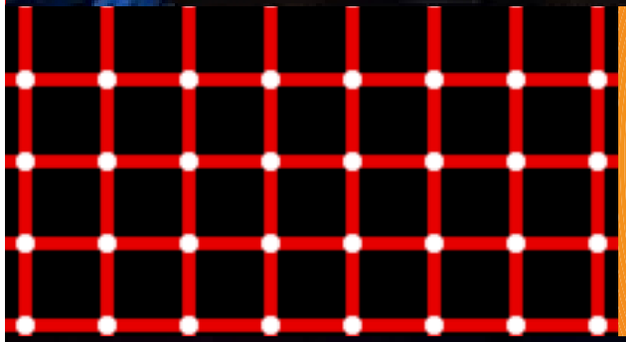
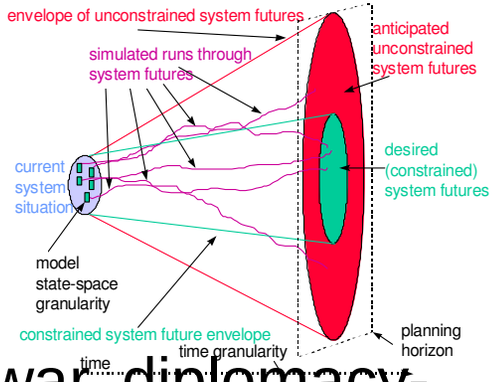
Cyber Warfare – The Big Picture



Fred Cohen
2017-06-12

The nature of the space

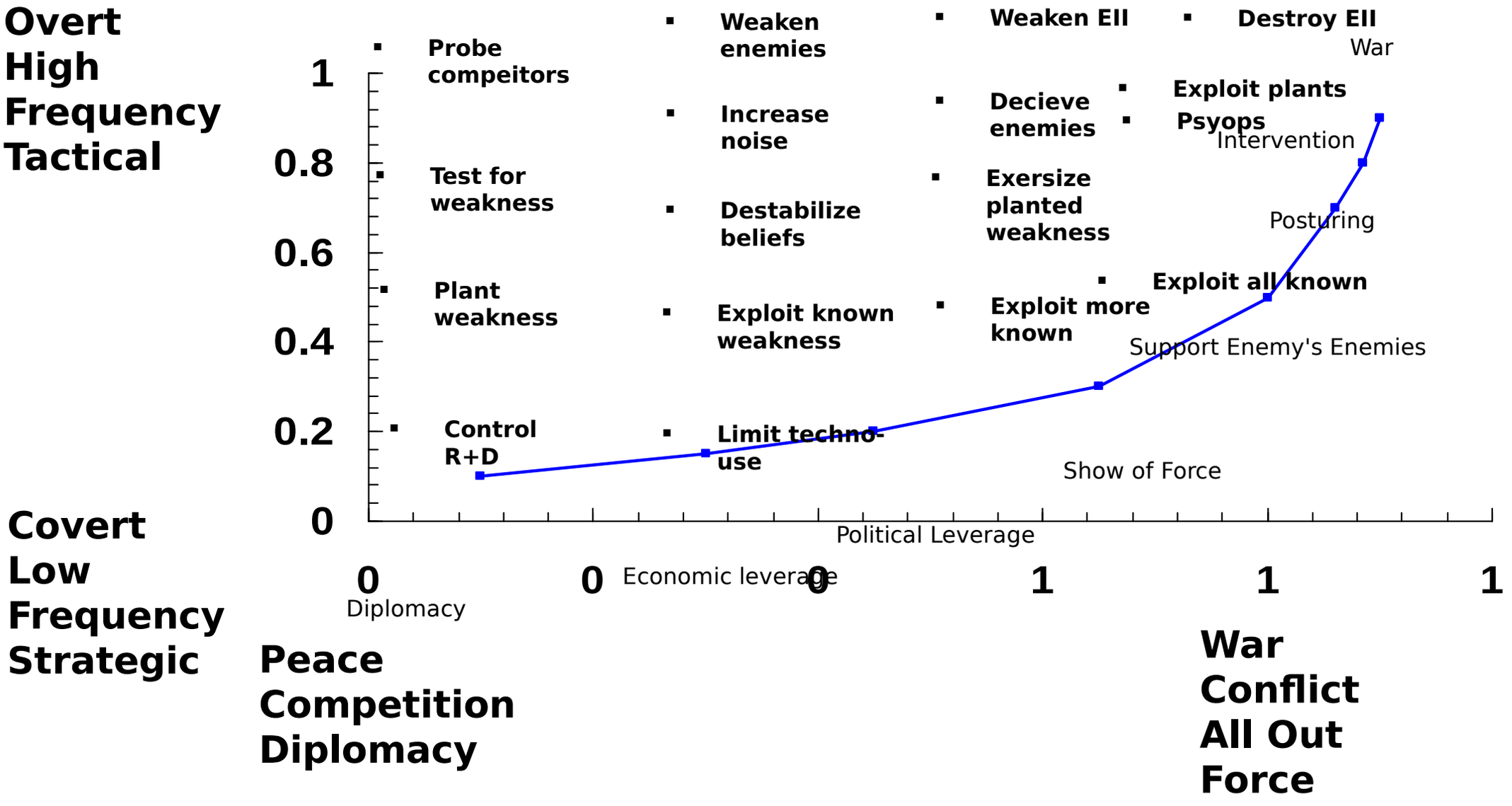
- Cyber:= {sensors, actuators, communications, control}
- Warfare:= Acts of high intensity conflict (between nations?)
- Where: {Land, Air, Space, Water, Physiology, Cyber}
- Targets: {People (mind/body), places, things, dependencies}
- Situations: {Distant, Proximate, Enveloped}
- Tactics: {Speed, Force, Influence}
  - 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}

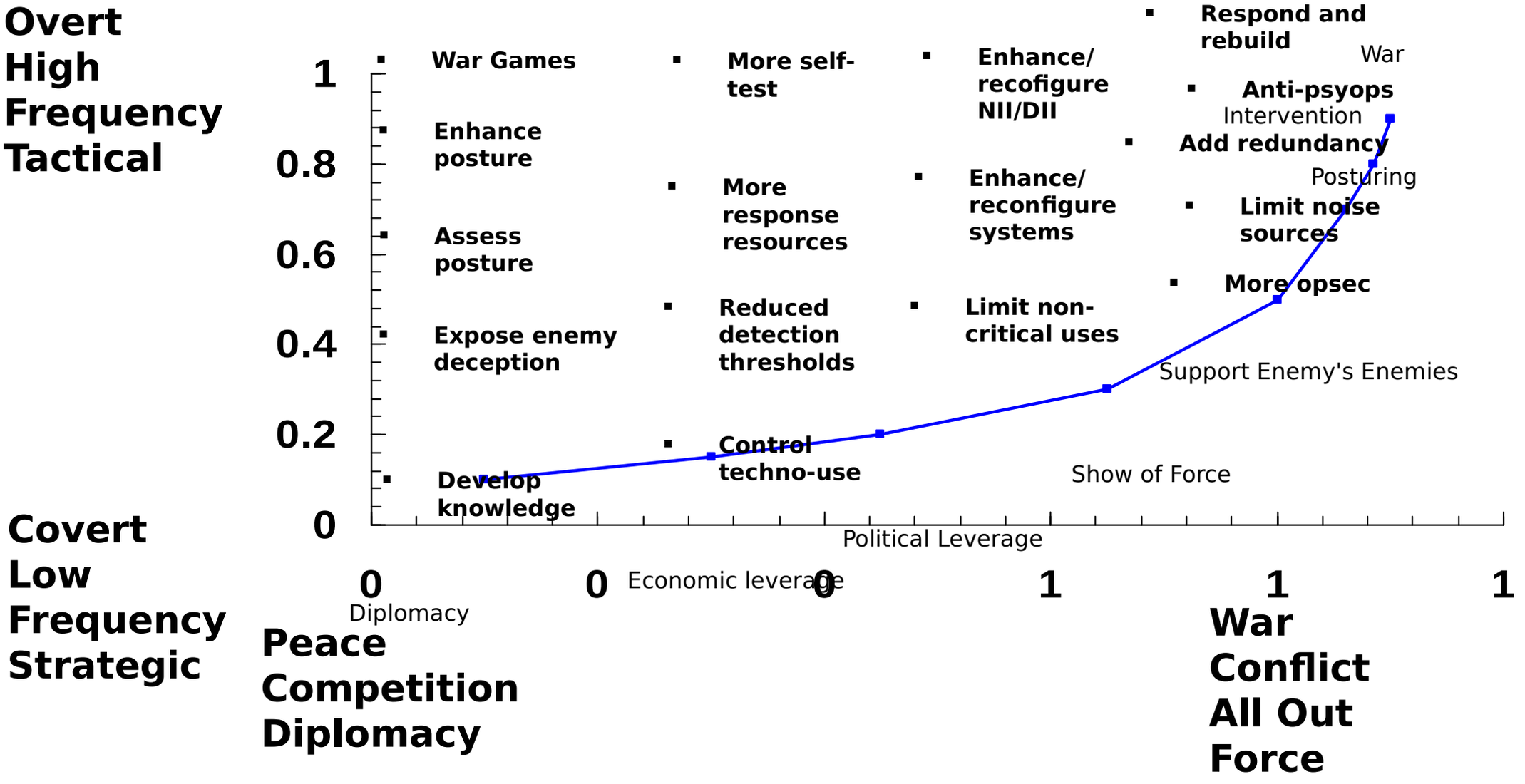
~20 years ago

Offensive IW Space

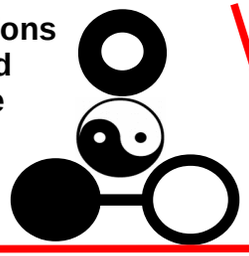


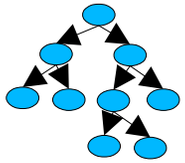
~20 years ago

Defensive IW Space

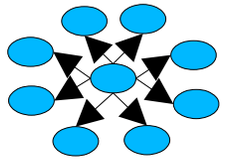


The 3 situations
- Enveloped
- Proximate
- Distant

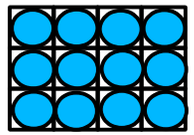




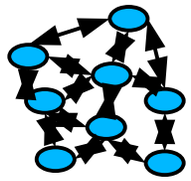
Move Roots



Move Center



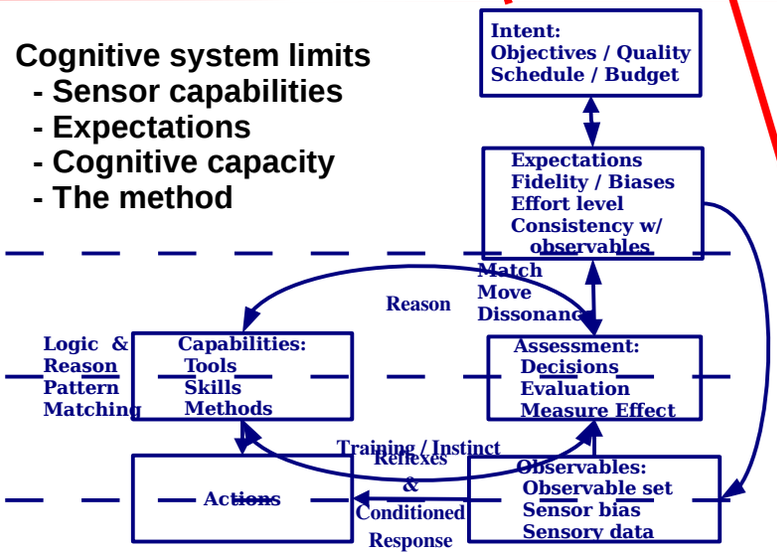
Move R,C



Move foci

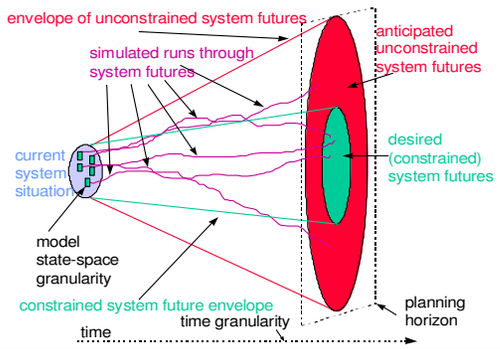
~20 years ago

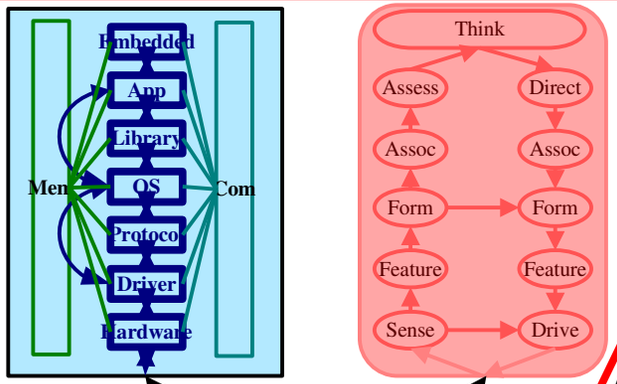
Cognitive system limits
- Sensor capabilities
- Expectations
- Cognitive capacity
- The method



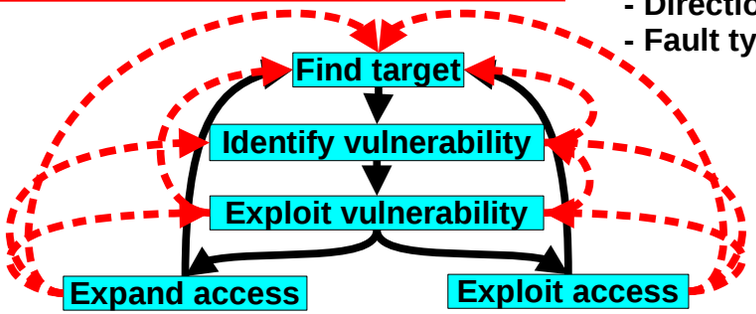
Deception:= induce / suppress enemy signals

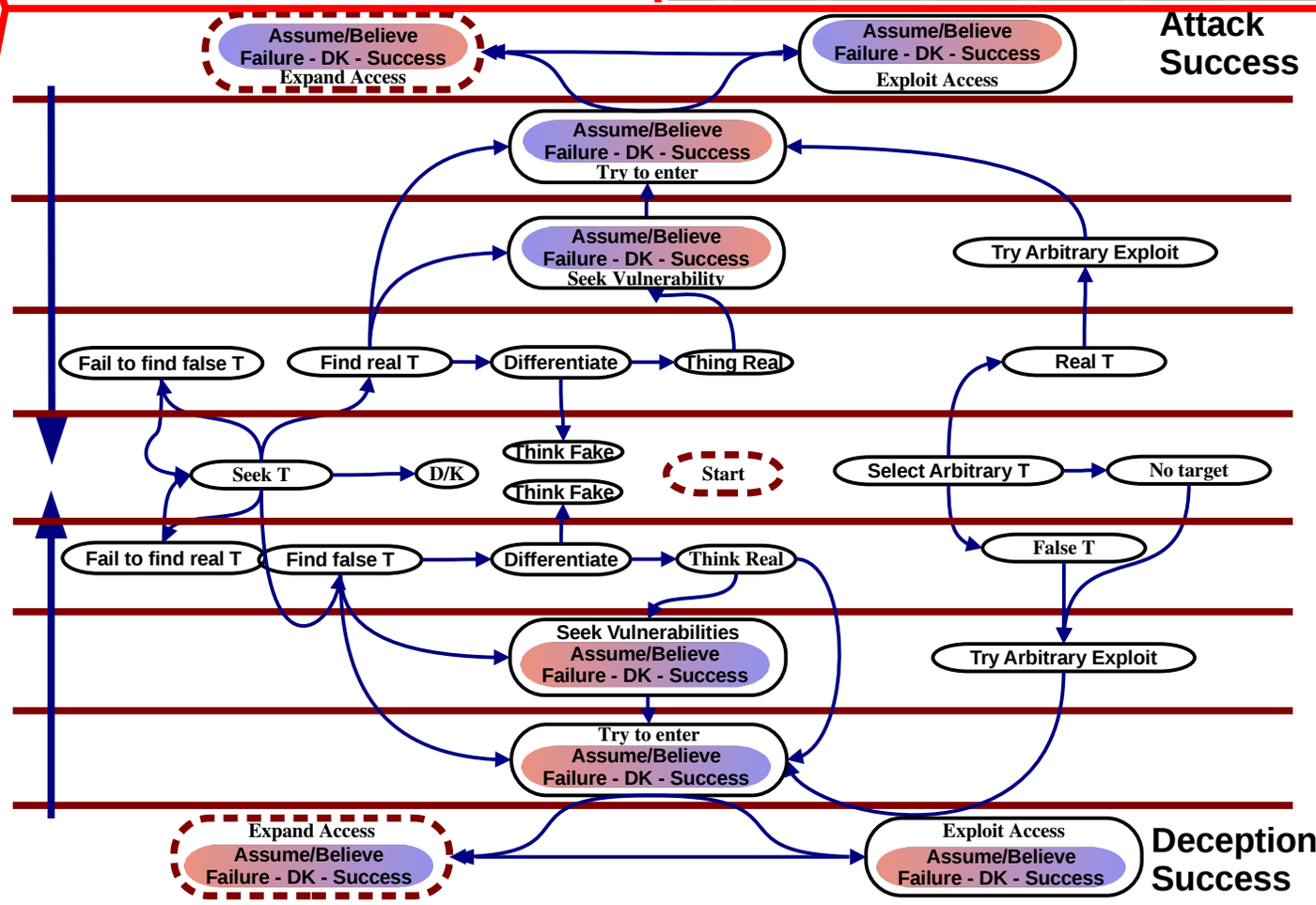
Model-based
Situation
Anticipation
& Constraint
Granularity
Precision
Cycles
Moves
Envelopes





Attack graphs
- Progress(t)
- Direction
- Fault types





Human Cognitive Limits, Errors, Attacks, Defenses

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

- 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...

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

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

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

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

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)

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

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

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

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

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

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

Overcoming Resistance to Change
a.k.a. Expectation Management

Cycle of resistance
- Always present
- Everyone goes through it
  - Some go faster than others
- It cannot be avoided
  - It can be managed

Introduce change
- "You must be crazy"

Experience change
- "No way"

New becomes norm
- "I always knew it"

time

1/3 Ready for change
1/3 Unsure but listen
1/3 Resist change

Early adopters
Wait and see
Still not convinced

"I know what, why, and how it is happening."

What will be different?
- Process, tech, roles, metrics

Who will be affected?
- Buy-in plan

How will they be prepared?
- Communication Plan

What could make it fail?
- Risk / resistance identification

How will we manage the risks?
- Risk treatment plans

Risk Treatment Plan

Reduce resistance by:
- Obtain organizational alignment
  - Align leaders
    - Vision, goals, success metrics
  - Engage stakeholders
    - Plan for level of involvement (t)
- Smooth state transition
  - Prepare for performance
    - ID knowledge and skills needed
  - Manage transition
    - Provide information to bridge gap

Involve, inform, and prepare people for change

Buy-in plan

Executives
- Who are the leaders?
  - (are they trusted?)
- Who is the sponsor?
  - (do they win a lot?)

Managers
- Are executives supportive?
- Are my peers lining up with it?
- What are metrics for success?

Workers
- What do I have to do next?
- How will it be measured?

Communication Plan

What	Goal
Announce	Awareness
Discuss	Understanding
Agree	Alignment
Involve	Participation
Prepare	Adoption

time

Direct involvement x Peers:
When/often? What? Goal? form?
Executives, Managers, Workers

Type 2 errors
- Not enough information
- They make it up

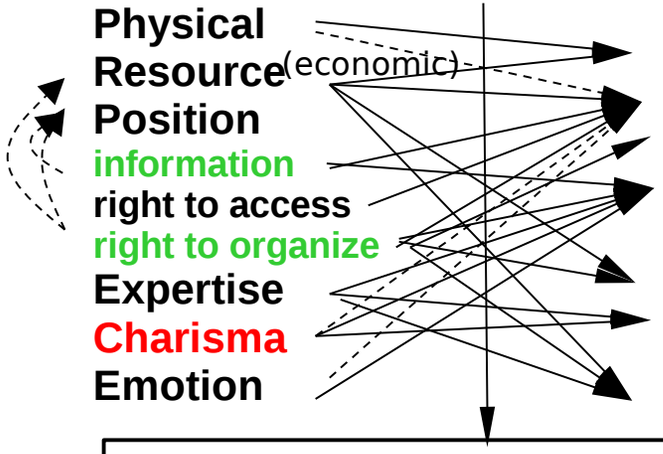
Type 1 errors
- Too much information
- Miss parts - overload

Type 3 errors
- Substitution
- Clarity for objections

Power is used to produce Influence

Best → Worst

P→I



Overt
- **force**
- **exchange** (one-time OK, repeated→expectation)
- **rules&procedures** (perceived right, enforcement)
- **persuasion** (weight f(belief in source))

Covert
- **ecology** (control environment*)
- **magnetism** (highly relative)

Bridging
- **threat of force** (economic)

reason, friendliness, coalition, bargaining, assertiveness, sanctions, higher authority

Friendliness: benefit person, success unlikely, position is low
Reason: benefit organization, success likely, position is high
Assertiveness: benefit organization, success unlikely, position is high

Adjusting to influence:
- compliance (no choice & resentment)
- identification (like idea/person & keep recharging)
- internalization (adopt as own & ownership changes)

Limit opponent's options
keep your options open

Credibility in context
Multi-thread stronger

Noise impairs performance
Variety relieves monotony
Seating effects interaction
Layout effects communication
Segregation inhibits communication
Danger increases tension
Smaller groups easier to participate
Attainable challenge → commitment
Worthwhile challenge → commitment
Interaction increases sentiments

Greater position or resource power → more strategies used
Reason on bosses, other methods on subordinates is common
More power distance → fall back on assertiveness is common
Reason is used most when expectation of success is high

Power is relative to the thing being influenced
Balance of power is achieved in most influence
Power is relative to the domain of Influence

Timing Patience, deadline, speed, fait accompli, surprise, status quo, stretchout
Inspection Open, limited, confession, qualified, third party, no admittance
Association Alliances, associates, disassociates, United Nations, Bribery
Authority Limited, approval, escalation, missing man, arbitration
Amount Fair and reasonable, Bullwarism, nibbling, budget bogey, blackmail, escalation, intersection, non-negotiable, Chinese auction
Brotherhood Equal, bigger, smaller, long-lost, brinkmanship
Detour Decoy, denial, withdrawal, good and bad guys, false statistics and errors, scrambled eggs, low balling, scoundrel

Tactics

Cause	Emotion	Behavior	Cure
Frustration	Hostility	Aggression/apathy	Venting
Threat	Fear	Fight/flight	Safety
Conflict	Anxiety	Inefficiency	Resolution
Violation of values	Guilt	Arbitrary Rejection	Punishment
Loss	Sorrow	Crying	Grieving
Failure	Self-pity	Overindulgence	Try try again

Reciprocation
- Costs more => worth more
- People tend to reciprocate any gifts

Contrast
- Substantial differences tend to be exaggerated

Reject and retreat
- Ask for something then lower request

Authority
- Experts know more

Commitments
- Are honored

Consistency
- Highly valued

Liking
- Say yes to who you like
- Physical attraction +
- Similarity +
- Compliments +
- More contact +
- Groups together bond
- Groups competing hate
- Associate with things that enhance self-image

Commitment
- Small commitments lead to big ones
- Active commitments better than passive
- Public image leads to self-image
- Increased compliance with investment
- Consistency causes decisions

Social proof
- Interpret as others do
- Replaces hard proof in uncertainty

Scarcity
- Scarcity implies value
- Loss > Gain
- Want restricted stuff
- Have it our way
- Exclusive info more valued
- Drop from abundance => more valued

Authority
- Cultural duty to authority
- Appearance => authority

Automaticity
- Desire not to think
- Strong desire not to rethink
- Default decision process
- Because
- Enhanced by rush, stress, ..

Mechanisms

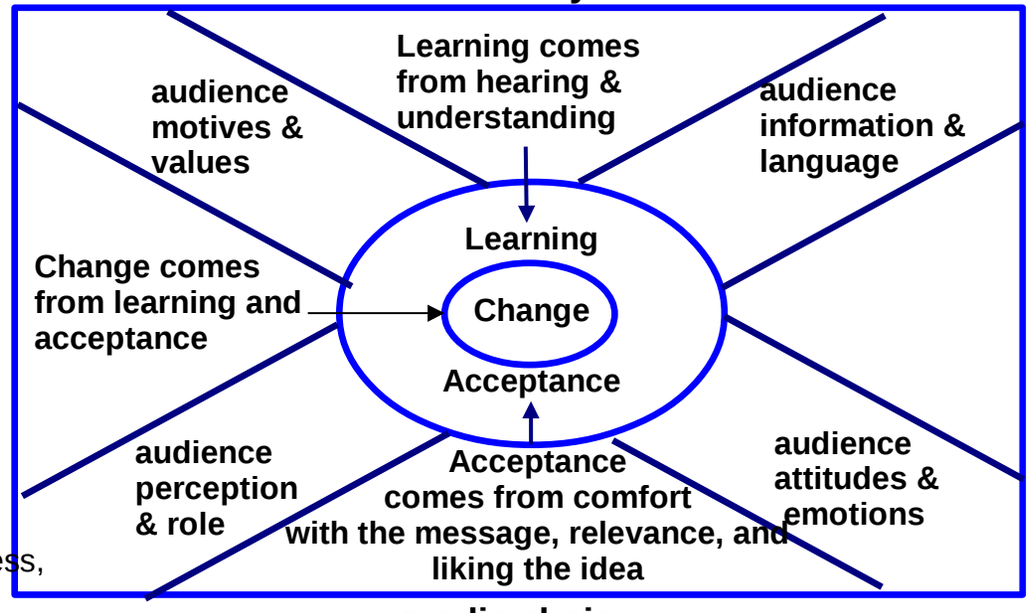
Persuasion Model

Message content & appeal

Present both sides
favored viewpoint last
start /end remembered
end remembered best
state conclusions
repetition helps
arouse need then fulfill
threats are rejected
desirable message first
ask for more, get more
stress similarities
tie hard issues to easy
don't create defensive
don't belittle other views
friendly/sympathetic
ask advice
appeal to self-worth, fairness, excellence

credibility

Introduce as an expert and you will be believed as one
Unless you're damned sure, say I reckon - Media may lend credibility



media choice

Letters are good when establishing justification or to get a letter back or when interruption is dangerous
Face to face is better when presence brings regard/respect, visual indicators will help, or more or less may be desired

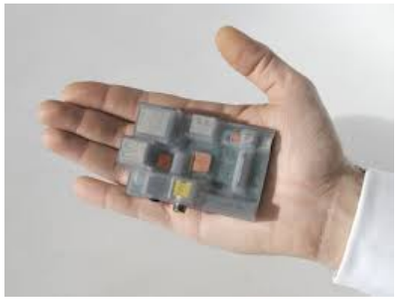
situation setting & rewards

make the audience feel worthwhile
reinforce opinions
people like balance
ambiguity upsets
tendency to resolve ambiguity quickly
social forces
account for audience facts, methods, goals, and values
power issues

Influence

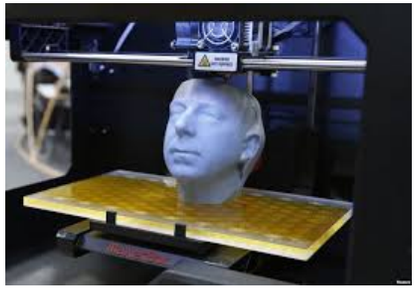
~5 years ago

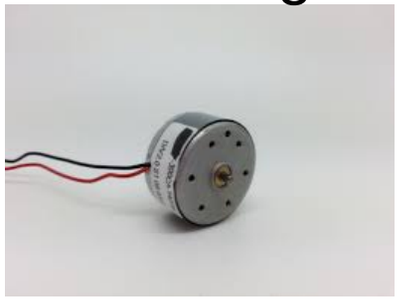
Hacking tools

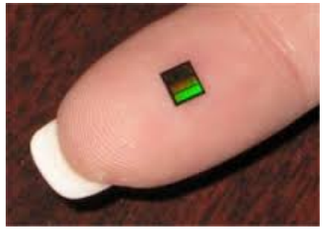

Airport Extreme – USB sniffer – raspberry pie - bootable linux - nano bug



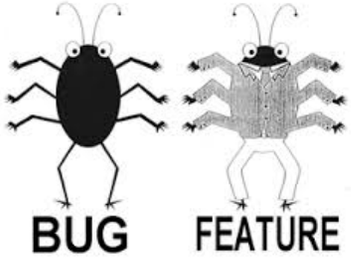




Quad copter – 3d printer – 3d printer mask – gene sequencer – EM generator

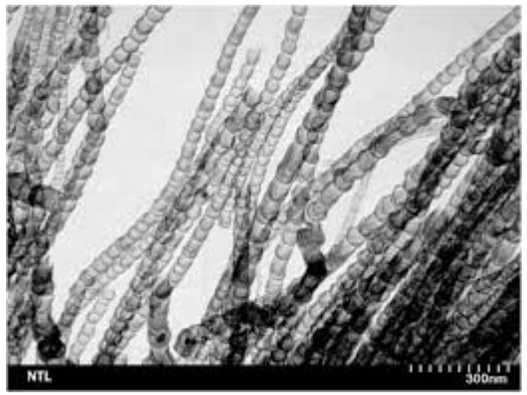



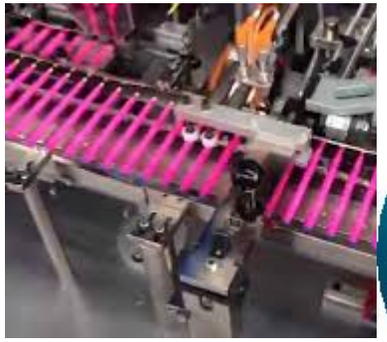


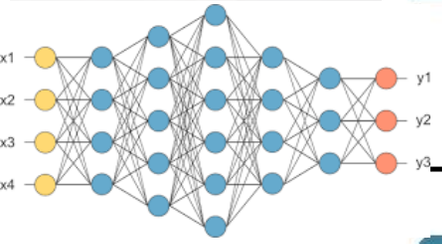


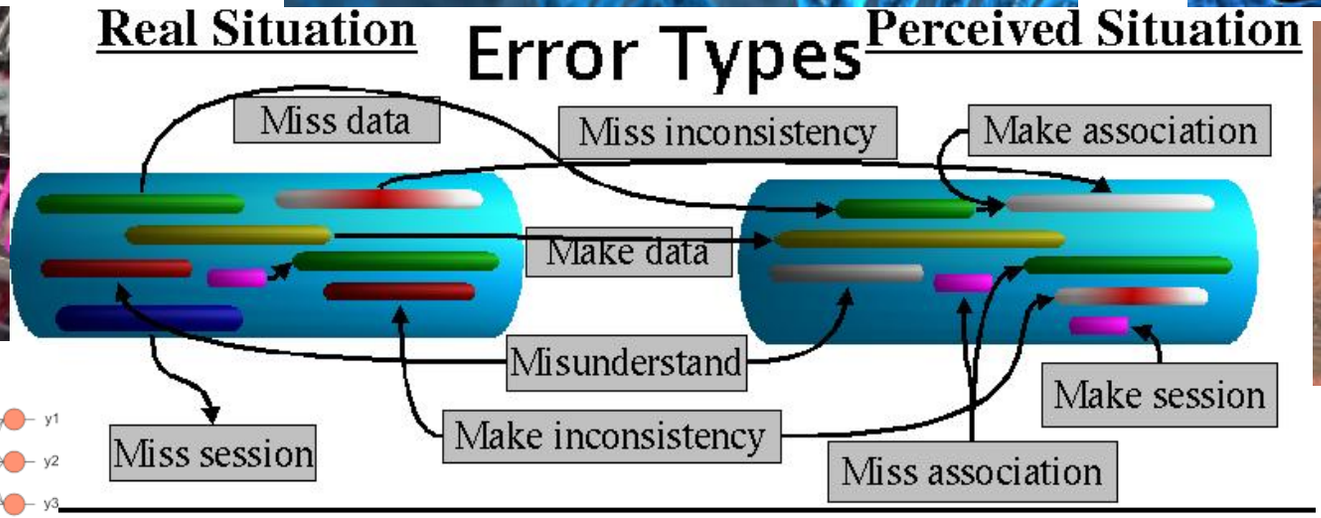
Fiber camera – tracking device – better bug – false eye computer - feature

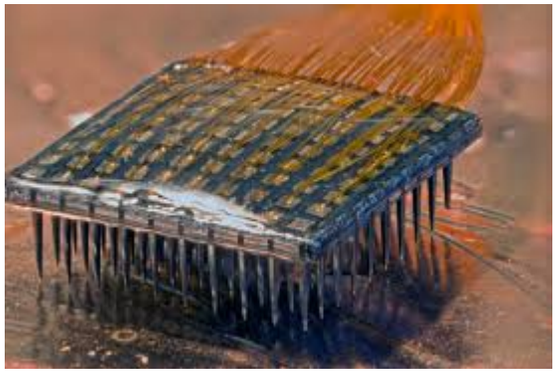
Cyber Warfare – The Small Picture

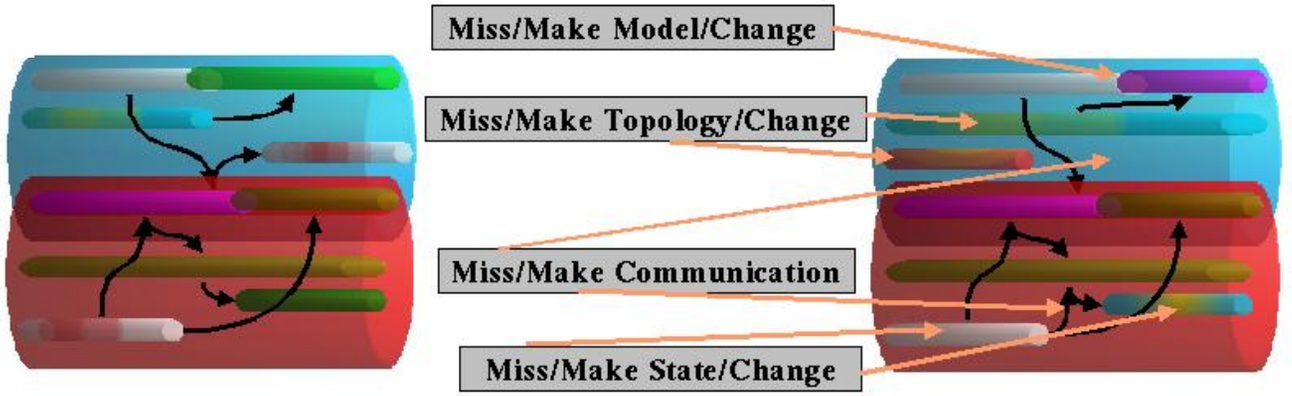




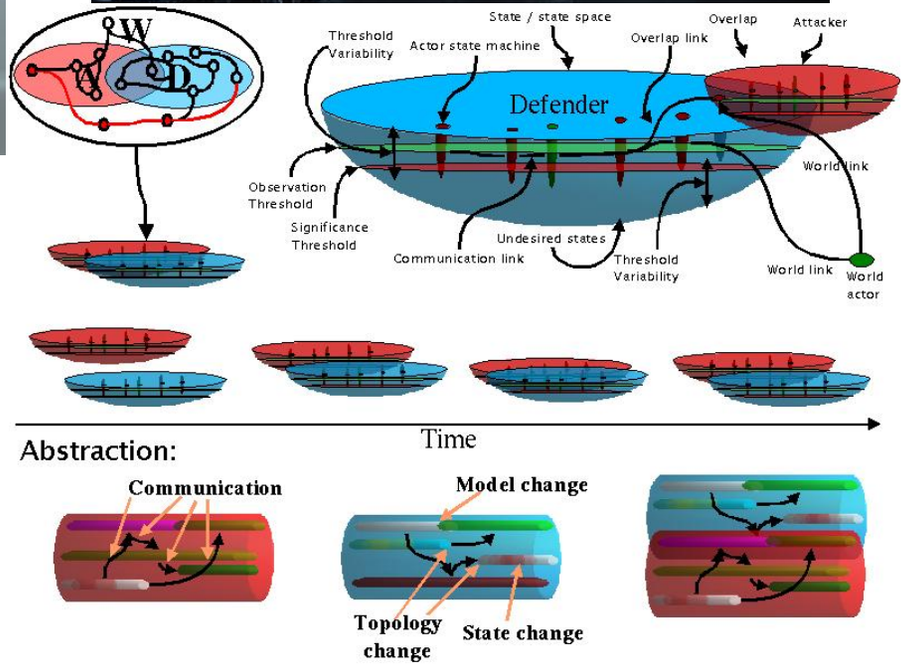








Cyber Warfare: Roll-up



Source: Shutterstock

Thank You