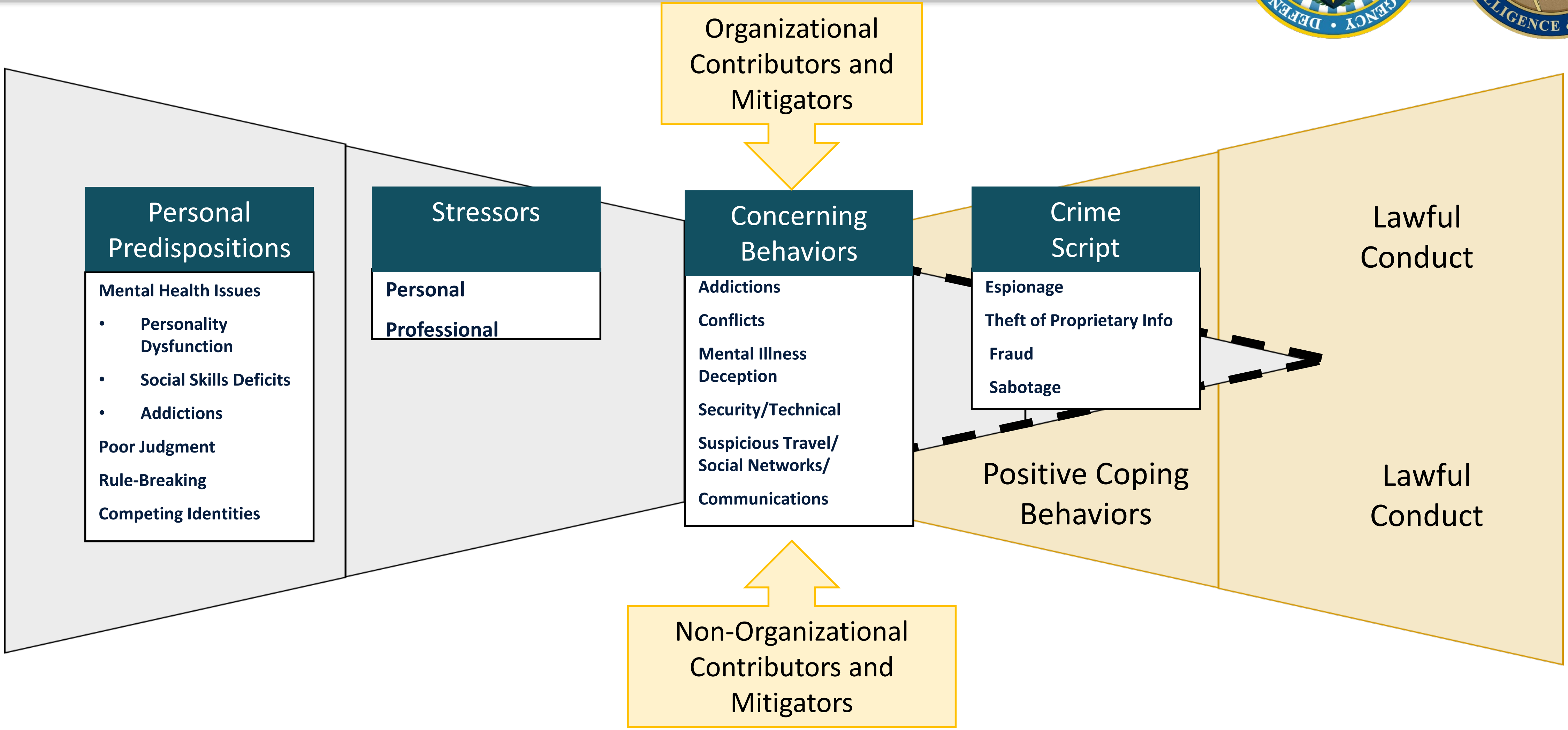
- Addictions
- Conflicts
- Mental Illness Deception
- Security/Technical
- Suspicious Travel/ Social Networks/
- Communications

Crime Script

- Espionage
- Theft of Proprietary Info
- Fraud
- Sabotage

PATH TO WHITE COLLAR CRIME

CRITICAL PATHWAY



Organizational Contributors and Mitigators

Personal Predispositions

- Mental Health Issues
  - Personality Dysfunction
  - Social Skills Deficits
  - Addictions
- Poor Judgment
- Rule-Breaking
- Competing Identities

Stressors

- Personal
- Professional

Concerning Behaviors

- Addictions
- Conflicts
- Mental Illness Deception
- Security/Technical
- Suspicious Travel/ Social Networks/
- Communications

Crime Script

- Espionage
- Theft of Proprietary Info
- Fraud
- Sabotage

Lawful Conduct

Positive Coping Behaviors

Lawful Conduct

Non-Organizational Contributors and Mitigators

BREAK

BREAK TIME

Please rejoin us at 2:00 p.m. ET

PRESENTATION

How Countering the Insider Threat Resulted in Good Mental Health

Lieutenant Martin "Marty" Thorp

Threat Management Unit, Office of Counter Insider Threat, National Geospatial-Intelligence Agency

Betsy Smith

Division Chief, Case Control, Office of Counter Insider Threat National Geospatial-Intelligence Agency

Video – NGA

We invite you to download and view NGA Video titled

“Show the Way”

located in the 2022 INT handout pod.

You may also view the video on YouTube at the below link:
https://www.youtube.com/watch?v=VZz5HBALMqE

Executive Order

- Presidential E.O. 13587 – establish an Insider Threat program
- Threat assessment w/in the intelligence community (IC)
  - Damage to facilities through sabotage
  - Protect against intelligence entities and attempts to breach Department of Defense (DoD) systems from both outside and potentially inside
  - Degradation of capabilities

Insider Threat Program w/in the IC and Dept of Defense

- Protect People
- Protect Facilities
- Protect Information Systems

How do you know what personnel are thinking?

Insider Threat and the TMU

Counter Insider Threat Office

- ➢Deploys computerized activity monitoring to detect specific threats for violence

  "Leakage"

Threat Management Unit (TMU)

- ➢ Focuses on:
  - ➢ the human threat
  - ➢ workplace violence
  - ➢ threats to self or others

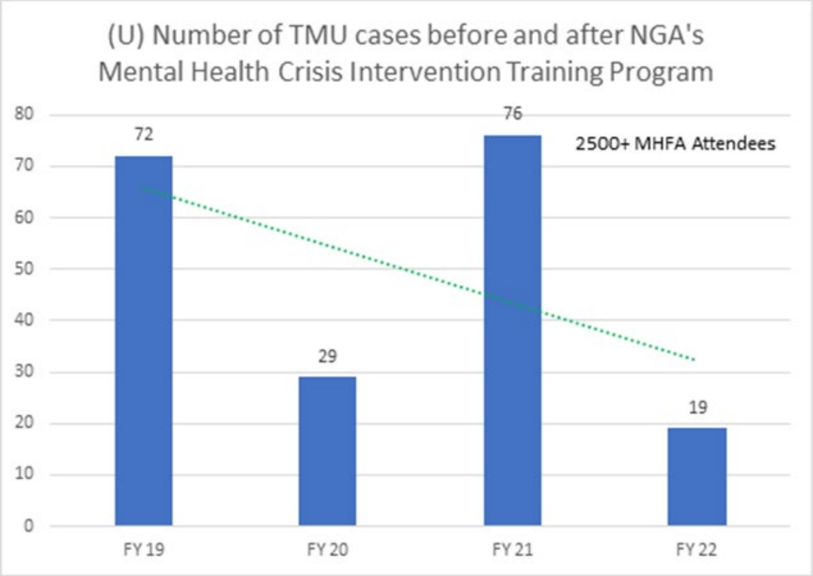
You are accessing a US Government IS provided for USG-authorized use only. By using this IS, you consent to:

- USG routinely intercepts and monitors communications
- At any time the USG may inspect and seize data stored on this IS
- Communications using or data stored on this IS are not private and are subject to routine monitoring

USG computers have login banner
Log into USG computer = consent to monitor

Unexpected Consequence

Looking for a Spy, Found Mental Health Concerns



Now at 3000+

Now at 80 (Aug 22)

Why Mental Health Training ?

Because mental illness . . .

- Affects a person's thinking, emotional state and behavior
- Disrupts the person's ability to
  - Work
  - Carry out daily activities
  - Engage in satisfying relationships
- Response to employee's needs

Source: Mental Health First Aid Instructor Manual Revised 2015

Why Mental Health Training ?

Our jobs demand the workforce to be at their mental peak

- Depression, anxiety, and psychosis are present
- Stressful jobs
- Products delivered to high ranking policy makers and the war fighter
  - Bad intelligence can lead to loss of a soldier’s life
  - An analyst suffering from a mental illness, even the most common such as depression or anxiety can lead to missed deadlines or a poor work product; their expertise is instrumental in what we do

American Adults with Mental Disorders Per Year

- Types of Mental Disorders

Type of Disorder - % Adults

Anxiety Disorder - 21.3%

Major Depressive Disorder - 7.1%

Substance Use Disorder – 7.6%

Bipolar – 1.8%

Schizophrenia (Psychosis) - .3%-06%

Eating Disorder - .05%-.44%

Any Mental Disorder – 18.5%

Who Can Benefit ?

- Useful for supervisors in helping identify an employee struggling with a mental health issue
- Useful for coworkers in helping identify someone struggling with a mental health issue
- Mental Health training became mandatory for all NGA police officers and Counter Insider Threat team members

NGA – A Microcosm of Society, but with Additional Stressors

- High number of NGA government, military and contract employees with military experience, many serving in combat zones
- Location: Worldwide
  - Other IC agencies, DoD facilities, U.S. Embassies, etc.
- Wounded Warrior Program – PTSD not unheard of

Who Can Benefit ?

- The Word Spread . . .
  - 3000+ trained
  - Outreach to CONUS and OCONUS personnel
  - Additional instructors – accommodating the increase

Benefit, Resiliency in the Workplace

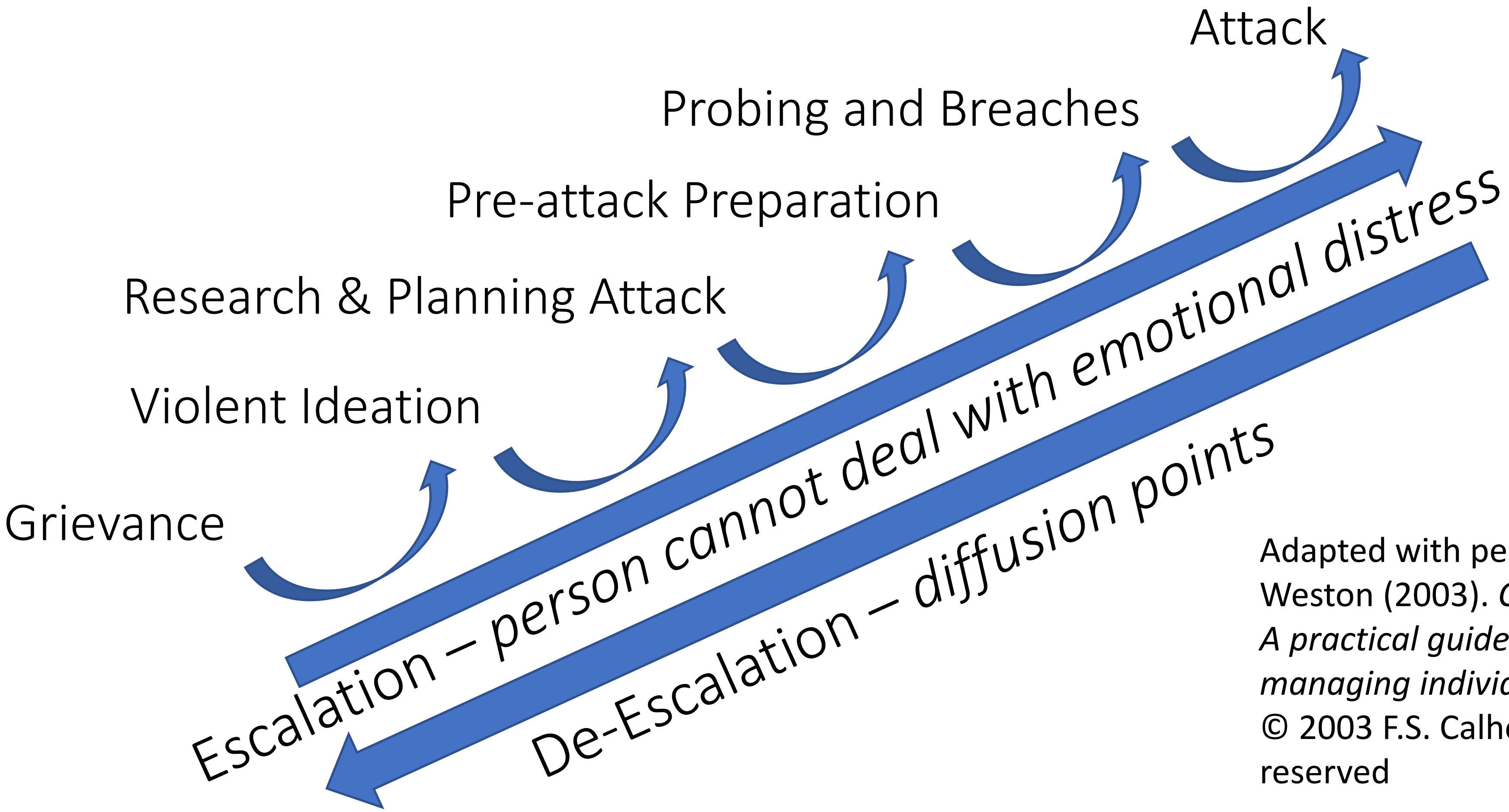
Approximately 24% of the U.S. population experiences a mental health issue each year. If you can get ahead of the curve and teach personnel how to become self-aware in recognizing burgeoning mental health disorders in themselves or others and get professional help before the problem becomes significant, your organization and people are stronger and better prepared for potential threats

How Does This Help Your Organization ?

Early Recognition = Early Intervention = Early Recovery

The individual gets treatment before the illness can become more entrenched, which in the worst case scenario, can lead to suicide

Get Ahead of the Curve


Attack
Probing and Breaches
Pre-attack Preparation
Research & Planning Attack
Violent Ideation
Grievance
Escalation – person cannot deal with emotional distress
De-Escalation – diffusion points

Adapted with permission from F.S. Calhoun and S.W. Weston (2003). *Contemporary threat management: A practical guide for identifying, assessing and managing individuals of violent intent*.

How Does This Help Your Insider Threat Program ?

- Destigmatize your program
  - class is viewed as enlightening and helpful
  - Threat Management ceases to be nebulous and scary
- When employees feel comfortable with you they are more likely to report suspicious behaviors or activities

Just because we teach mental health awareness does not mean we got out of the threat management business

How Does This Help Your Insider Threat Program ?

We have seen an increase in reporting of non-mental health referrals that can be directly related to teaching what to do in crisis during class – making the connect is important.

Good Mental Health is a Collaboration Within Your Organization

- Informed Business Partners
  - Working Groups: Force Protection, Leadership
  - Council Meetings: Supervisors, Instructors
  - Specialized Training/Mentoring
  - National Security Psychologists – Mental Health Status
  - Professional Development
  - Partnerships with Threat Assessment, Risk Assessment, Human Resources, Personnel Security, Inspector General, General Council

Good Mental Health is a Collaboration Outside Your Organization

- Informed Business Partners
  - Assoc. of Threat Assessment Professionals (ATAP)
  - Joint Analysis Center, St Louis
  - St Louis County Police Academy
  - Washington Council of Government (CoG) Joint Police Intelligence Committee
  - National Council for Mental Wellbeing
  - Law Enforcement, Crisis Intervention Training

Case Study 1: Possible Psychosis

- Loss of touch with reality

- *The most common complaint of an intelligence community officer experiencing a psychotic event . . .*

being followed by members of a foreign intelligence agency

Case Study 1: Possible Psychosis

- Employee staring at blank computer screen

  - Hears crackling
  - Sees files burning
    - “Can’t you see them? The flames?”
  - Work performance declining
  - Believes co-workers are hacking into computer
  - Behavioral change

does this sound familiar ?

Case Study 1: Possible Psychosis

- Female employee (28 years of service)
- Average work performer with declining performance
- Complained to supervisor co-workers were hacking into computer system, erasing her name from work and adding their names
- It’s summertime and employee is wearing a knee length overcoat
- Started asking for money from co-workers for breakfast and lunch

Case Study 1: Possible Psychosis
TMU Interview

- Complaint originated by supervisor.
- TMU interviewed employee – employee could not offer explanation for odd behavior
- Believed co-workers were hacking into her computer system
- TMU recommended EAP, she agreed
- Employee met with EAP counselor who provided referrals
- No suicidal ideations or thoughts of harming others
- Employee returned to work

Case Study 1: Possible Psychosis
TMU Interview

- Three days later, supervisor notified TMU of change in behavior
- TMU arrives. Employee was seated at her desk staring at a blank computer screen. TMU asked how things were going she pointed to the screen stating she can see her files burning and heard the crackling of the flames
- An assessment by the medical suite determined medical issues are present
- Employee agreed to be transported to the hospital by local EMS

Case Study 1: Possible Psychosis Results

- Employee treated and released from the hospital
- Employee provided diagnosis of serious medical condition and mental health disorder
- Employee had enough service years and elected to retire

Case Study 2: Potential for Violent Behavior ?
The Report

- Male employee (15 years of service)
- Retired Disabled Military Veteran
- Numerous deployment tours overseas
- Work performance started to decline
- Was becoming increasingly loud, boisterous, and disruptive in the workplace
- Employees including his supervisor believe he could be the next active shooter because he claimed to have PTSD

Case Study 2: Potential for Violent Behavior ?
TMU Interview

- Likes his job
- Diagnosed in early 2000's with head injury (TBI)
- Frequent headaches - Constant ringing causing hearing in both ears to diminish
- Single – primary care giver and only child for his mother who lost her battle with cancer several months prior
- No suicidal ideations or thoughts about harming himself or others
- Unaware he was being loud causing a disruption with his co-workers

Case Study 2: Potential for Violent Behavior ?
TMU Interview

- TMU suggests employee return to VA regarding his medical condition
- TMU recommended Employees Assistance Program (EAP) who could help with referrals to help him deal with the stressors of his medical condition and the recent loss of his mother
- TMU follows up with the supervisor. Behavior is a result of declining medical condition
- TMU assesses he is not a threat to self or others

Case Study 2: Potential for Violent Behavior ? Update

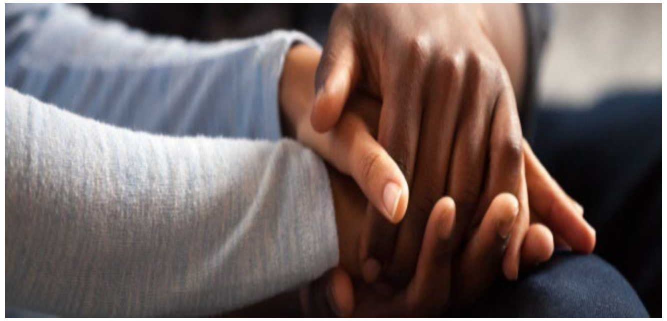
- Contacted VA who reopened his disability claim, and the VA determined he has PTSD and updated his disability – VA made his claim retroactive to the early 2000s resulting in financial compensation
- He is receiving treatment for his headaches and hearing issues
- EAP referred him to a counselor to assist with his stressors

As Employers, we invest a lot of time and money in our employees

- People can and do recover = resiliency
- Employees face unique challenges
- TMU has a high number of reports
  - personnel are confident they will be helped
  - people share their stories
- Mental Health Crisis Intervention Training (MHCIT) works well
  - covers all employees
  - easy to understand guidance
  - good tools to work with in and outside work

How does this help your organization ? Feedback

"I wanted to thank you for your class on Mental Health First Aid. Literally, two days after taking your class I had a friend who had a mental health break down. With the understanding and tools you gave me I was able to save my friend's life. I couldn't be more thankful than that. My friend will be released from the hospital later today and he is a completely a different person after getting the help he needed. Again, THANK YOU"



How does this help your organization ?
Feedback

"My best friend was experiencing suicidal ideations. After attending the class, I knew immediately what to do. I drove him to the hospital where he got help. He is here today because of what I learned in Mental Health training. "

"I never thought I would use what you taught us, but just last week I was able to help my niece who was going through a mental health issue that I would not have understood prior to your training."

How does this help your organization ? Feedback

"Three of my employees were talking about suicide. I attended Mental Health training and had the courage to immediately get help for them. Thank you. They are experts who just need help."- Manager

"'EVERYONE' in the agency should attend this class."

"I want all my supervisors to attend this class" – KC Director.

How does this help your Management Team? Feedback

Three supervisors within a one month period had separate employees who were having suicidal ideations due in part to the sensitivity of their work. The supervisors were able to successfully intervene and get each employee the help they needed

"I attended MHFA training. As a supervisor I feel better equipped to address the concerns of my employees".

"This class teaches how to have the difficult conversation."

"This might be the most important course NGA offers. It's well worth the small time commitment." - Former Director of ODE

QUESTIONS ?

CDSE INSIDER THREAT DIVISION

MISSION

CDSE serves as the Insider Threat Center of Excellence coordinating training, awareness, professional development, education, research outcomes, and public outreach efforts in support of the Counter Insider Threat mission for the DOD, U.S. Government, industry, and critical infrastructure sectors.

TRAINING

Deploying Training to Insider Threat Program/Hub Pillar Personnel and Security Professionals

AWARENESS

Providing Annual Awareness and Vigilance Campaign for the General Workforce

PROFESSIONALIZATION

Supporting the development of tradecraft for Insider Threat Analysts and Operations Personnel. Supporting the certification program validating Insider Threat Professional Achievement of Skills and Competencies

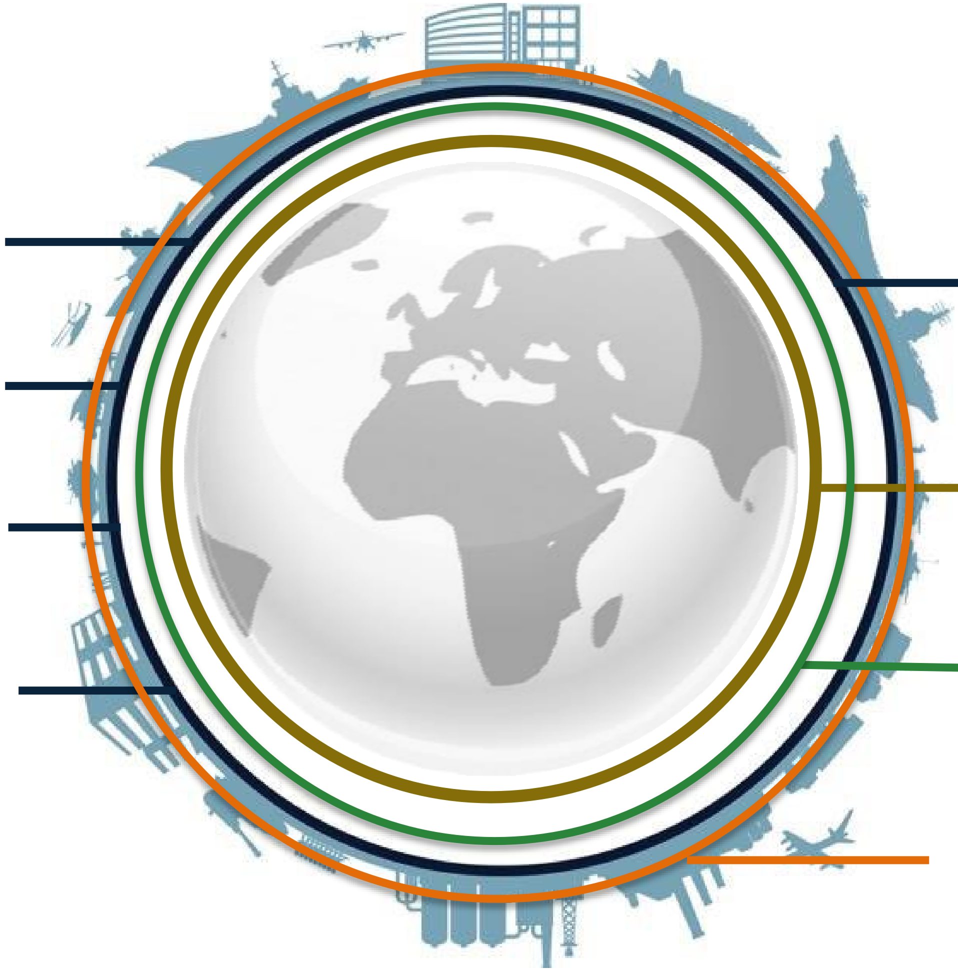
EDUCATION

Institutionalizing the Counter Insider Threat Mission for Future Security Leaders

PUBLIC OUTREACH

Providing a Public Forum for Best Practices, Research Outcomes, Training, and Awareness Materials

OUR AUDIENCE



DOD Civilian and Military Personnel

Federal Agency Personnel IC/NT-50

Industry under the NISP

Critical Infrastructure Sectors

TOTAL WORKFORCE

INSIDER THREAT PROGRAM and HUB PILLAR PERSONNEL

SECURITY PROFESSIONALS

GENERAL PUBLIC

□ **TRAINING**

□ **AWARENESS**

□ **PUBLIC OUTREACH**

□ **PROFESSIONALIZATION**
(EDUCATION, TRAINING, TRADECRAFT, CERTIFICATION)

NATIONAL INSIDER THREAT AWARENESS MONTH

UPCOMING EVENTS

WEBINARS

Counter Insider Threat Resources For Your Organization
Thursday, September 8, 2022
12:00 p.m. to 1:00 p.m. ET
Please join us for our webinar that will highlight all Insider Threat resources CDSE has to offer.
Register Now:
https://cdse.acms.com/pspsid/event/registration.html

Disinformation and Insider Threat
Tuesday, September 13, 2022
12:00 p.m. to 1:00 p.m. ET
Please join us as our expert panel discusses the security, legal, and social implications of disinformation for DOD insiders.
Register Now:
https://cdse.acms.com/disinformationint/event/registration.html

NEW PRODUCTS

INSIDER THREAT JOB AID

Employment Application Risks and Mitigation for Insiders with National Security Eligibility

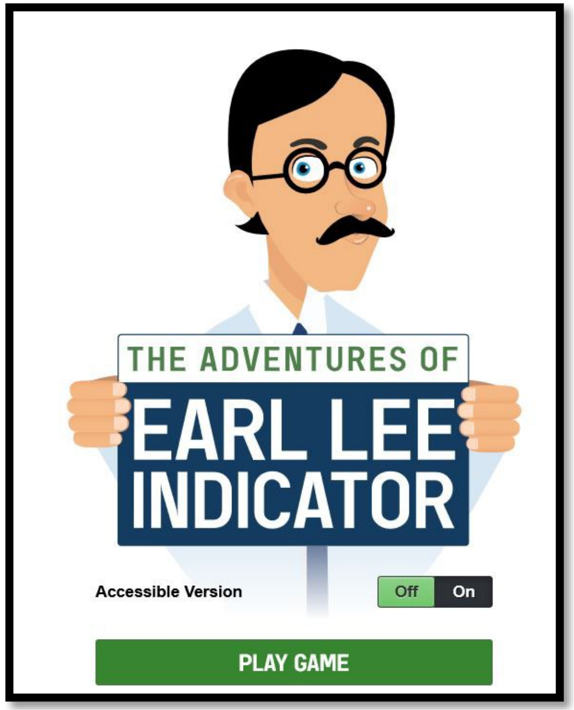
CDSE Center for Development of Security Excellence

An Insider's Digital Footprint and Associated Risks

JOB AID

CDSE Center for Development of Security Excellence

JUNE 2022



THE ADVENTURES OF EARL LEE INDICATOR

Accessible Version Off On

CASE STUDY

Unlawful Retention and Transmission National Defense Information

REALITY WINNER

- 26 years old (at time of sentencing)
- Defense contractor supporting an NSA facility
- Six-year Air Force veteran prior to contract position

WHAT HAPPENED

Reality Winner was a contractor at the National Security Agency (N facility in Georgia. Prior to that position, she served in the United S (U.S.) Air Force from 2010-2016 and held a Top Secret/Sensitive Compartmented Information security clearance (TS/SCI). She con to hold a TS/SCI at the NSA.

Winner had a deep distrust of the current administration according journal discovered during an investigation. She also posted on soc media and expressed support for Taliban leaders and Osama bin l as well as proclaiming that she wanted to burn down the White Ho

CASE STUDY

Unauthorized Disclosure

Daniel Everette Hale

- 33 years old at the time of sentencing
- Sentenced to 45 months in federal prison
- Defense Contractor who held TS/SCI clearance and access to national defense information
- Disclosed classified information to journalists
- Possessed malicious software applications to transfer data

WHAT HAPPENED

Daniel Everette Hale, 31, of Nashville, Tennesse enlisted airman in the U.S. Air Force from July 2009 t receiving language and intelligence training, Hale was at the National Security Agency (NSA) and deployed an intelligence analyst.

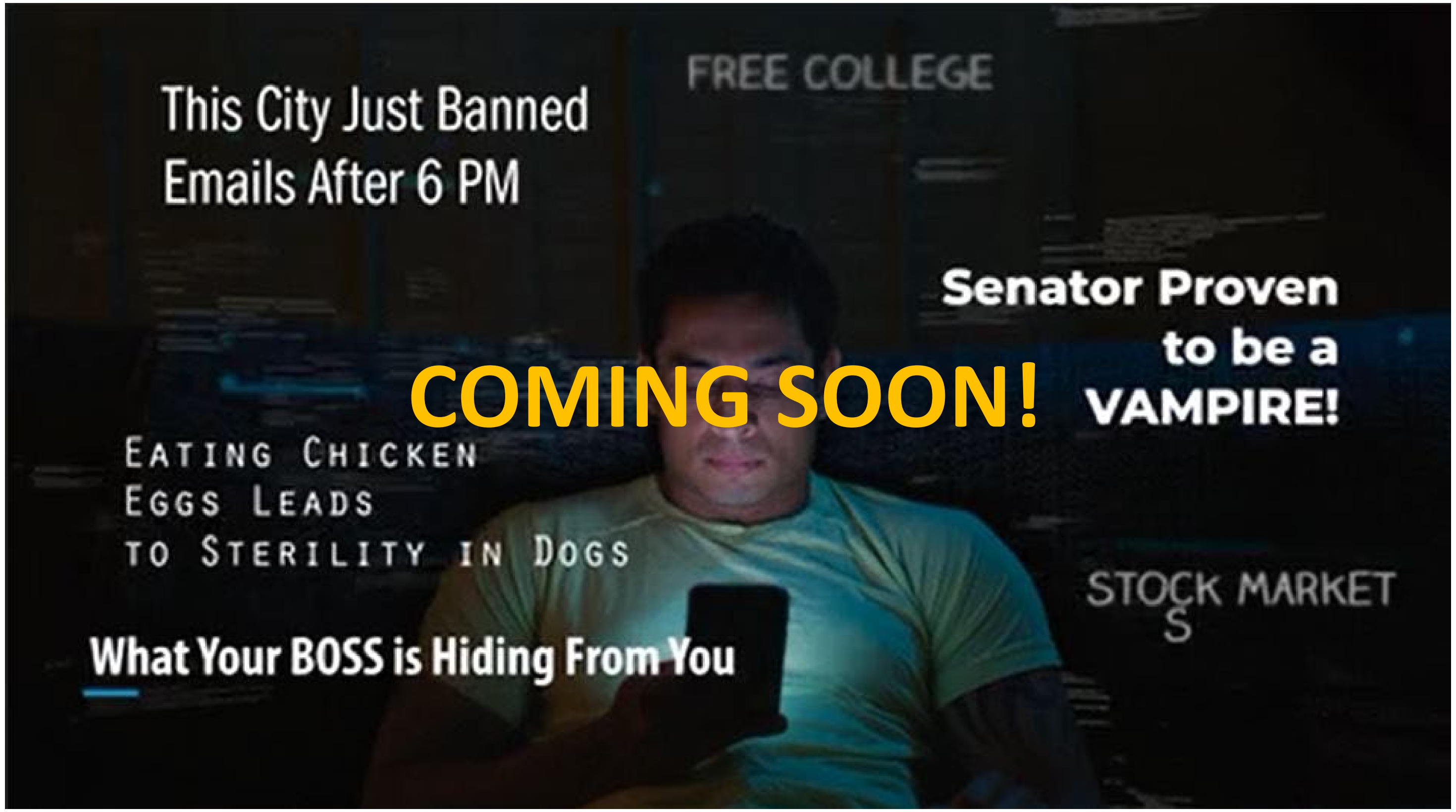
After leaving the Air Force in July 2013, Hale was defense contractor and assigned to the Natio Intelligence Agency (NGA), where he worked as a p analyst between December 2013 and August 2014. I his active-duty service and work for the NSA, and d National Geospatial Agency (NGA), Hale held a Top Compartmented Information (TS/SCI) security cle entrusted with access to classified national defense i

Hale admitted that he took classified documents he retain from his work at the NGA and sent them to purposefully disregarding the law. Hale's cell phone co contact information for the reporter, and he posse drives. One contained a page marked "SECRET" document he printed and attempted to delete from the other contained Tor software and the Tails oper anonymously "leak" documents.

Hale became an anti-war activist and released docum his opposition to war and the use of drone warfare. A of the Drone Wars Papers, he spoke at events and ga interviews.

NEW PRODUCTS

INSIDER THREAT VIGILANCE VIDEO SERIES – SEASON THREE


This City Just Banned Emails After 6 PM
FREE COLLEGE
Senator Proven to be a VAMPIRE!
Eating Chicken Eggs Leads to Sterility in Dogs
STOCK MARKET S
What Your BOSS is Hiding From You

COMING SOON!

S1/ TURNING THEM AROUND, NOT TURNING THEM IN

S2/ THE CRITICAL PATHWAY

WHERE TO FIND US

https://www.facebook.com/TheCDSE

@InT_Aware
@TheCDSE

https://www.youtube.com/user/dsscdse#p/u

Download our free mobile app -
Insider Threat Sentry

https://www.cdse.edu/Training/Insider-Threat/

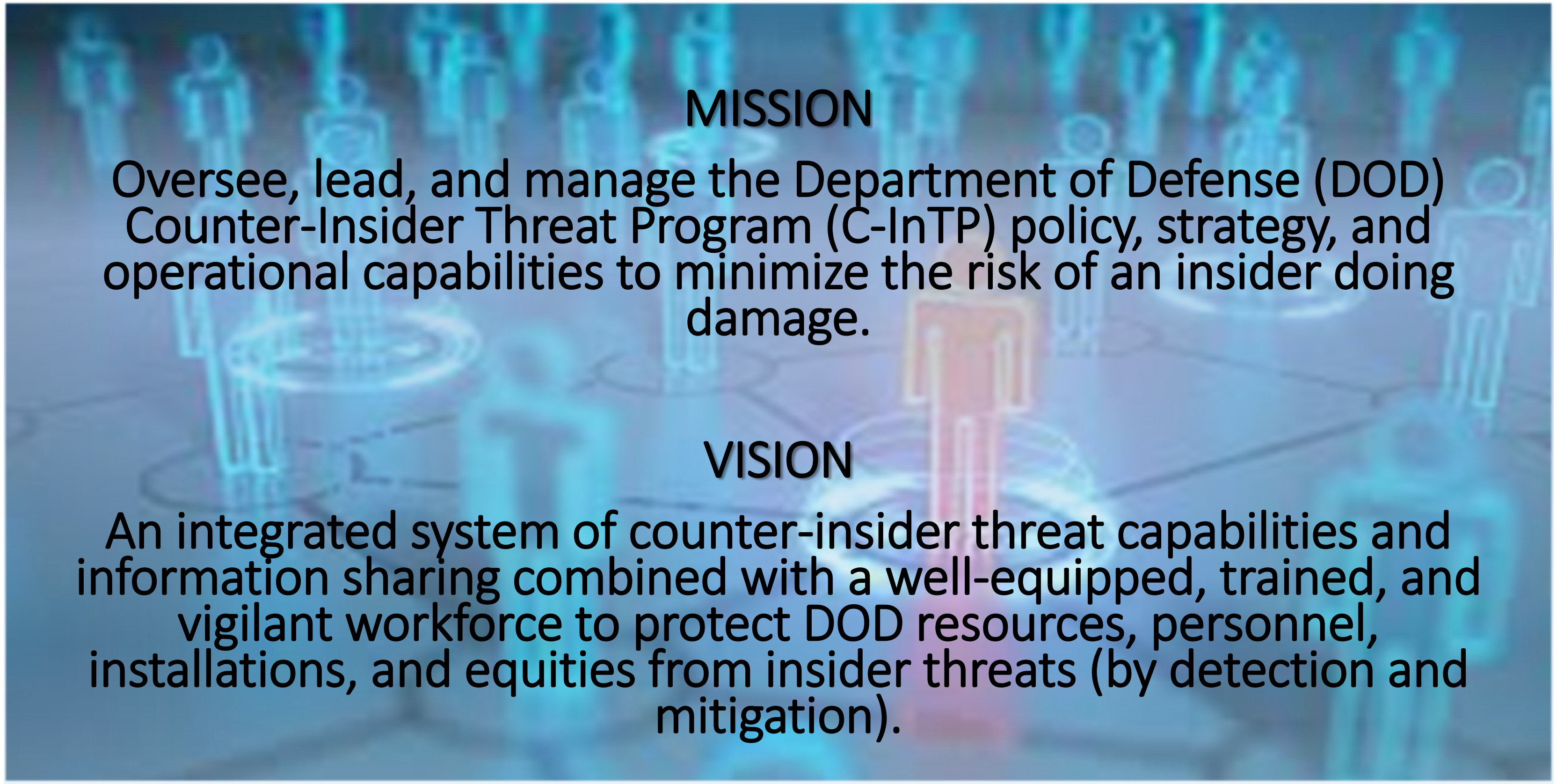
CONCLUDING REMARKS

Office of the Under Secretary of Defense for Intelligence and Security

Kristin Gallagher

Program/Insider Threat Analyst
OUSD(I&S) Counter-Insider Threat Program

OUSD(I&S) C-INTP OVERVIEW



MISSION

Oversee, lead, and manage the Department of Defense (DOD) Counter-Insider Threat Program (C-InTP) policy, strategy, and operational capabilities to minimize the risk of an insider doing damage.

VISION

An integrated system of counter-insider threat capabilities and information sharing combined with a well-equipped, trained, and vigilant workforce to protect DOD resources, personnel, installations, and equities from insider threats (by detection and mitigation).

POINTS OF CONTACT

CDSE Website

www.cdse.edu

OUSD(I&S) Website

https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

Contacts

Amber Jackson	Kristin Gallagher
amber.d.jackson16.civ@mail.mil	kristin.n.gallagher3.ctr@mail.mil

Thank You for Your Participation – Please Complete the Survey

NITAM

National Insider Threat Awareness Month

https://securityawareness.dcsa.mil/cdse/nitam/index.html