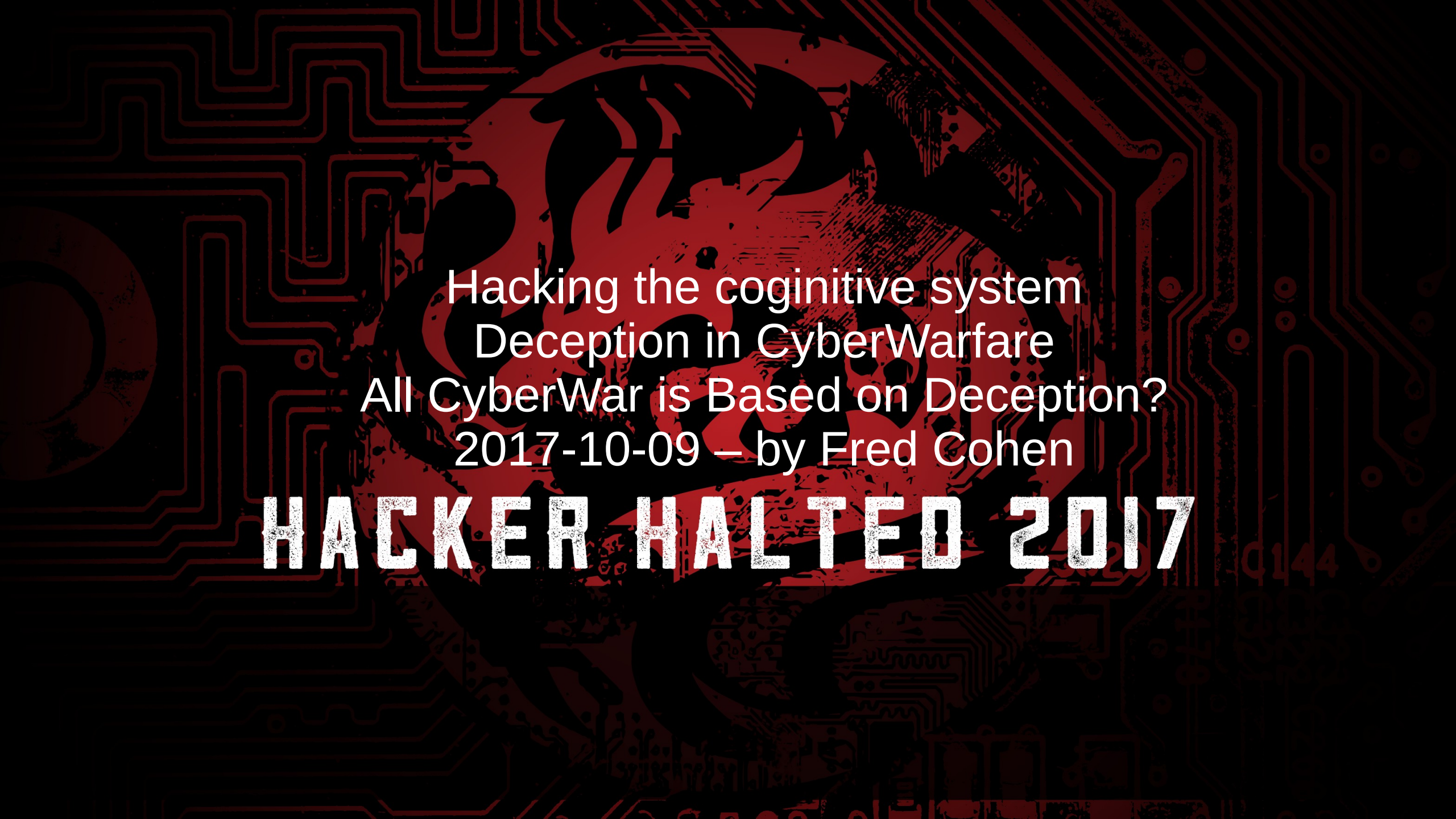

Hacking the coginitive system
Deception in CyberWarfare
All CyberWar is Based on Deception?
2017-10-09 – by Fred Cohen
HACKER HALTED 2017

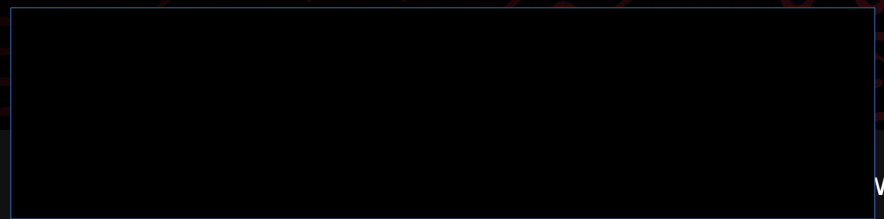
- Background of your speaker
  - When introduced as an expert, you will be perceived as one
    - I have more than 60 years of experience in deception and counter-deception
    - I have done US Government funded research in the field
    - I invented, designed, implemented, and/or operated counter-deception methods in use in more than 90% of the computers in the world
    - I have used deception to enter facilities, systems, groups, enterprises, etc.
    - I have won global awards in deception and counter-deception
    - I was named the “most famous hacker of all time” (in 2009 by ABC News)
    - I have never been accused or convicted of any crime (I’m honest)
    - I have held top level US Government security clearances
    - I founded the College Cyber Defenders at Sandia National Labs – the precursor of the US Cyber Corps
    - …
  - I’m a friggin’ expert in how to lie and counter your lies – don’t even try it!

What they say and what it means

- How to close the sale*
  - You can trust me
  - You can trust my business
  - You really want what I have
- The thing is
  - It works
  - He’s telling the truth
  - At least it worked to get me here in front of you today!
- *According to whom?
  - A convicted criminal
  - With fraudulent businesses
  - Selling advice on how to sell
- Just because he’s a crook
  - Doesn’t mean everything he says is a lie!
  - And he’s done his time
  - Fallacy: it worked so it must be right

Another real-world example

- I worked at Sandia National Labs for many years
- I have spoken officially on Nuclear Weapons Security for Sandia
- No US Nuclear Weapon has ever fallen into the hands of any adversary



Another real-world example

- I worked at Sandia National Labs for many years (1)
- I have spoken officially on Nuclear Weapons Security for Sandia (2)
- “No US Nuclear Weapon has ever fallen into the hands of any adversary”
  - Note that this is not a “real” quote and I don’t know the underlying facts.

- (1) In cyber-security
- (2) About Y2K issues
- Let’s assume the statement is true
  - What does it really mean?
- What is a “US” N.W.?
- What is an “adversary”?
- What is “fallen into hands”?

Summary and conclusions

- More words → more deception opportunities
- Put another way, the more verbiage presented in regards to any specific subject, the more opportunities are present for suppression and induction of signals so as to lead the recipient toward conclusions they might otherwise not come to.
- Note:
  - Hacker Halted only provided 4 slides in the official template
    - I have lots more to say, but it won't fit in 4 slides
    - But I may have misinterpreted what they sent me
    - So being as a hacker at heart…

The nature of the space

- Cyber:= {sensors, actuators, communications, control}
- Warfare:= Acts of high intensity conflict (between nations?)
- Where: {Land, Air, Space, Water, Physiology, Cyber}
- Targets: {People (mind/body), places, things, dependencies}
- Situations: {Distant, Proximate, Enveloped}
- Tactics: {Speed (OODA loop), Force (wave forms), Influence (cognition)}
- Intensity: {covert-overt, rare-often, strategic-tactical, peace-war, diplomacy-force, competition-conflict}
- Venue: {crime, nation-states, corporate, political, infrastructure, waveform}
- Game: {multi-player, repeated, memory, differing objectives}
- Tools: {technology, research, computation, models}
- Interactions: {interdependencies within and between all}

But I only have 40 minutes...

- Actually... by now... 30 minutes
  - 20 minutes if you ask complicated questions
    - 10 minutes if I keep drilling down...
      - So I won't...
    - So where do you get more details?
  - I provide free online resources
- fc0.co (about me and the spectrum of things I do)
  - All.Net (gobs of technical details, recordings, slides, papers, and so forth)
    - Or you could engage me on a consulting basis
      - High fees – no guarantees
      - We won't quit till you run out of money!
- So I'm going to do an overview with some drill-down

Outline and Drill-down

- **Definitions**
- Weapons
- Strategy and tactics
- Examples
  - Strewn throughout
- Cognitive Security (COGSEC) vs.
  - influence, information and deception (I2D) campaigns
- Just did that – except
- Deception:=
  - Induction and/or suppression of signals
  - To cause behavioral changes
  - In targets
- Issues:
  - Induce/Suppress/What signals?
  - What behavioral changes?
  - What are the targets?
  - What about side effects? Time?

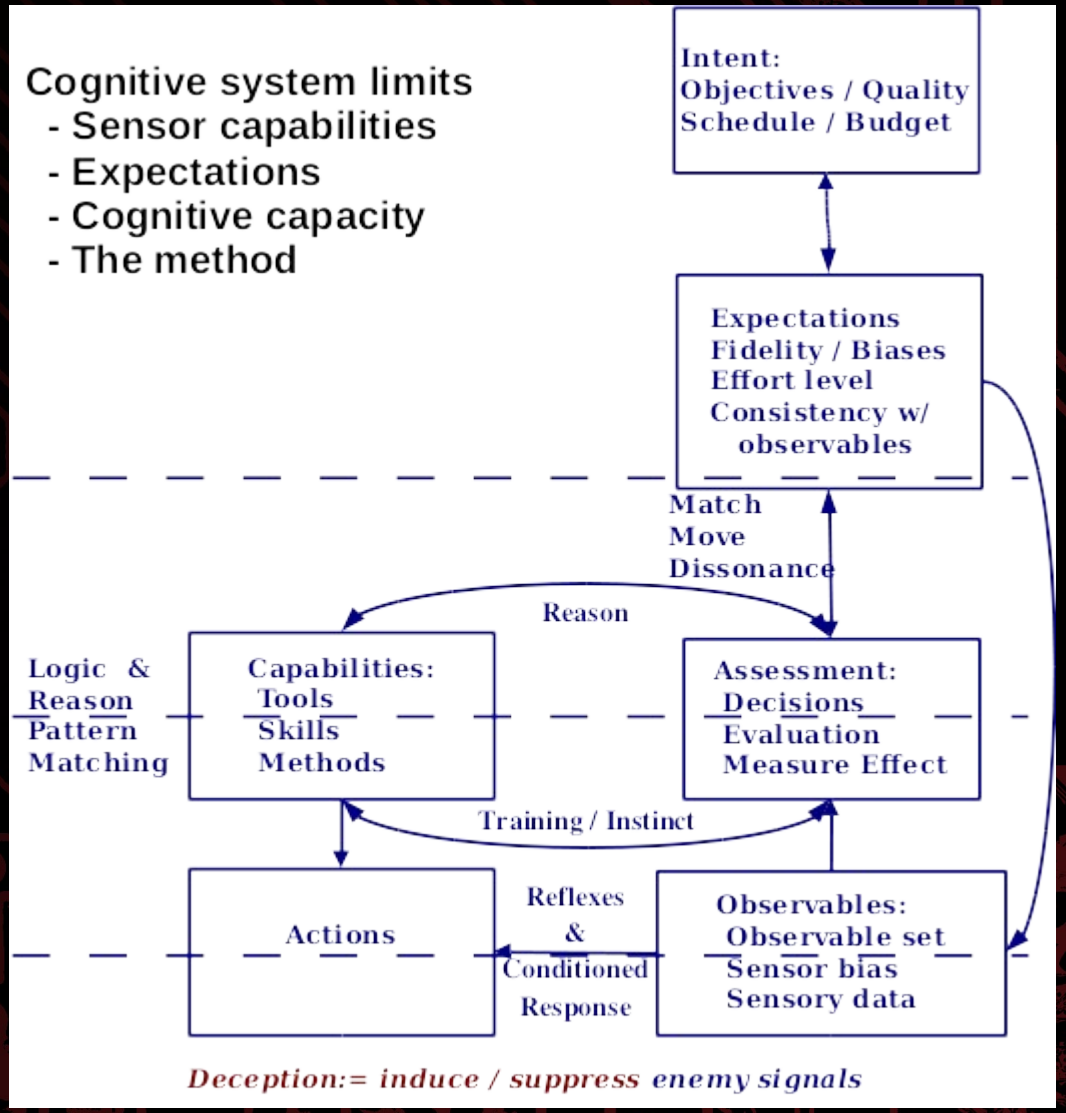
Outline and Drill-down

- Definitions
- **Weapons**
  - Tools of the trade
- Strategy and tactics
- Examples
  - Strewn throughout

- Communications media (1 → 1, direct)
  - Talking, email, telephone, text messages, etc.
- News media (broadcast, 1→ many, intermediated)
  - Broadcast TV, Cable, Satellite, books, magazines, etc.
- Social media (many → many, not (as) intermediated)
  - Youtube, twitter, email lists, Facebook, LinkedIn
- Technical meme analysis and projection
- Spectrum (waveforms)
- State machines (HW, Firmware, SW, Net)

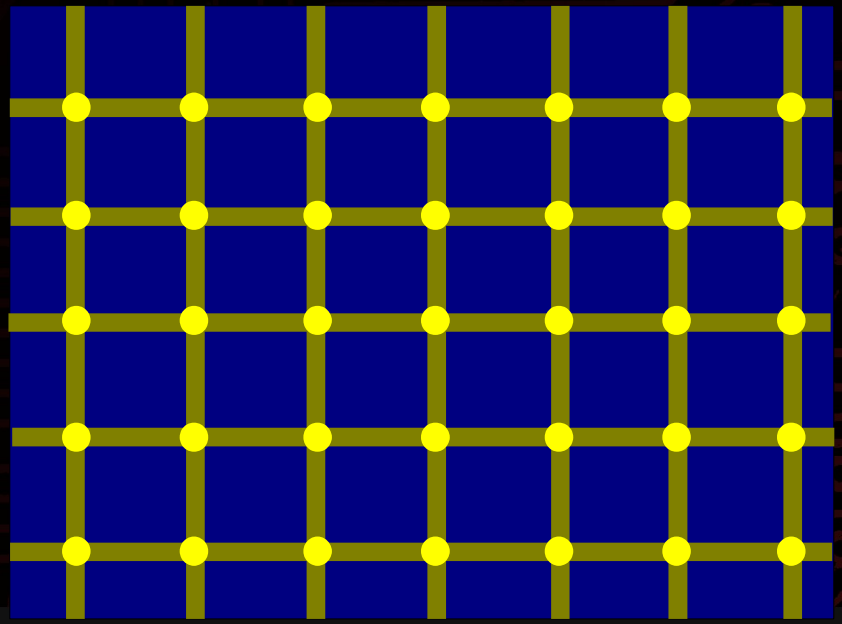
Weapons

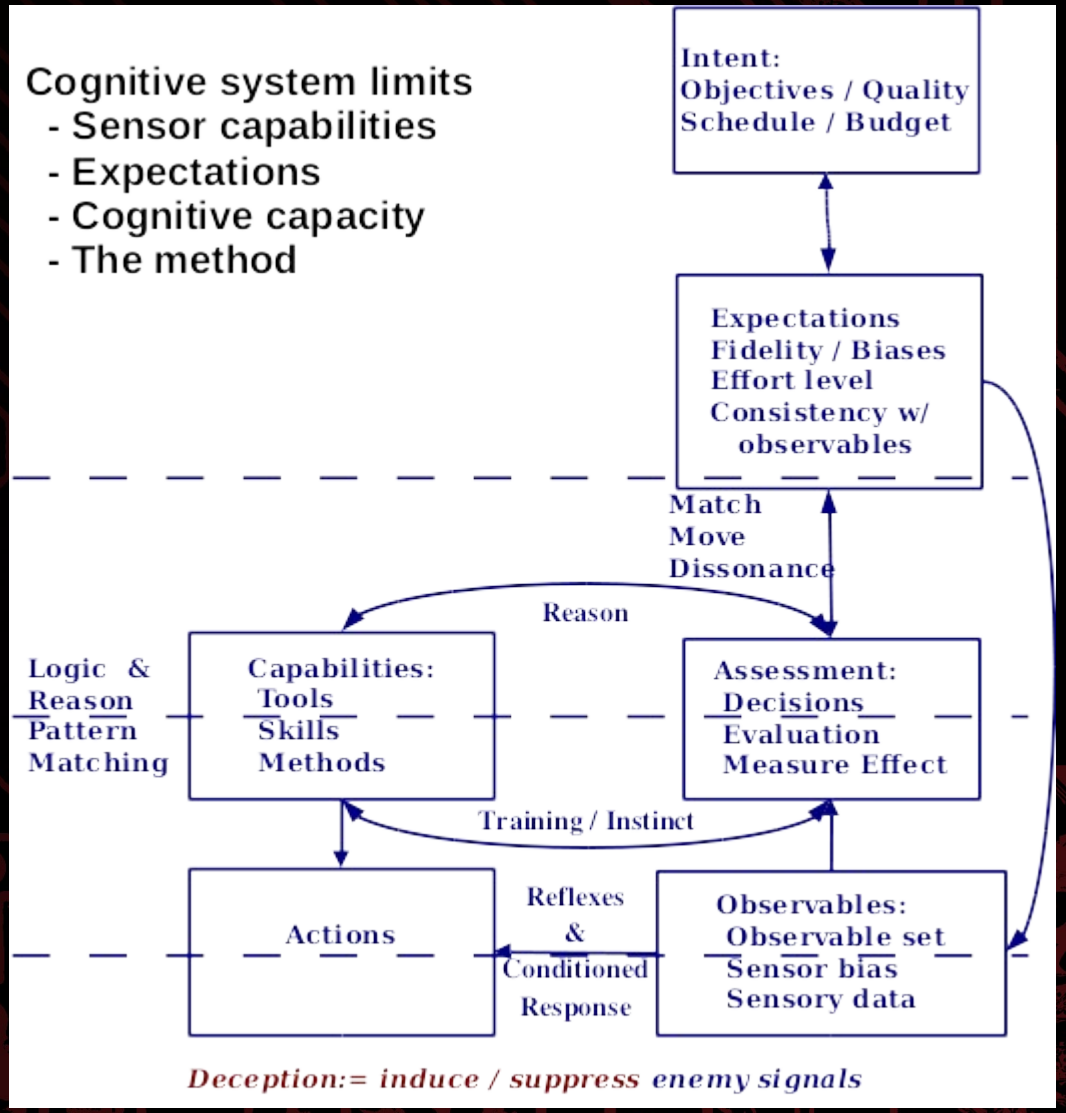
- Definitions
- **Weapons**
  - Things that cause failures in the cognitive systems of targets
    - Input processed at ~4 levels
    - Different levels => different time frames & mechanisms
    - Expectation => interpretation
    - Cognitive capacity limited
    - Cognitive systems imperfect
  - → *Confuse sensors / Set expectations / Overrun capacity*
- Strategy and tactics
- Examples
  - Strewn throughout



Weapons

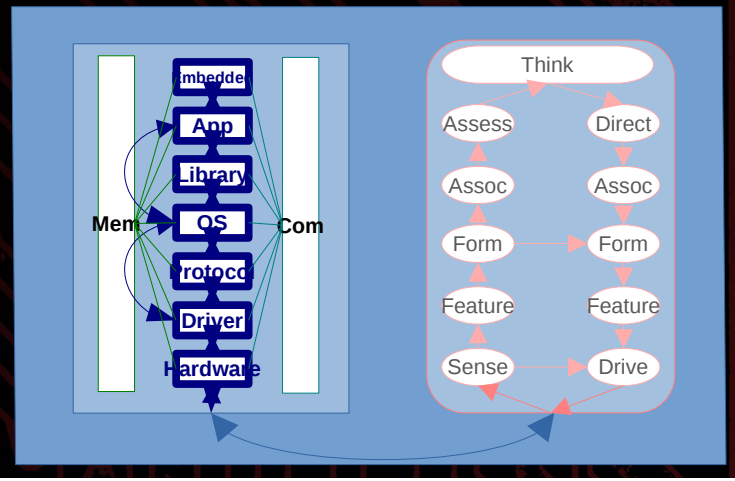
- Definitions
- **Weapons**
  - Example dazzlement
- Strategy and tactics
- Examples

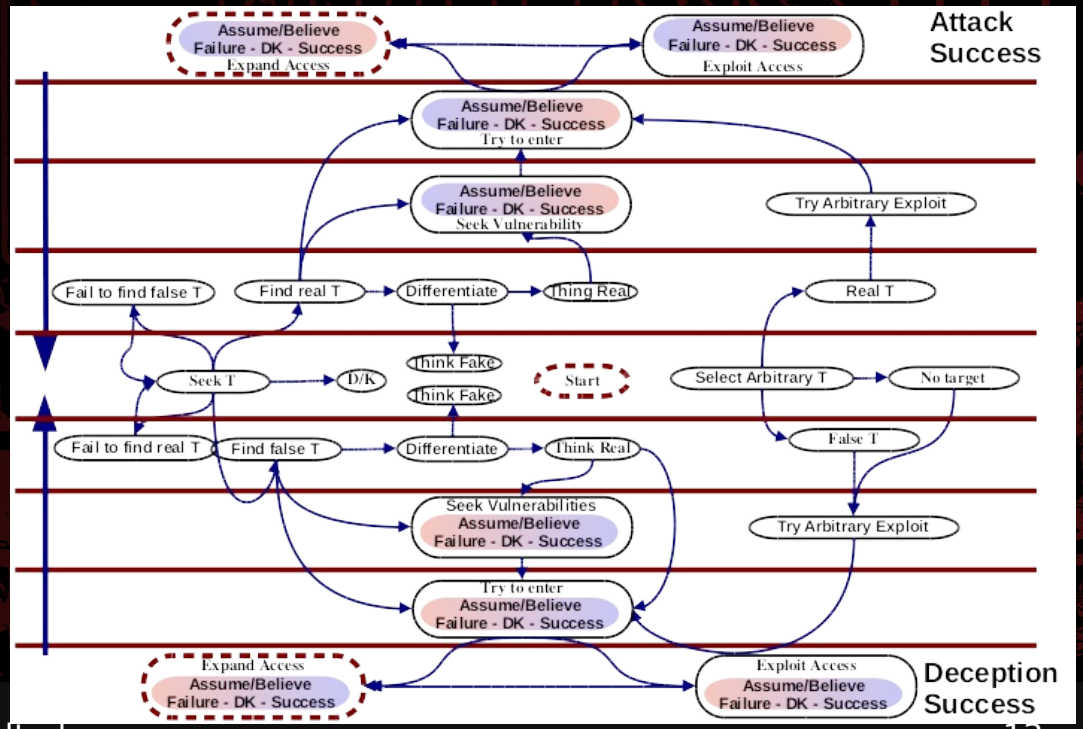




Weapons

- Definitions
- **Weapons**
  - Another cognitive system
  - Attack methodology
  - Under deception defense
- Strategy and tactics
- Examples
  - Strewn throughout





Weapons

- Definitions
- **Weapons**
  - Example
- Strategy and tactics
- Examples
  - Strewn throughout

Weapons

- Definitions
- **Weapons**
  - Example
- Strategy and tactics
- Examples
  - https://information-professionals.org/category/blog/

- The Lisa Case in Germany
  - A 13-year-old Russian-German girl had gone missing for 30 hours in January 2016
  - This was first reported by First Russian TV to have been a rape by 3 men “of Middle Eastern appearance.” The story was intensively reported in Russian domestic and foreign media
  - The story turned out to be fake. The German police established that she had been with a friend that night
  - The story dominated headlines and impacted on German public discussion for two weeks
  - There was clear evidence of several of the different current Russian elements of influence in Germany working in a coordinated way

Weapons

- Definitions
- **Weapons**
  - Example
- Strategy and tactics
- Examples
  - https://information-professionals.org/category/blog/

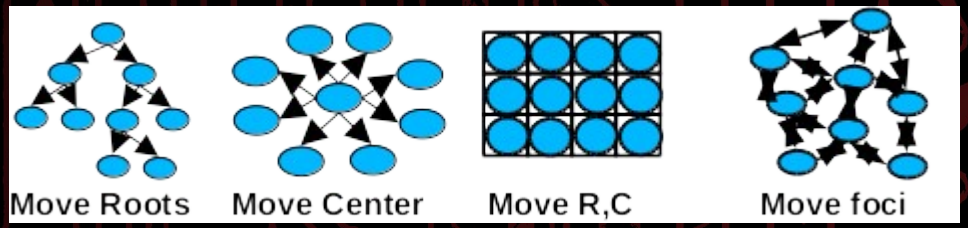
- The Lisa Case in Germany – campaign time-line:
  - A journalist from the First Russian TV channel picked up the case of the Russian-German girl and brought it to the main news in Russia
  - Russian foreign media (RT, Sputnik, and RT Deutsch) reported it
  - Social media and right wing groups distributed details via Internet
  - Demonstrations organized via Facebook by German-Russian minority (Deutschlandrussen) and neo-Nazi group representatives
  - Russian foreign media in Germany reported from the demonstrations, which brought it to the German mainstream media
  - Russian Foreign Minister Sergej Lavrov made two public statements about his concerns about the inability of the German police and legal system to take such cases seriously because of political correctness

Outline and Drill-down

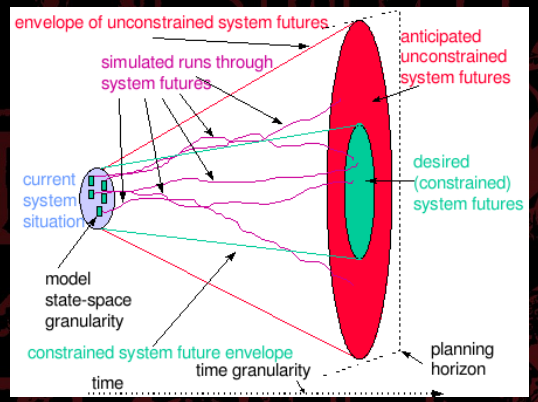
- Definitions
- Weapons
- **Strategy and tactics**
  - Things you understand and may apply to achieve goals
    - Strategy: What and why you do
    - Tactics: How you do it
- Example (strategy)
  - Take over the Republican party
    - Largely a hierarchy
    - Tea party creates a new root
    - Take over branches → a network
    - Underway: Move foci →
    - Fuse foci → New root

- Situational understanding

- Structural strategies



- Models



Strategy and tactics

- Definitions
- Weapons
- **Strategy and tactics**
  - Things you understand and may apply to achieve goals
    - Strategy: What and why you do
    - Tactics: How you do it
- Example (tactics)
  - Propaganda
    - Long and short term messaging
      - Theme and story
    - Delivery mechanisms
      - Multi-modal (all media)
    - Counter alternative messages
      - Fake news etc.
- Propaganda and messaging
  - Us v. Them (and divider)
  - We were great (older folks)
  - Will be again (younger / middle folks)
  - It’s their fault (you decide on “them”)
- Cognitive error exploits
  - Equivocation
    - Nazis are the same as anti-Nazis
  - Ambiguity
    - They interpret – you claim they/you are right
  - Outcome asymetries
    - Hillary lied (unquantified)
      - → When we lie - equivocate

Human Cognitive Limits, Errors, Attacks, Defenses

Miller's law:
- Assume they are telling the truth
- Figure out what they are telling the truth about

Biased evaluation of ambiguity and inconsistency
- Ambiguous data interpretation in context
--- Tendency to find things like what you look for
- Unambiguous data shaded
--- Tendency to explain away falsifications
- Multiple endpoints problem
--- Ambiguous data associated with expected outcomes
- Confirmations and non-confirmations
- Focused and unfocused expectations

Misrepresentation of incomplete data
- Excessive impact of confirmations
--- Small number of confirmations taken as proof
--- Refutations ignored or explained away
- Tendency to seek confirmations
--- Pattern matching rigged for target detection
--- Other targets ignored
--- Non-detection ignored
- Hidden or absent data problems
--- Non repeatable experiments:
you don't know what would have happened in the path not taken.
- Self fulfilling prophecies
--- Market crashes

Biasing of second hand information
- Sharpening and leveling
--- People emphasize (sharpen) focal points
--- People de-emphasize (level) side points
--- Focal vs. Side depends on the interpreter
- Corruption with transitivity (game: telephone)
- Telling a good story (enhance reader interest)
- Distortion for informativeness (exaggeration)
- Distortion for entertainment (humor/interest)
- Distortion for self interest (greed)
- Distortion for plausibility (urban legends)
- Outcome asymmetries
--- Hedonic: Overemphasis on more striking things
----- Seems more informative if more unusual or stranger
--- Pattern: Overemphasis of specific patterns
----- Remember 1:11 more than 3:46
--- Definitional: Loose definitions / interpretations
----- You won't get better till you hit 'rock bottom'
----- If a tree falls in a forest and nobody is there...
--- Base rate: You only measure survivor views
----- "80% of Cancer survivors 'thought' healthy thoughts"
90% of those who died may have thought healthy thoughts – and you can't ask them...

Motivational determinants of belief
- Empirical support for wish to believe
--- Interpreting the same information in different ways
----- After the Nixon / Kennedy debates, supporters on both sides said that they believed that they won
- Mechanisms of self-serving beliefs
--- Believers ask "Can I believe?"
--- Non-believers ask "Must I believe?"
- Optimistic self-assessment
--- Most people believe they are above average In beauty & mental capacity

Emotion effects cognition
- Affects: --- Likes+, dislikes-, fear-, happiness+, etc.
-----Positive affect improves sensory detection and recall
- Values: --- Fairness, right and wrong, etc. impact interest
----- Tendency to be more interested in 'good' things
- Needs:
--- Lack of air, water, food, drive sensor focus
----- Tendency to see food in randomness when hungry
- Interests: --- More interest leads to better learning

Intel errors
- pre-existing notions given excessive weight
- desensitization degrades vigilance
- generalizations or exceptions based on limited data
- failure to fully examine the situation limits comprehension
- limited time and processing power limit comprehension
- failure to adequately corroborate
- over-valuing data based on rarity
- experience with source may color data inappropriately
- focusing on a single explanation when others are available
- failure to consider alternative courses of action
- failure to adequately evaluate options
- failure to reconsider previously discarded possibilities
- ambivalence by the victim to the deception
- confounding effect of inconsistent data

Satire's Modes: (* mismatch between beliefs & expressed beliefs)
* Blaming (all, none, every…) match -> fight
* Placating (you are right boss) match -> unproductive delay
- Computing (generalities/abstractions) match -> slow productive delay
* Distractive (flip from one to the other) match -> helter skelter
- Leveling (simple truth as they see it) match -> honesty - not always good

Feed it – it will grow - match modes to grow

Suppress it – it will fester or die - mismatch to suppress

Sensory Modes: (see, smell, hear, taste, feel)
- match modes -> like and agree
- no modes -> neutral
- mismatch modes -> dislike, clash, slow resolution

Self-defense process:
1) Detect attack
2) Characterize it
3) React appropriately
4) Follow through

Friendly defense:
- 3-part message: When you do X, I feel Y because Z
- avoid structural twerks: constant use of blaming,
--- placating, or distraction1

Attack Techniques:
- presupposition:
--- to avoid apposition,
--- to generate assumptions
- illusion of choice when none

Detect Attack
Presuppositions & baiting & harsh emphasis -> attack
- Ignore bait (even you could do that)
- Find presuppositions (you are incompetent)
- Transmit 'it won't work', 'I won't play' (ignore bait)
- Known how to follow-through (ask 'when' leveler mode)

Characterize and respond
If it is general, agree in general
… anyone who would X should/is Y
… some people… any fool could ...
.or. you're not the only X that Y
=> I agree

Everybody knows... and we understand
=> I'm sure they do understand and I appreciate it.
If you cared about X, you wouldn't Y
=> When did you come to think I didn't care?

Behavioral inconsistencies have causes

Strategy and tactics

- Definitions
- Weapons
- **Strategy and tactics**
  - Some common warfare related things to understand
- Example (strategy)
  - Throughout

Offensive Space Examples

Overt

High Frequency

Tactical

Covert

Low Frequency

Strategic

War

Take control of media

Force messages

Intervention

Threaten direct actions

Propaganda

Posturing

Direct support power and influence changes

Restrict capabilities and intent

Support Enemy's Enemies

Selective controlled demonstrations

Support political allies

Show of Force

Influence elections

Political Leverage

Direct capabilities and intent

Investment approach

Influence body-politic desire

Economic leverage

Influence capabilities and intent

Investment approach

Diplomacy

Peace Competition Diplomacy

War Conflict All Out Force

Strategy and tactics

- Definitions
- Weapons
- **Strategy and tactics**
  - Some common warfare related things to understand
- Example (strategy)
  - Throughout

Defensive Space Examples

Overt

High Frequency

Tactical

Covert

Low Frequency

Strategic

War

Mass media direct messaging

Intervention

Refute direct actions

Counter Propaganda

Posturing

Direct support for their enemies with capabilities

Explain intent

Support Enemy's Enemies

Close ranks with political allies

Demonstrate support for views

Invest in capabilities and intent

Secure elections **Show of Force**

Use reputation and credibility

Political Leverage

Detect undesired influences and shame them

Influence body-politic desire

Build reputation

Economic leverage

Invest in credibility

Diplomacy

Peace Competition Diplomacy

War Conflict All Out Force

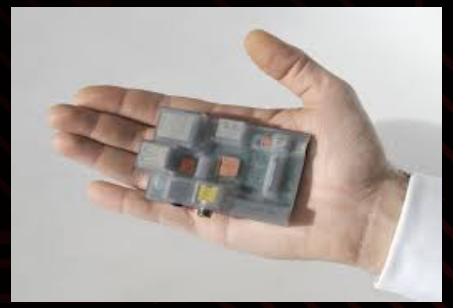
Outline and Drill-down

- Definitions
- Weapons
- Strategy and tactics
- Example: Speed & stealth
  - Wins: Internet memes & news
    - Flash mobs
    - 24 hr news cycle
    - Dis-intermediation of editorial
  - Credible lies spread faster than truth
    - Reagan and German discotheque bombing
    - Kennedy facing down Russia in Cuba
    - Lots of modern examples
- Stealth is a deception issue
  - Currently moderated at the national level in the US for equities issues
  - Tactically used all the time
  - Sources and methods vs. ineffective operations
- Attribution and stealth
  - True attribution
  - False attribution
  - N. Korea and Sony
  - Russia and DNC hacks

Hacking (deception) tool examples

Airport Extreme –

USB sniffer –



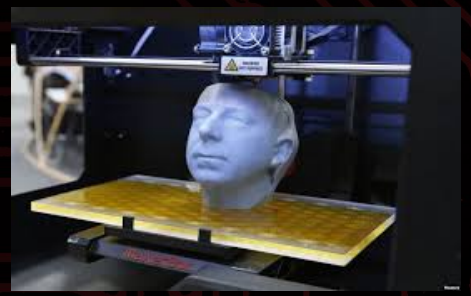
raspberry pie -

bootable linux -

nano bug

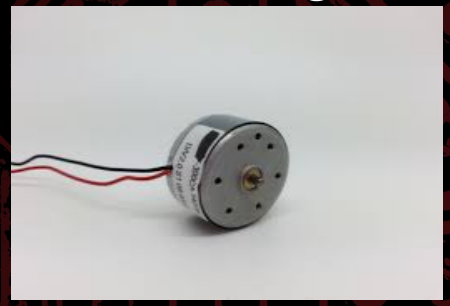
Quad copter –

3d printer –



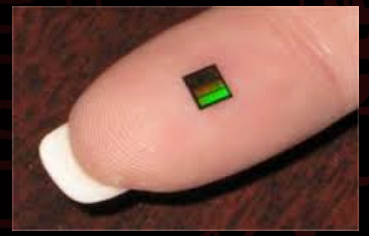
3d printer mask –

gene sequencer –



EM generator

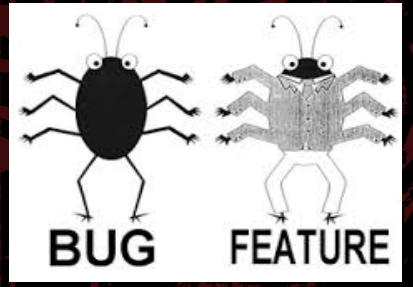
Fiber camera –



tracking device –

better bug –

false eye computer -



feature

Examples

- Definitions
- **Weapons**
  - Example
- Strategy and tactics
- Examples
  - https://information-professionals.org/category/blog/

- Chinese concept of deception strategy
  - All types of measures and activities designed to confuse an opponent
    - Confusing the opponent then leads him to make “major errors in judgment and decision-making,”
    - Strategic deception aims at foreign intelligence institutions
    - Influences the “highest military authorities responsible for formulating strategic decisions.”
  - Not limited to the military
    - Seamlessly spans the spectru, from peace to war
    - Interweaves diplomacy, politics, media, networks, military applications, and spies
    - All controbute to the struggle over influencing the mind

- Background of your speaker (skeptical inerpretaiton)
  - When introduced as an fraud, you will be perceived as one
    - I am 61 years old – and I have lied since birth
    - I was the subject of a psychology experiment in college
    - I wrote a checksum program once
    - I lied on a job application
    - Joseph Global gave me two certificates over the Internet
    - I was called a computer criminal in the news
    - I wasn’t arrested for it
    - I once carried mail containing US Government paperwork
    - I came up with a brand name used by someone in the government
- Trust me!

- Time for your questions?
  -