Exploiting Complexity

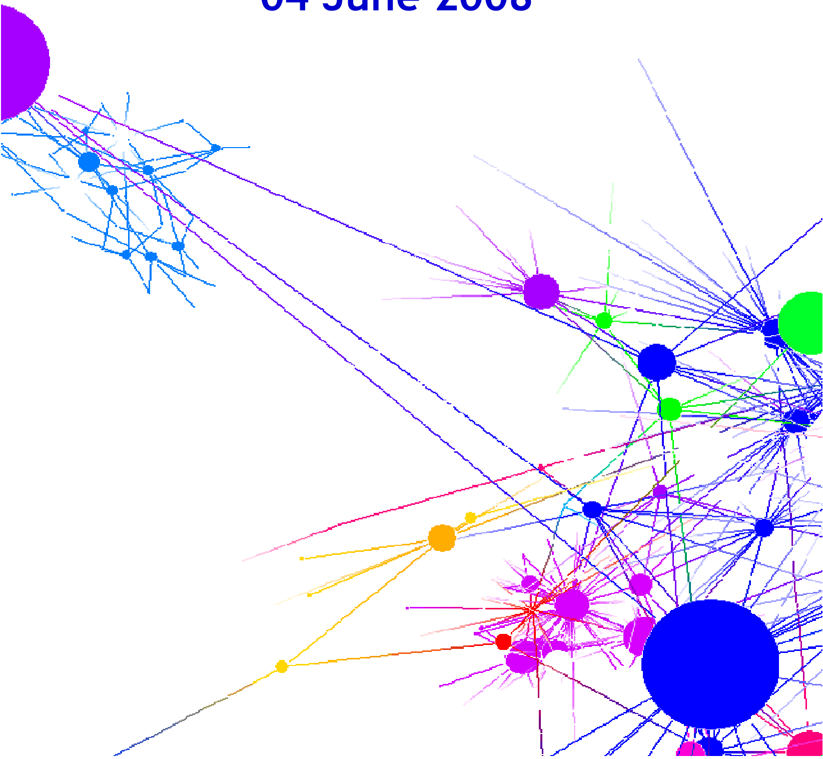
The abaci Partnership

The Impact of Cyberspace on the Nature of Command

Patrick Beautement

For the Portuguese Military Academy

04 June 2008



Contents

What is Cyberspace?

The electromagnetic domain.

A 'logical' world which extends the real world.

A world inhabited by purposeful, 'artificial beings'.

The virtual domain of 'stored mind'

Contents

01 A Model of Command for Cyberspace

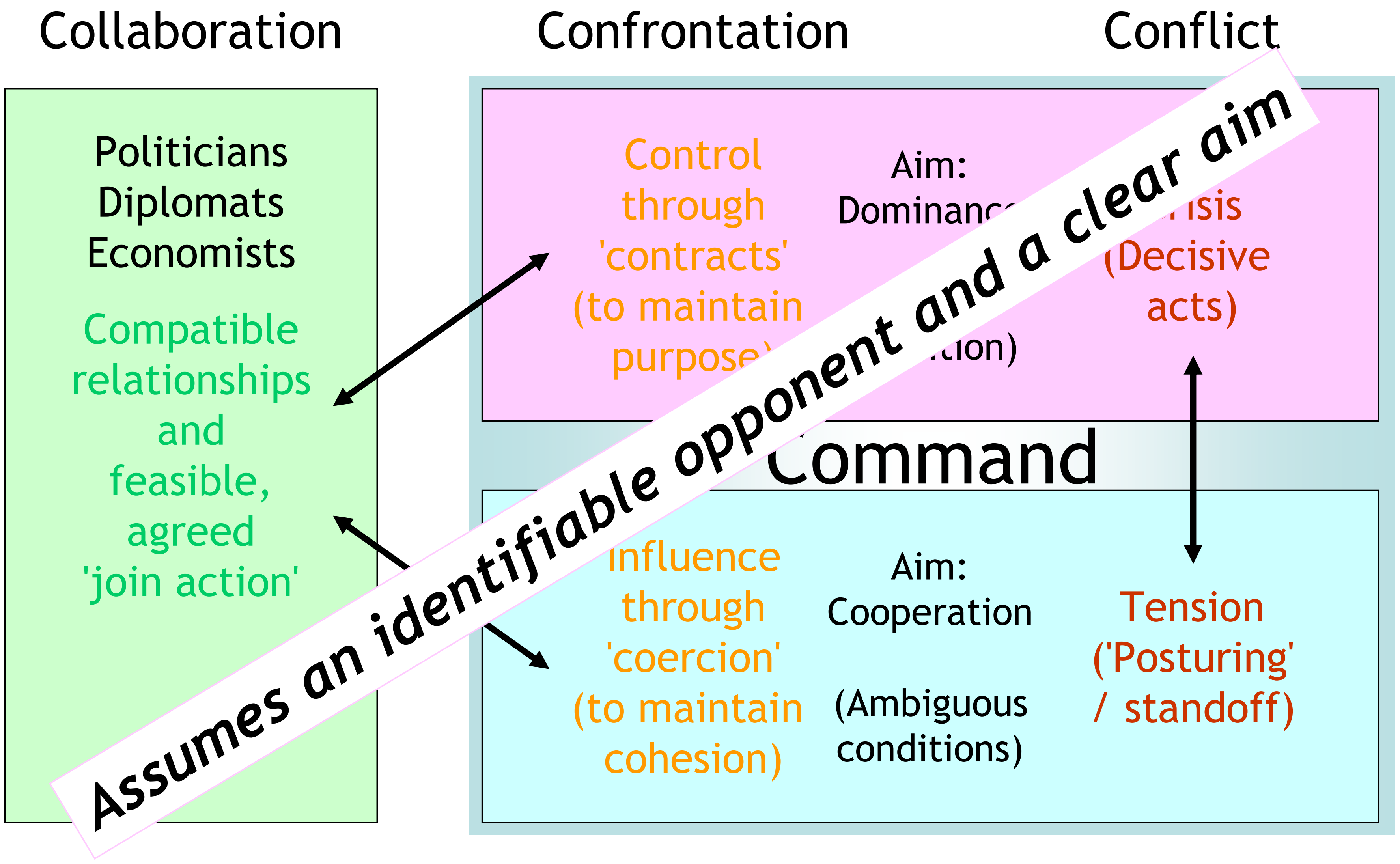
02 Opportunities for Command in Cyberspace

03 Working with Cyberspace - Human-machine Teams

04 Vulnerabilities and Countermeasures

05 Impacts - Guiding Principles for Command in Cyberspace

01 A High-level model of Command



Collaboration

Confrontation

Conflict

Politicians
Diplomats
Economists

Compatible relationships and feasible, agreed 'join action'

Control through 'contracts' (to maintain purpose)

Aim:
Dominanc

tion)

isis
(Decisive acts)

Command

Influence through 'coercion' (to maintain cohesion)

Aim:
Cooperation

(Ambiguous conditions)

Tension
('Posturing' / standoff)

Assumes an identifiable opponent and a clear aim

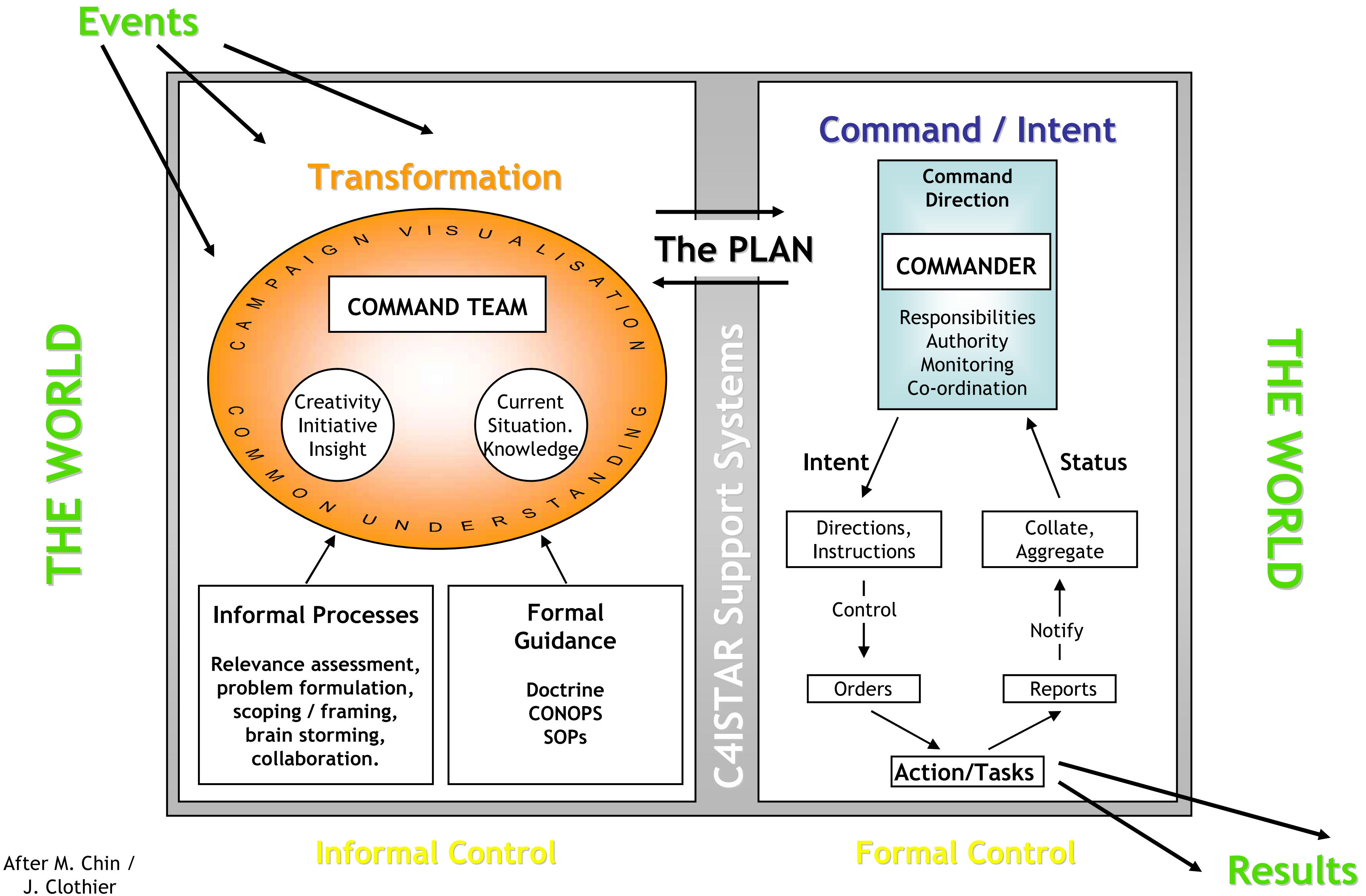
01 Command and the use of 'Force'

- Commanders* understand the Clausewitz Trinity (People, State and Force) in confrontation and conflict hey:
  - provide the driving 'logic' - they are th of the 'force' they command and th
  - develop and compare in options
  - understand opp metric force' and unleash it t to decisive effect
  - con ys and means available - judge es and assimilate their significance
  - he organisation - setting authorities and ities to enable adaptation 'on the day'
  - ntinually judge between conflicting imperatives - striking and accepting 'compromise' - to exploit flexibility

What is the nature of 'force' and the role of command - in "War among the People" - and in Cyberspace? .. ..

* See "Utility of Force" by General Sir Rupert Smith

01 Command in the Industrial Age



After M. Chin /
J. Clothier
DSTO 1998

01 Command Mindset for Cyberspace

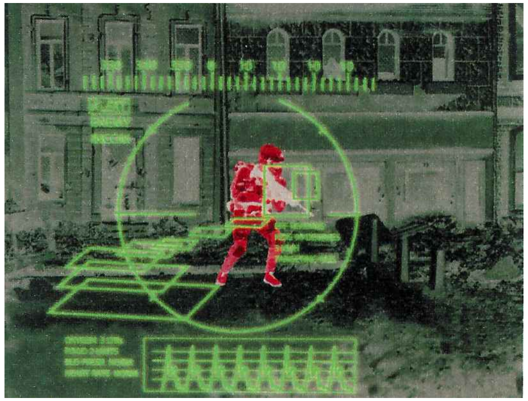
Industrial Command Mindset	Mindset for 'War-among-the People'	Mindset f Cybe
Clear start, conflict, outcome (win / loose)	Always ongoing - not 'our' type of success	Alwa
Known enemy with clear doctrine	Opponents and ai hard to identi	and aims ually adapting
Know us / them and ours / theirs	Many va flui	Many varied 'actors' including non-human
The Plan: end-states defined. One 'pic	state, intent stated	***No Plan***. Who's values / intentions matter?
Conduct wi 'agreed'	nduct seen as 'extremist' / alien	Conduct unbounded and always novel
B eld, eapons	Conflict anywhere, anytime, anything	Influence anywhere, anyhow - nothing safe
real world. ecided by politicians	In the real world. Decided by the people	Virtual, 'inaccessible' - never decided

Needs: open eyes, open minds and an adaptive stance - ready to be exploited through comprehensive approaches

Contents

01 A Model of Command for Cyberspace

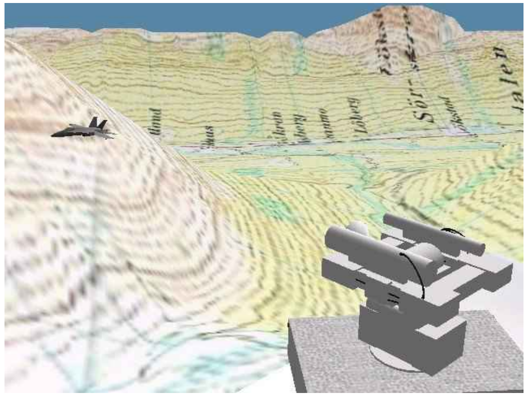
02 Opportunities for Command in Cyberspace



But, such consummate skill,
such ability,
such adaptability,
such numbing ruthlessness,
such a use of weapons ...

when *anything* could become a weapon...

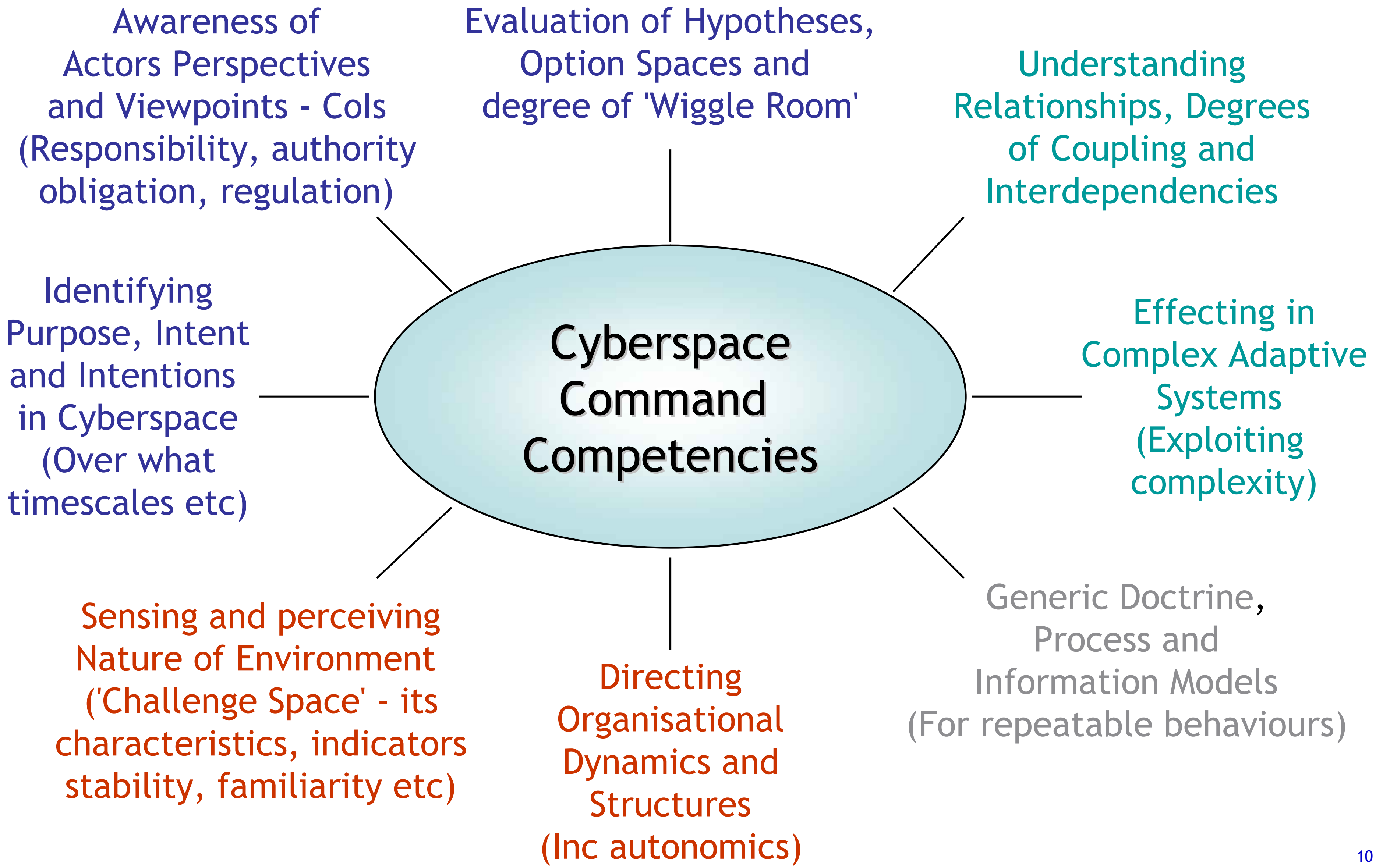
From Iain M Banks "Use of Weapons"



02 Opportunities for Command in Cyberspace

- The unbounded, uncontrolled nature of Cyberspace seems a threat, but it is full of command opportunities eg, providing:
  - routes to change public opinion, shape markets etc
  - novel ways of sensing and acting 'at a distance' - undetected
  - new means to deceive - rich opportunities for innovation
  - new ways of influencing - eg, via a myriad of intermediaries
  - means to exploit 'swarm intelligence' - via new 'creatures'
- However, to exploit these we must master (at a minimum):
  - sensing (ISTAR), perception and visualisation of Cyberspace
  - intent, purpose and opportunities available in Cyberspace
  - Human-machine Teaming and effecting of Cyberspace actors
  - vulnerabilities and countermeasures

02 Command of Cyberspace - Challenges



Cyberspace Command Competencies

Awareness of Actors Perspectives and Viewpoints - CoIs (Responsibility, authority obligation, regulation)

Evaluation of Hypotheses, Option Spaces and degree of 'Wiggle Room'

Understanding Relationships, Degrees of Coupling and Interdependencies

Identifying Purpose, Intent and Intentions in Cyberspace (Over what timescales etc)

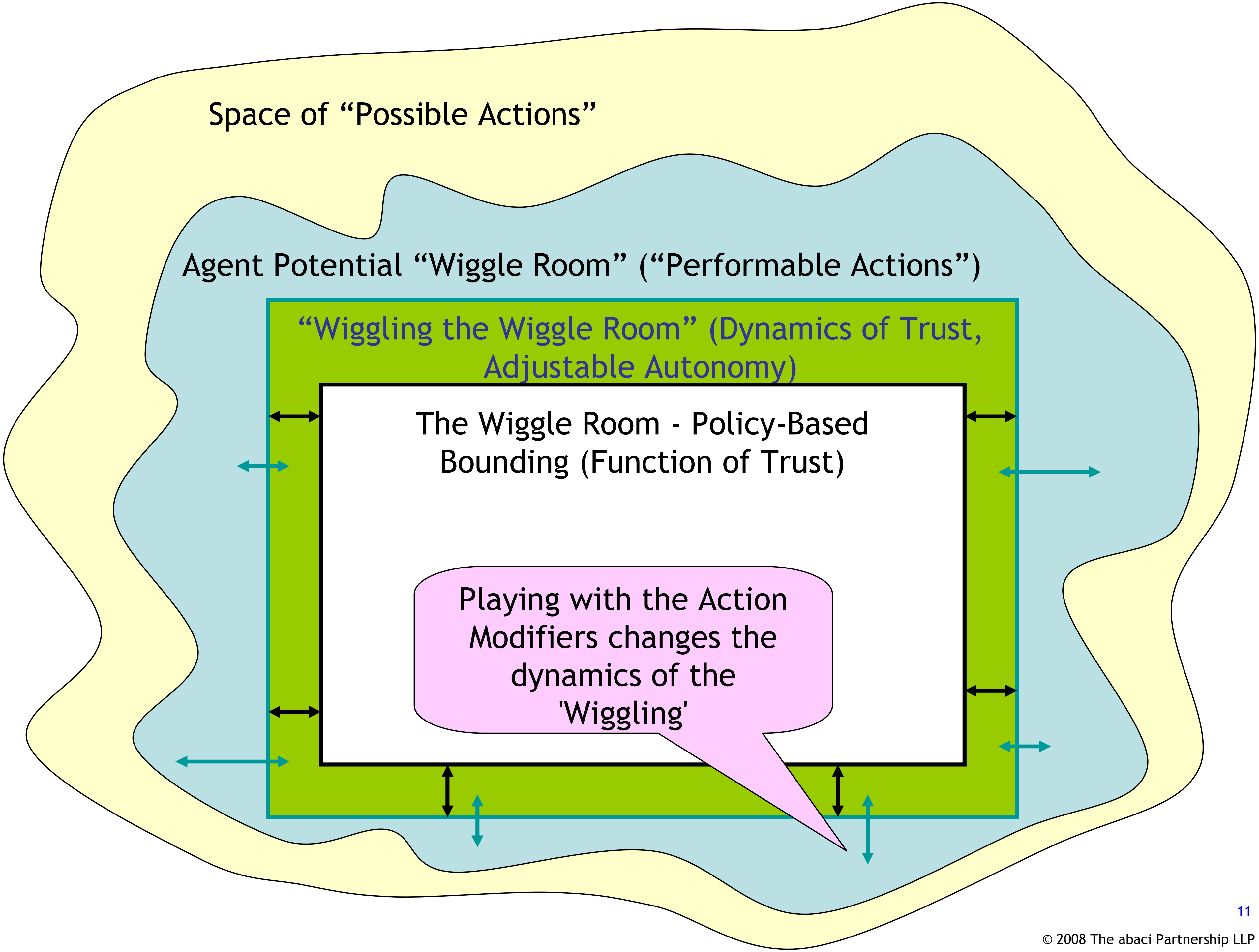
Effecting in Complex Adaptive Systems (Exploiting complexity)

Sensing and perceiving Nature of Environment ('Challenge Space' - its characteristics, indicators stability, familiarity etc)

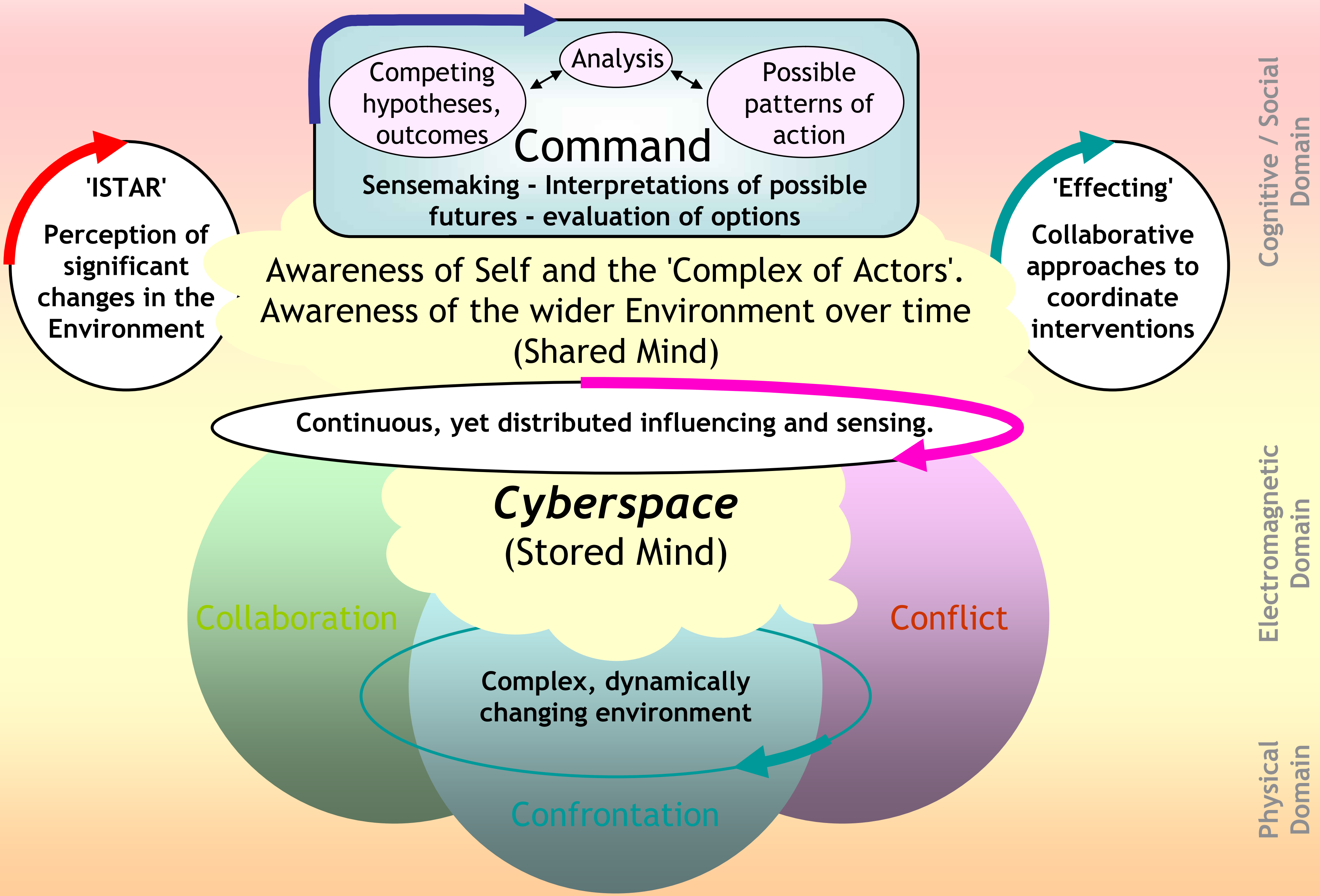
Directing Organisational Dynamics and Structures (Inc autonomics)

Generic Doctrine, Process and Information Models (For repeatable behaviours)

CoI = Communities of Interest


Space of “Possible Actions”
Agent Potential “Wiggle Room” (“Performable Actions”)
“Wiggling the Wiggle Room” (Dynamics of Trust, Adjustable Autonomy)
The Wiggle Room - Policy-Based Bounding (Function of Trust)
Playing with the Action Modifiers changes the dynamics of the 'Wiggling'

02 Model of Command for Cyberspace



Competing hypotheses, outcomes

Analysis

Possible patterns of action

Command

Sensemaking - Interpretations of possible futures - evaluation of options

'ISTAR'

Perception of significant changes in the Environment

'Effecting'

Collaborative approaches to coordinate interventions

Awareness of Self and the 'Complex of Actors'. Awareness of the wider Environment over time (Shared Mind)

Continuous, yet distributed influencing and sensing.

Cyberspace

(Stored Mind)

Collaboration

Conflict

Complex, dynamically changing environment

Confrontation

02 War among the People - where is the 'New Enemy'?

- Probably (See Michael Lwin's "General Tzu's Army - OPFOR of the Future") not:
  - on a defined battlefield - where we expect them to be
  - constrained by boundaries - they act wherever / whenever. culturally 'strange' - different motivations, values etc
  - part of a western-style 'fighting force' - commanded 'from the centre' - employ social networks
  - necessarily part of 'them', 'out there' … they are 'in here' and transparent to us
- Hard to find because we are blinded by our assumptions:
  - we use of inappropriate sensors which leads to inappropriate perceptions
  - they know where we look, and so they make sure they are not there to be seen

02 Effects-based ISTAR - From information to abstract i2

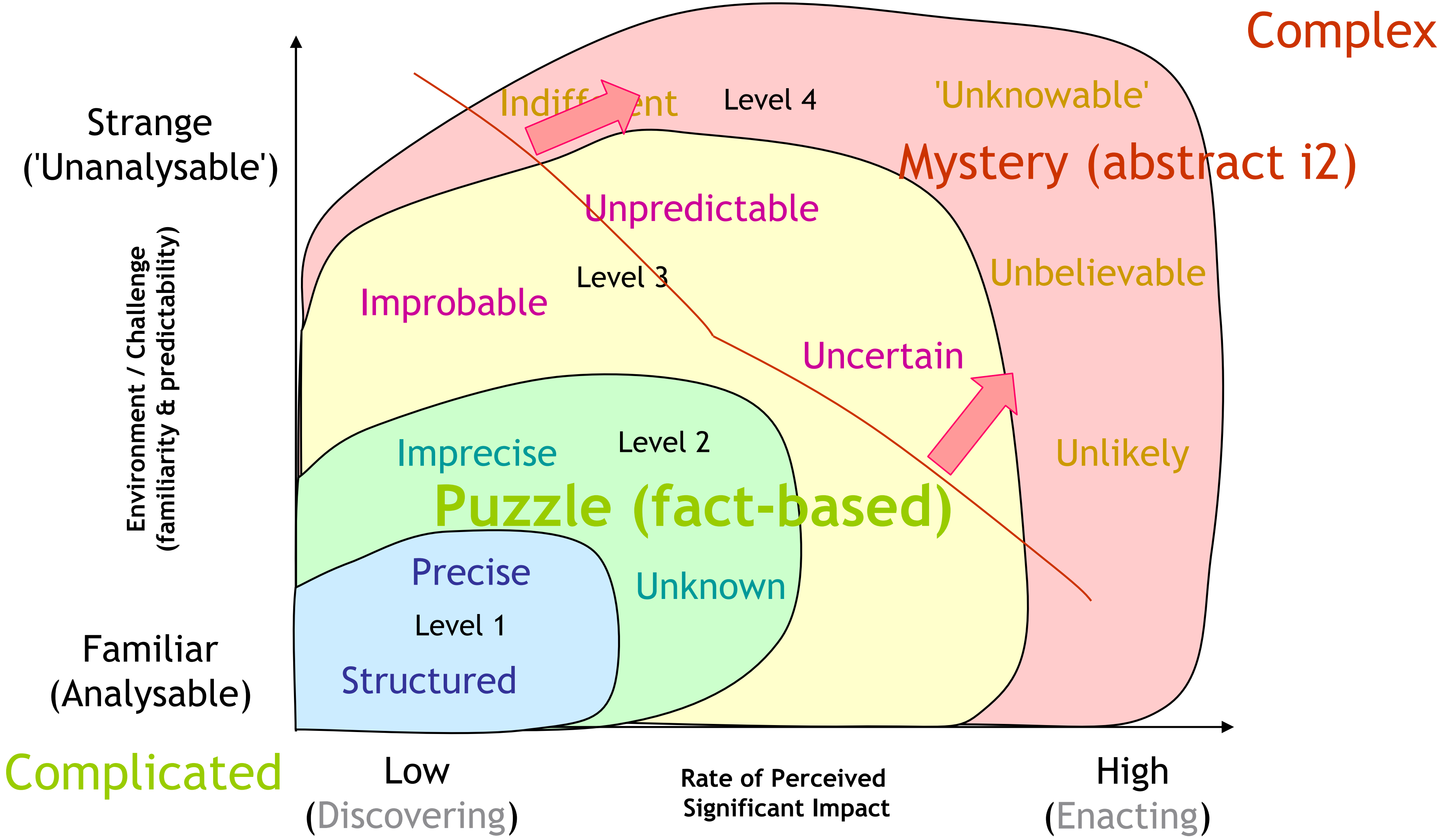
- Puzzle: eg, Gulf War 1 (can be a procedure where envir :
  - Know the puzzle (bound the pr omething is missing
  - Able to clas m(s) and describe them in 'fact-like' terms
  - rch for or collect the missing item(s)
  - Able to fit the new fact in the puzzle and confirm it is the 'right' piece

Pre-defined taxonomies and fact-based data-structures

- Mystery: eg, Iran's intentions (not a 'process' - involves imagination, creativity because environment strange / uncertain):
  - Have no / little knowledge of the nature or extent of t
  - Build theories / alternative comp r 'fantasies'
  - Project the 'm ure and compare to the perceived world
  - cators / weights of evidence that might exist / be required
  - Purposefully direct the sensing (shake the tree first) to support / refute etc
  - No 'final, correct' answer, instead: judgement, assessment, probability etc

Dynamically-generated meaning - linked, evolving nets of abstract i2

02 ISTAR of Cyberspace



i2 = Information and Intelligence

02 Views on 'Abstract Information and Intelligence' (Abstract i2)

- Commanders (We use abstract i2):
  - I solve problems and need ISTAR partnership from Levels 1 to 4
  - ISTAR must support me while I work with multiple, inconsistent hypotheses
  - I need to make a decision
- Int Analysts (We work with abstract i2):
  - I analyse data - I add meaning, linkages
  - I look for indicators, trends, patterns …
  - I develop abstractions - I need to store, work with, retrieve and share these
  - I weigh hypotheses, am concerned with confidence, trust and source protection
  - I make judgements / assessments

- ***BUT***, the Computer Science / System Engineering view is:
  - There are fact-like things
  - There exists a suitable taxonomy
  - All facts can be categorised
  - Relationships between facts can be defined (mostly a-priori)
  - Facts are used in processes
  - Toolsets store, retrieve, display and manipulate facts
  - The Higher-level abstractions used by humans are outside the 'system of interest' ***- I don't understand or cater for 'abstract i2'***

Contents

01 A Model of Command for Cyberspace

02 Opportunities for Command in Cyberspace

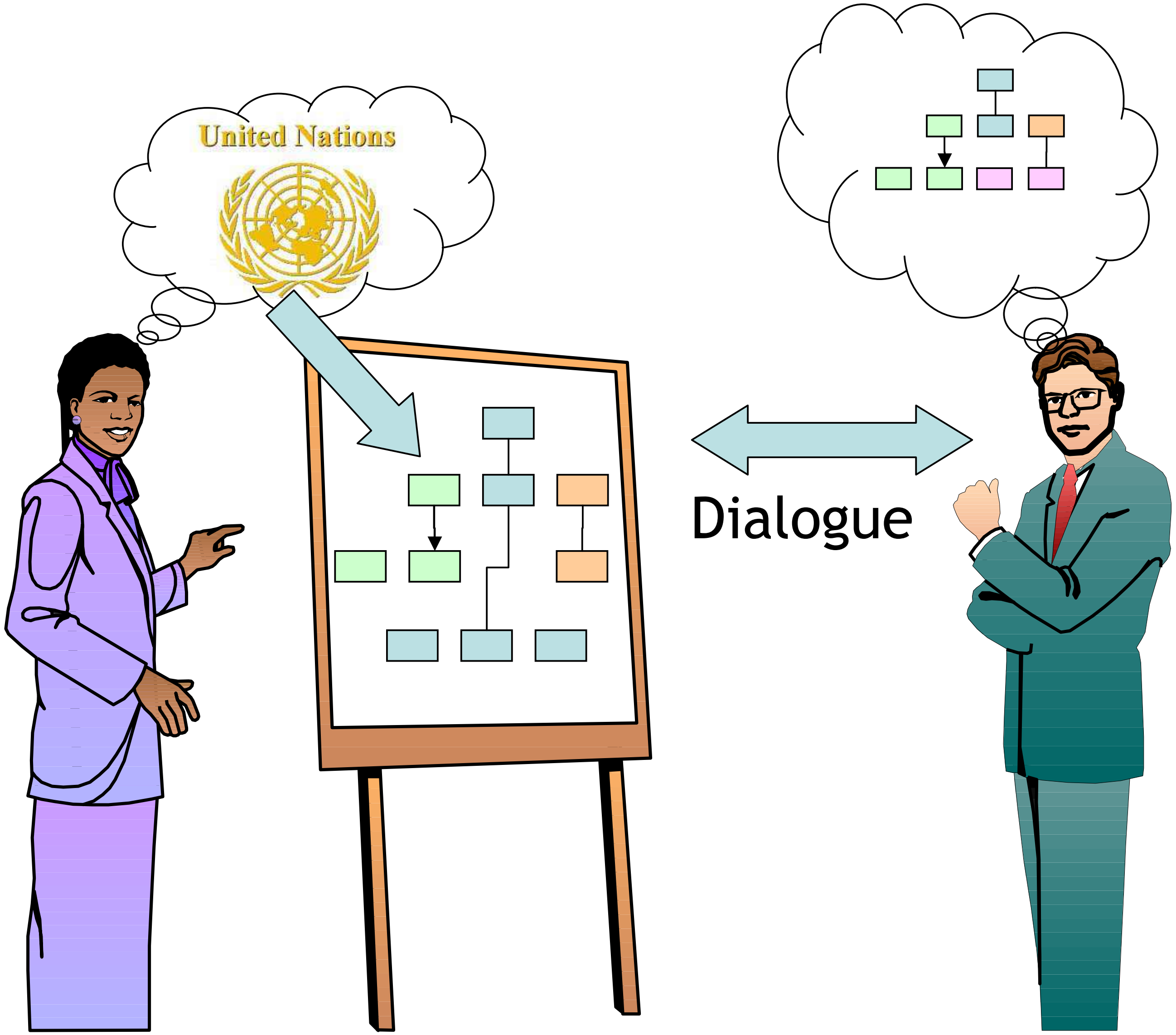
03 Working with Cyberspace - Human-machine Teams

04 Vulnerabilities and Countermeasures

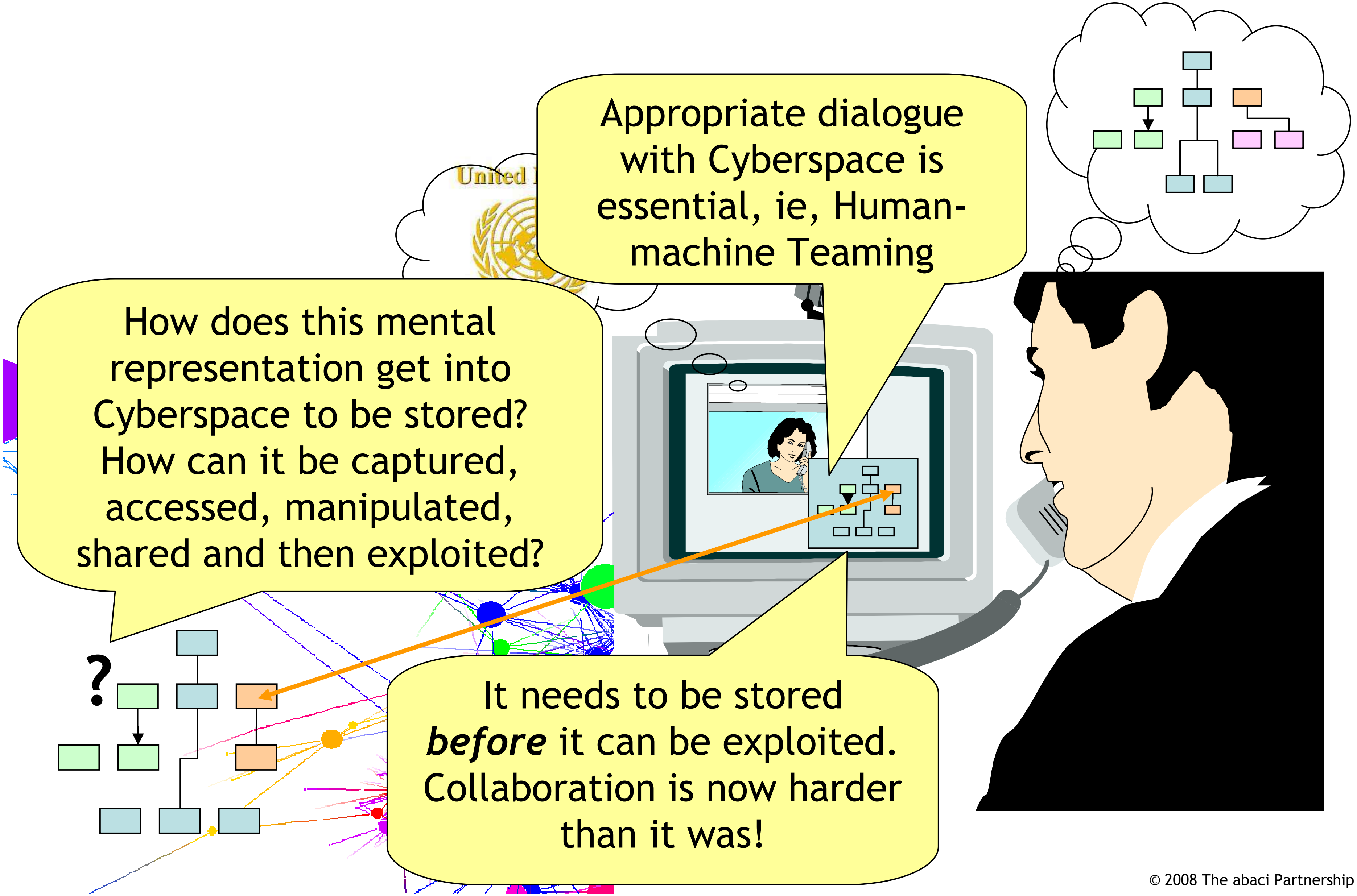
05 Impacts - Guiding Principles for Command

Courtesy of Mark Ho

03 Teaming before Machines



03 Human-machine Teaming (HMT)

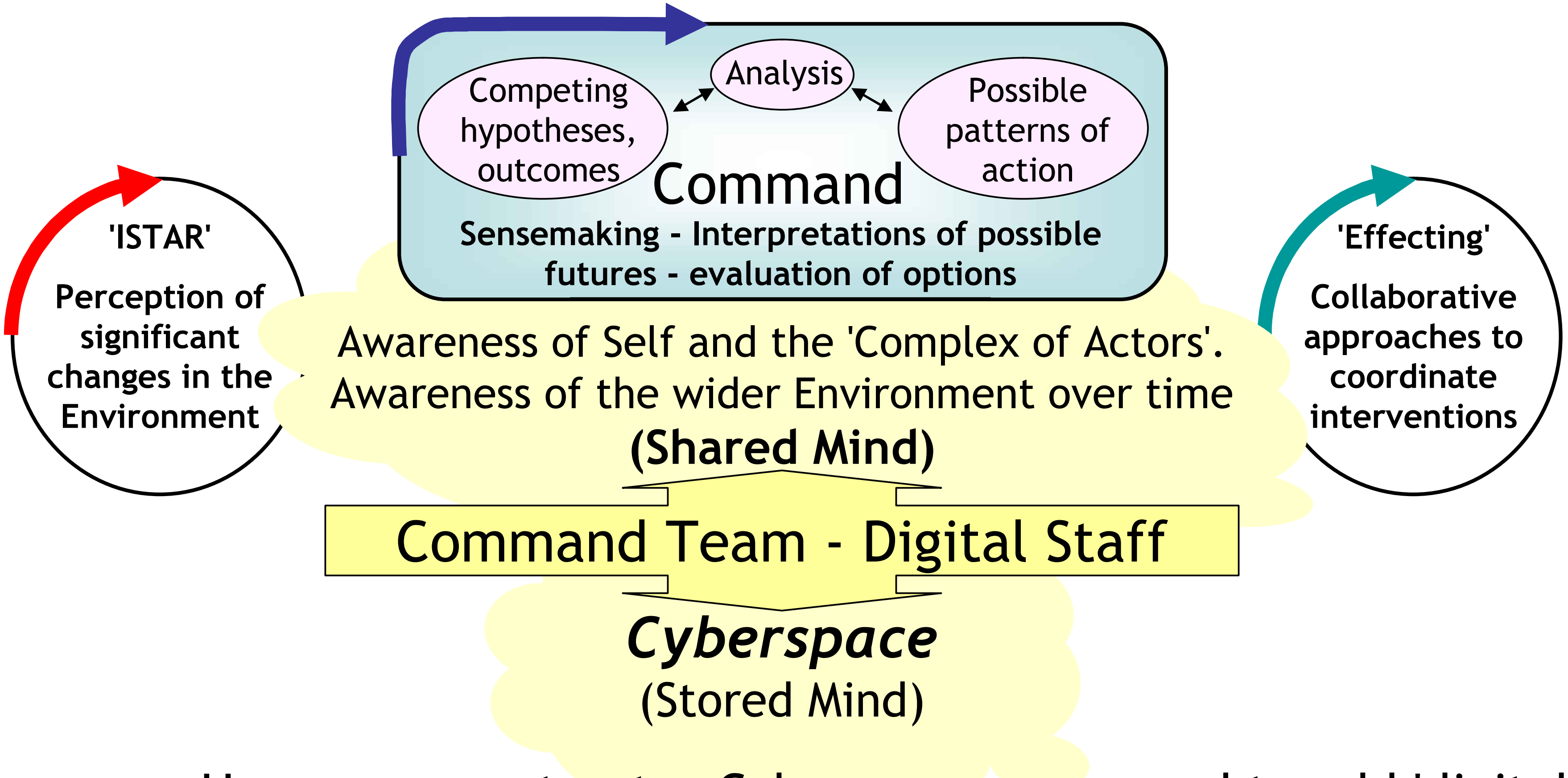


Appropriate dialogue with Cyberspace is essential, ie, Human-machine Teaming

How does this mental representation get into Cyberspace to be stored? How can it be captured, accessed, manipulated, shared and then exploited?

It needs to be stored ***before*** it can be exploited. Collaboration is now harder than it was!

03 Human-machine Teaming - the Need


Competing hypotheses, outcomes
Analysis
Possible patterns of action
Command
Sensemaking - Interpretations of possible futures - evaluation of options
'ISTAR'
Perception of significant changes in the Environment
'Effecting'
Collaborative approaches to coordinate interventions
Awareness of Self and the 'Complex of Actors'.
Awareness of the wider Environment over time
(Shared Mind)
Command Team - Digital Staff
Cyberspace
(Stored Mind)

- Humans cannot enter Cyberspace - we need to add 'digital agents' to our Command Team (who can act on our behalf)
- It is not enough for Cyberspace to just support structured storage and retrieval of facts - meaningful linking and exploration of hypotheses / meaning must be supported …

03 Human-machine Teaming

- Example 1: the topic under consideration is ‘simple’ and the dialogue between the user and machine is basic:
  - Human: “Are there any T80 tanks near location ‘L’?” Machine: “There are no tanks”. Human: “Is that because we have not yet looked, or we have looked and have seen none or that there are actually none there?”. Machine: “We over flew the area an hour ago and none were there then”.
- Example 2: the topic under consideration is more complex and the resulting dialogue will have to be much more sophisticated:
  - Human: “Why has the allegiance of person ‘Y’ changed?”. Machine: “Changed in which way?”. Human: “Such that we can no longer rely on their support”. Machine: “Do you have a previous example of such a change that I can use in my analysis?”

03 Dimensions of HMT Interaction

TIER 1

TIER 2

TIER 3

TIER 4

'BLIND' DELIVERY

INCRE

'Dumb' delivery (text reading)

'Tailored' delivery (based on assumptions: which nature t, filled clicked hat etc)

'Profiled' interactions

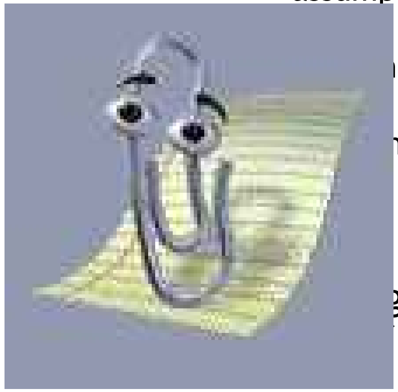
Stereotyped (limited) interaction

Rule-basec nteractior 'trees'

ised action (Business-like terac

truct egoti nse c nd ot ploys omir

Fully committed 'relationship'



guides

atars

eg: 'Smart' white goods

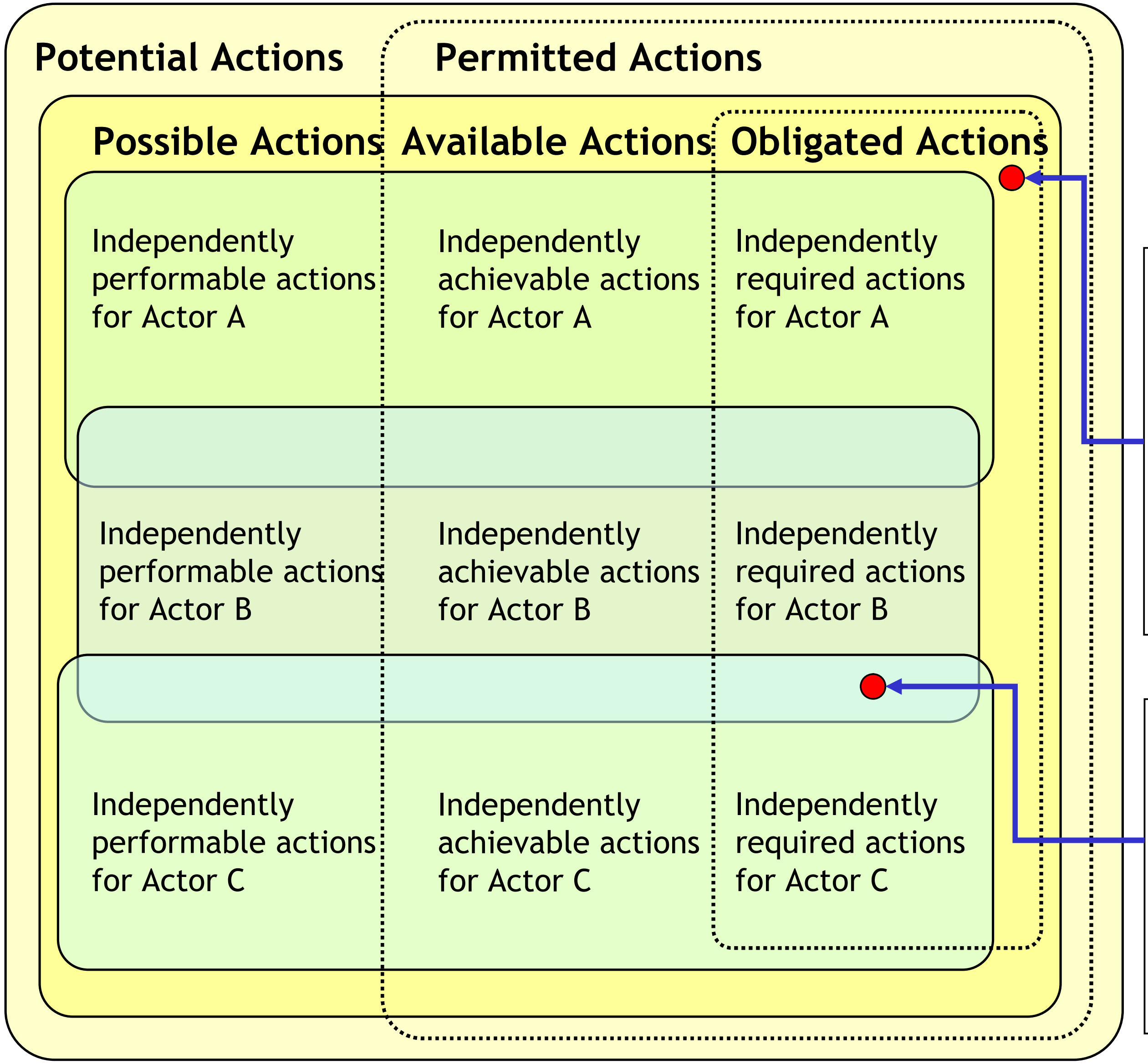
eg: Entertain

e

'Intelligent", free enough to take more than one possible future. Complex and emergent.

companions

03 HMT - Dimensions of Adjustable Autonomy



Potential Actions

Permitted Actions

Possible Actions	Available Actions	Obligated Actions
Independently performable actions for Actor A	Independently achievable actions for Actor A	Independently required actions for Actor A
Independently performable actions for Actor B	Independently achievable actions for Actor B	Independently required actions for Actor B
Independently performable actions for Actor C	Independently achievable actions for Actor C	Independently required actions for Actor C

ihmc
INSTITUTE FOR HUMAN & MACHINE COGNITION

Example 1: When an obliged action is not performable, do we increase the range of performable actions or decrease the range of obliged actions?

Example 2: How do we resolve tensions where there is overlap between individuals, teams, organisations and tasks?

CoAX - Coalition Agents eXperiment

**AIAI, BBN, CMU, Dartmouth, DSTO, GITI,
Lockheed Martin ATL, NRL, Potomac Inst., U.Maryland,
U.Michigan, QinetiQ, UT-Austin, UWF/IHMC**

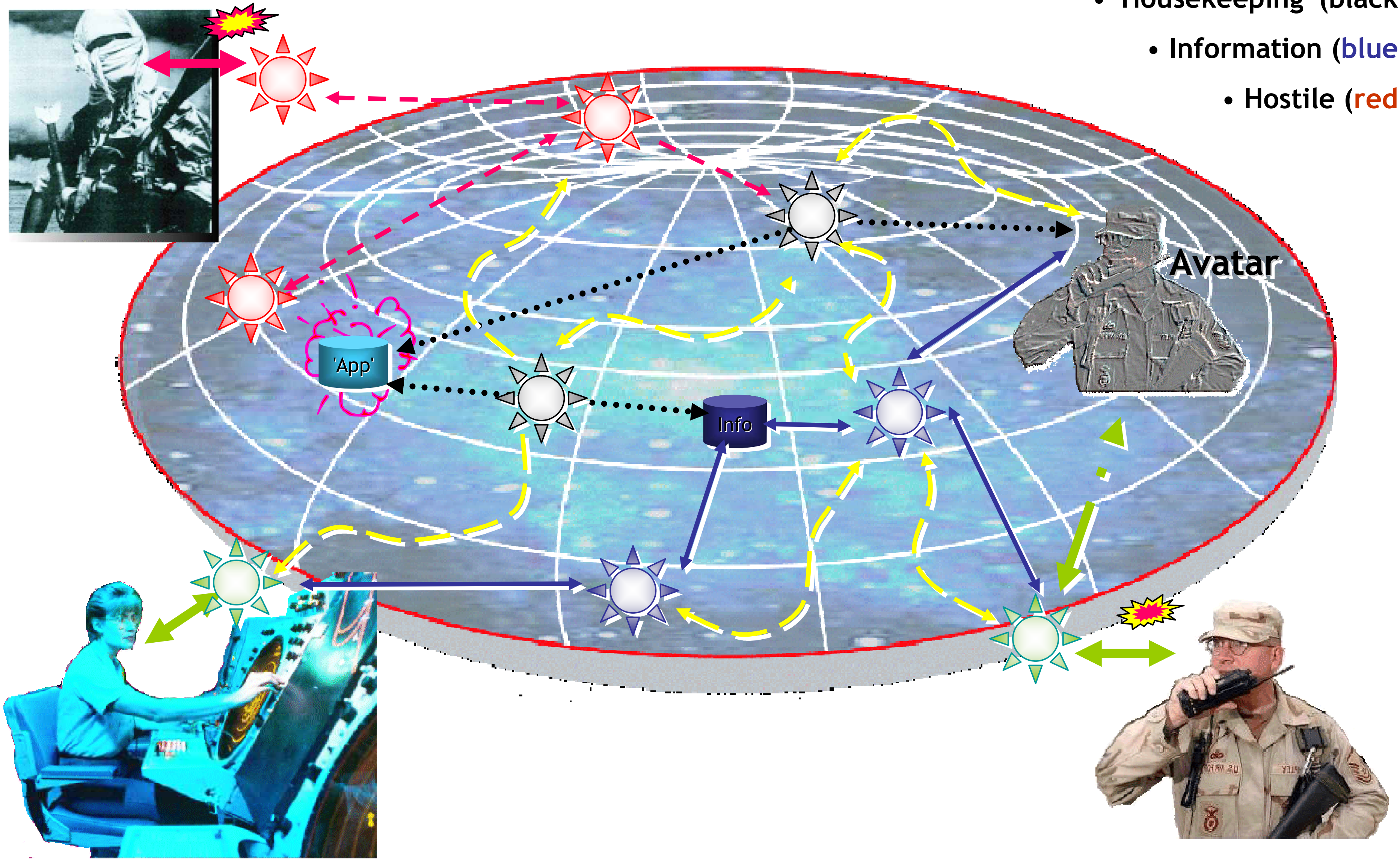
**Support from AFRL, ARL, Boeing, DRDC, DSTL, ISX, MITRE,
MIT Sloan, NWDC, OBJS, Schafer, Stanford, TTCP, USC/ISI, USPACOM**

http://www.aiai.ed.ac.uk/project/coax/

03 Types of Agent

Four types of agent:

- Mediator (green),
- 'Housekeeping' (black),
- Information (blue),
- Hostile (red).

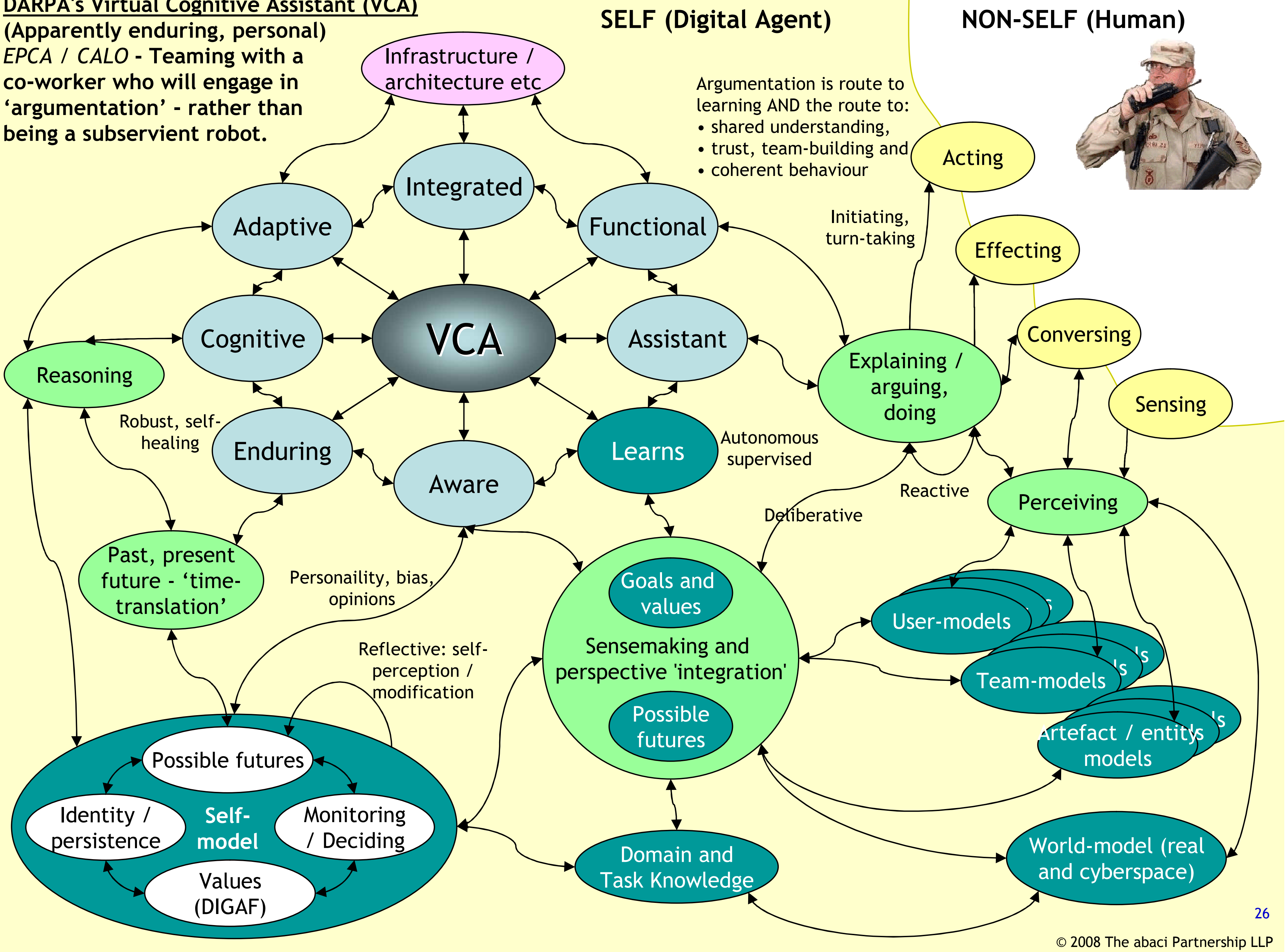


KEY: Opponent Activities ◀ – – – – ▶ Inter-Agent Conversation ◀ – – – – ▶ Human-Agent 'Conversation' ◀━━ · ━▶ 'Housekeeping' ◀••••••▶ Information transfers ◀━━━━▶

DARPA's Virtual Cognitive Assistant (VCA)

(Apparently enduring, personal)

***EPCA / CALO* - Teaming with a co-worker who will engage in ‘argumentation’ - rather than being a subservient robot.**



SELF (Digital Agent)

NON-SELF (Human)

Argumentation is route to learning AND the route to:
- shared understanding,
- trust, team-building and
- coherent behaviour

Infrastructure / architecture etc

Integrated

Adaptive

Functional

Cognitive

VCA

Assistant

Reasoning

Enduring

Aware

Learns

Robust, self-healing

Autonomous supervised

Past, present future - ‘time-translation’

Personaility, bias, opinions

Reflective: self-perception / modification

Goals and values

Sensemaking and perspective 'integration'

Possible futures

Possible futures

Identity / persistence

Self-model

Monitoring / Deciding

Values (DIGAF)

Domain and Task Knowledge

Initiating, turn-taking

Acting

Effecting

Conversing

Sensing

Explaining / arguing, doing

Reactive

Deliberative

Perceiving

User-models

Team-models

Artefact / entity models

World-model (real and cyberspace)

Contents

01 A Model of Command for Cyberspace

02 Opportunities for Command in Cyberspace

03 Working with Cyberspace - Human-machine Teams

04 Vulnerabilities and Countermeasures

05 Impacts - Guiding Principles for Command

CONTROL OF SPACE
Space Surveillance
Protection
Assured Access
Prevention
Negation
Ability to Assure Access, Freedom of Operations, and Deny it to the Enemy

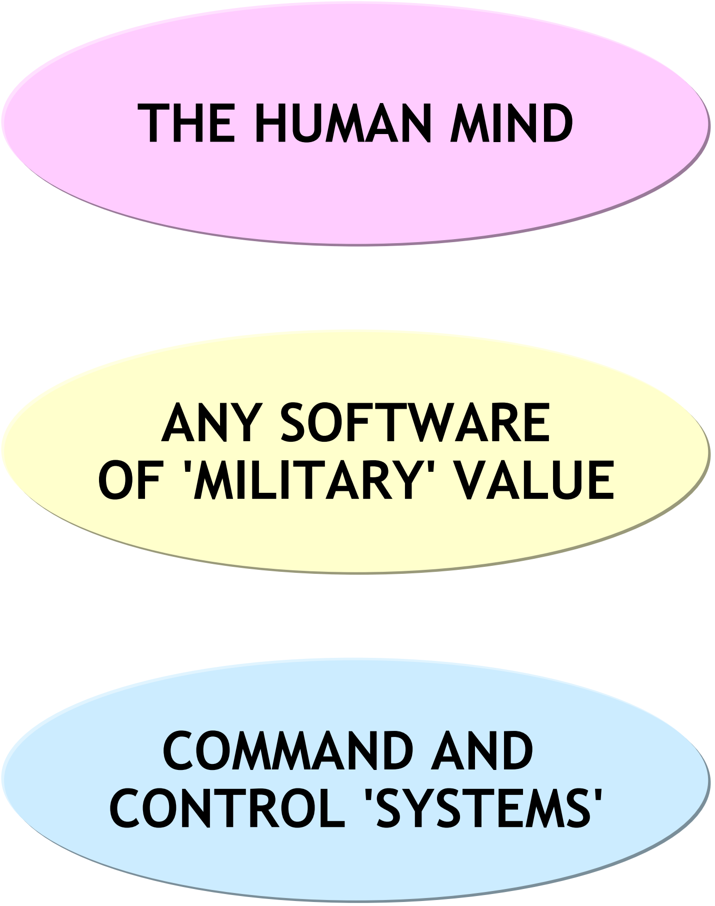
04 Vulnerabilities

- Vulnerabilities in three areas:

'INFORMATION':
Attack ability to think, including through information systems, psyops and deception, anywhere

'SOFTWARE':
Exploitation of software capabilities everywhere

COMMAND AND CONTROL:
Attack C4ISTAR wherever.
General means: EW, SW, IW, physical attack, etc



THE HUMAN MIND

ANY SOFTWARE OF 'MILITARY' VALUE

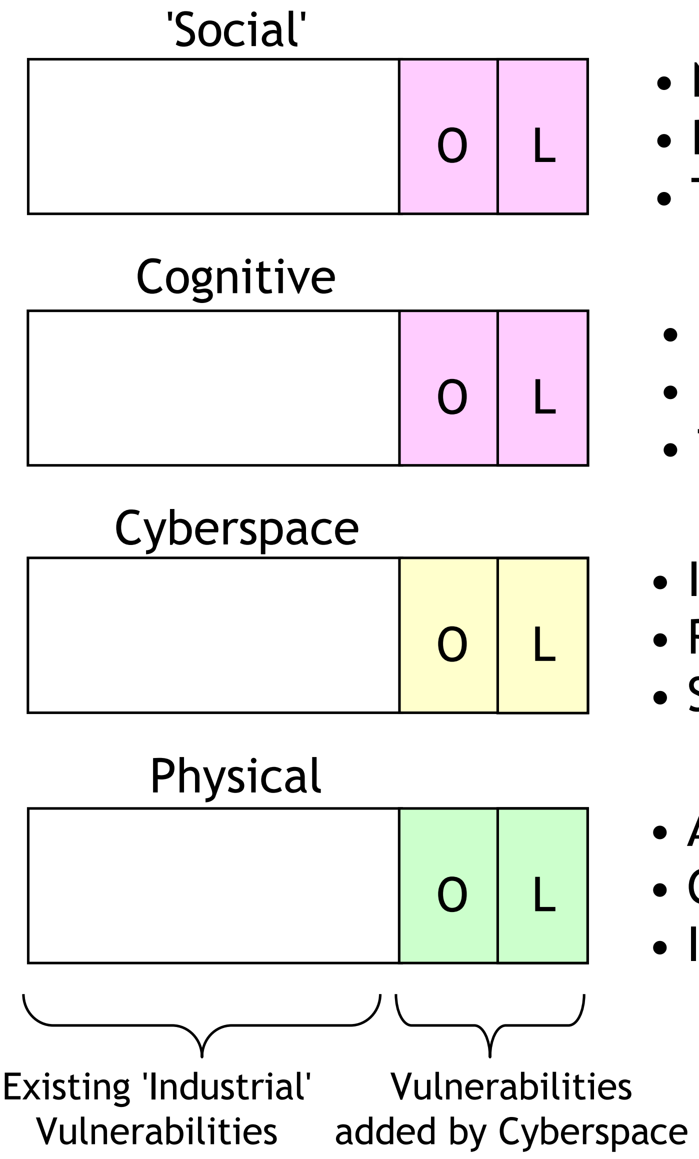
COMMAND AND CONTROL 'SYSTEMS'

EW = Electronic warfare, SW = Software warfare, IW = Information warfare

04 Vulnerabilities - Examples

- Complete dependence on information systems which are themselves vulnerable
- Possibility of actions to effect information and Information Systems:
  - **malicious software and hardware**
- Massive volumes of 'pushed' information:
  - **information overload (command treated as 'dumb process followers, not active decision-makers)**
  - **information management (misplaced drive for 'common taxonomy and picture' stifles necessary diversity of perspectives needed for 'war-among-the-people)**
- Software exploitation:
  - **weapons / agents**
  - **hacking / swarming**
  - **non-information systems**
- Brittle information systems and communication links
- Complexity of interactions / information flows:
  - **communications**
  - **data storage and handling**
- Long battery recharge cycles
- Counter C2 usually only employed in combat arena
- Possibility of actions against command (mind) in *all* environments - anytime - not appreciated

04 Vulnerabilities - Attack Domains



'Social'

O | L

- Nature of virtual organisation (CoIs)
- Reputation of commander
- Trust, confidence (peer, superior, HMT)

Cognitive

O | L

- Over precise / obsession with planning
- Groupthink - lack of alternative hypotheses
- Total belief in 'The Picture'

Cyberspace

O | L

- Information overload and provenance
- Reliance on information availability
- Susceptible to deception

Physical

O | L

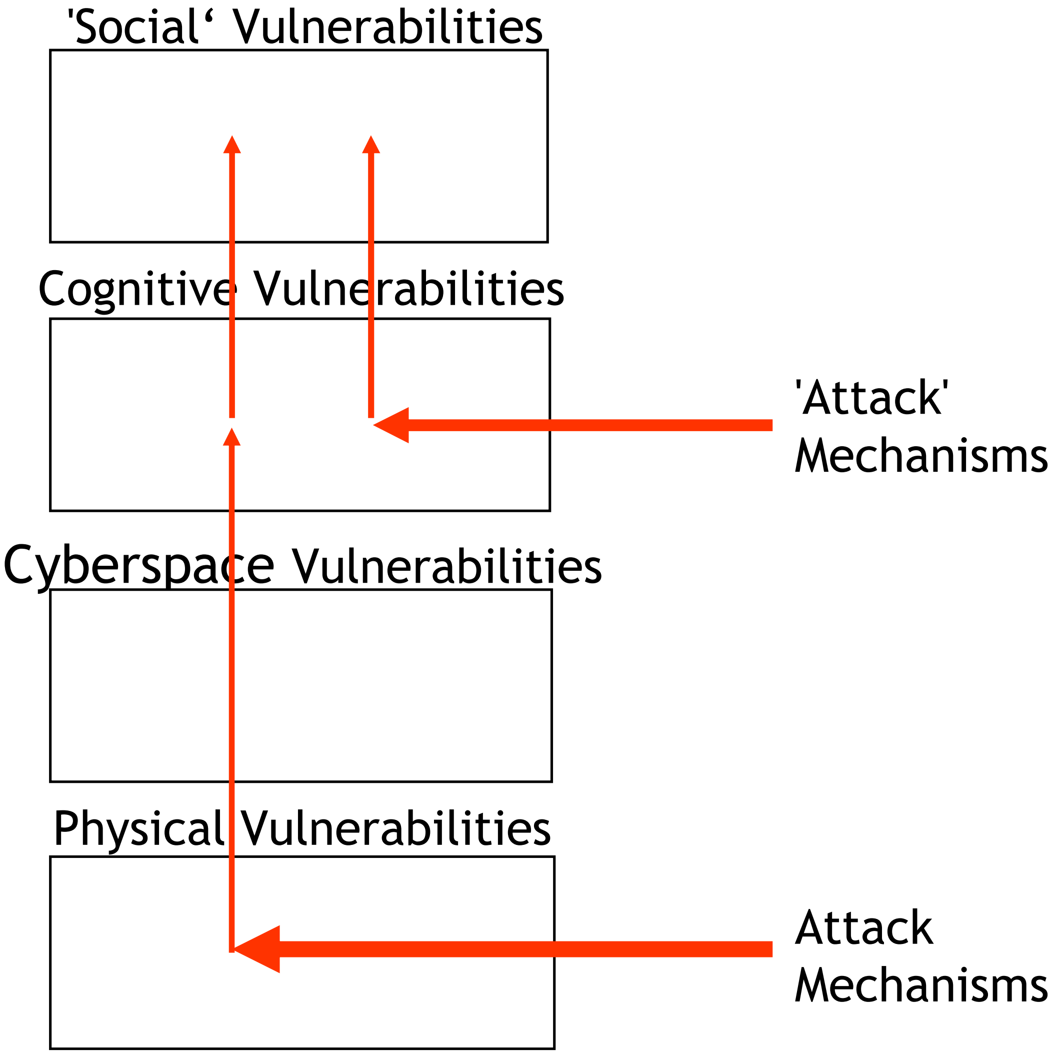
- Assume we 'own' the network
- Complexity of the network linkages
- Inability to influence network adaptation

Existing 'Industrial' Vulnerabilities

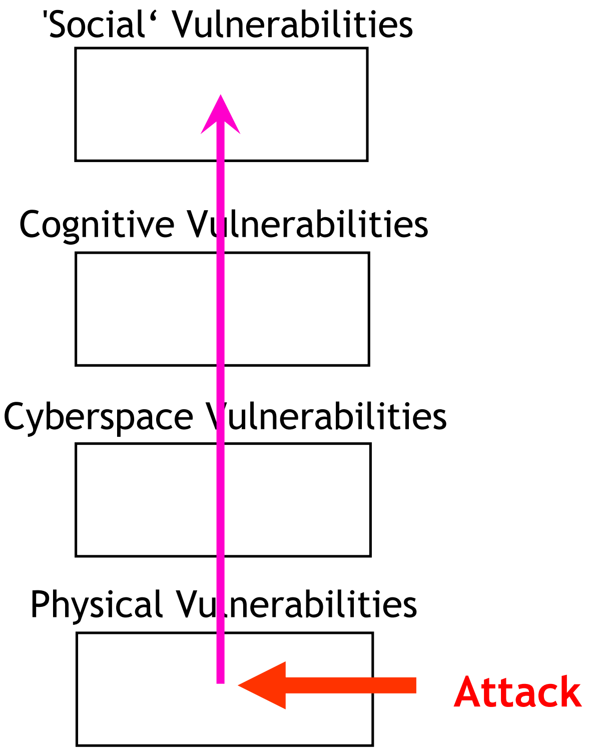
Vulnerabilities added by Cyberspace

O = Organic
L = Latent

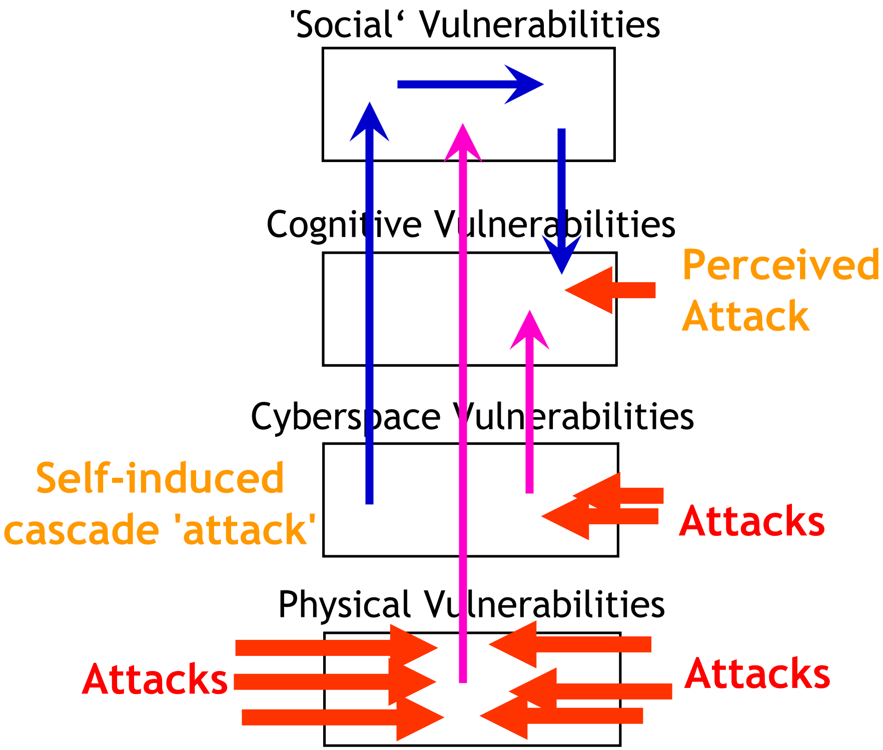
04 Cascades of Vulnerabilities



04 Vulnerabilities - Attack Methods



Single Cascade attack



Co-ordinated Cascade Attack

(With self-induced cascade)

04 Countermeasures

Fortress Mentality:

- ~~seeks to exclude~~
- ~~surrounds with layered-ring defences~~
- ~~impossible to have perfect defence~~
- ~~fails catastrophically~~
- ~~new measures put in place after the event~~

Adaptive Stance:

- *dynamic - accepts 'attack' as inevitable*
- *federated - encourages diversity*
- *provides adaptive capability at the outset*
- *impact localised - but understand cascades*
- *never totally off-line - able to always operate*
- *self-healing behaviour generates resilience (autonomic)*

Contents

01 A Model of Command for Cyberspace

02 Opportunities for Command in Cyberspace

03 Working with Cyberspace - Human-machine Teams

04 Vulnerabilities and Countermeasures

05 Impacts - Guiding Principles for Command in Cyberspace

05 Guiding Principles for Command in Cyberspace

- Cyberspace is NOT separate - command in Cyberspace is part of overall 'comprehensive approaches'
- Understand the realities and limitations of Cyberspace - adopt the adaptive mindset, embrace diverse perspectives
- Embrace and exploit the novel opportunities (don't control)
- Rethink command and intelligence doctrine
- Understand the vulnerabilities and countermeasures
- Develop techniques for dynamically (on-the-fly):
  - sensing and effecting in Cyberspace
  - visualising significant Cyberspace activity
  - forming and exploiting human-machine teams
  - exploiting complex and autonomic behaviour

05 References

- *Utility of Force*. General Sir Rupert Smith. 2007.
- *Agile and Adaptive Coalition Operations - Leveraging the Power of Complex Environments*. Patrick Beautement, Anthony Alston and Lorraine Dodd. At 11th International Command and Control Research and Technology Symposium, Cambridge, England. September 2006.
- *Run-time Science as a Route to Exploiting Emergent Phenomena*. Patrick Beautement. At 1st International Workshop on Engineering Emergence for Autonomic Systems - co-located with the 3rd International Conference on Autonomic Computing (ICAC), Dublin, Ireland June 2006.
- *Autonomous Agents and Multi-agent Systems (AAMAS) for the Military - Issues and Challenges*. Patrick Beautement, David Allsopp, Mark Greaves, Steve Goldsmith, Shannon Spires, Simon Thompson, Helge Janicke. *Defence Applications of Multi-Agent Systems: International Workshop*, DAMAS 2005, Utrecht, The Netherlands, July 25, 2005, Revised and Invited Papers Editors: Simon G. Thompson, Robert Ghanea-Hercock, 2006. Publisher: Springer Berlin / Heidelberg. From: http://dx.doi.org/10.1007/11683704_1.
- *Making Agents Acceptable to People (Terraforming Cyberspace)*. Bradshaw, J. M., Beautement, P., Breedy, M. R., Bunch, L., Drakunov, S. V., Feltovich, P., Hoffman, R. R., Jeffers, R., Johnson, M., Kulkarni, S., Lott, J., Raj, A. K., Suri, N., & Uszok, A. (2003). In N. Zhong and J. Liu (Eds.), Handbook of Intelligent Information Technology. Amsterdam: IOS Press / Springer, 2004.
- *Ad-hoc networks to support crises*. Strong Angel I, http://www.strongangel.org/ Strong Angel II - The Edge at Telescience, http://www.strongangel.telascience.org/ Strong Angel III, http://www.strongangel3.net/
- *The Coalition Agents Experiment: A Prototype for Network-Enabled Coalition Capabilities*. P Beautement et al. DARPA CoABS / CoAX. In Royal United Service Institute's (RUSI) "Defence Systems" Journal, April 2004.
- *Network-Centric Security - Approaches to Collective Run-Time Adaptation*. P Beautement. Adaptive and Resilient Computing Security Workshop, Santa Fe Institute. Nov 2003.
- *Towards Semantic Interoperability in Agent-based Coalition Command Systems*. David N. Allsopp, Patrick Beautement, John Carson and Michael Kirton. Given at the Semantic Web Working Symposium, July 29th-August 1st 2001.
- *General Tzu's Army - OPFOR of the Future*. Michael Lwin. Joint Force Quarterly. 1997
- *Coping with Uncertainty in the Command Process*. P Beautement, Anthony Alston. C2 Research and Technology Symposium, Rhode Island, USA – July 1999.

http://www.tbt.demon.co.uk/library/lib-index.htm

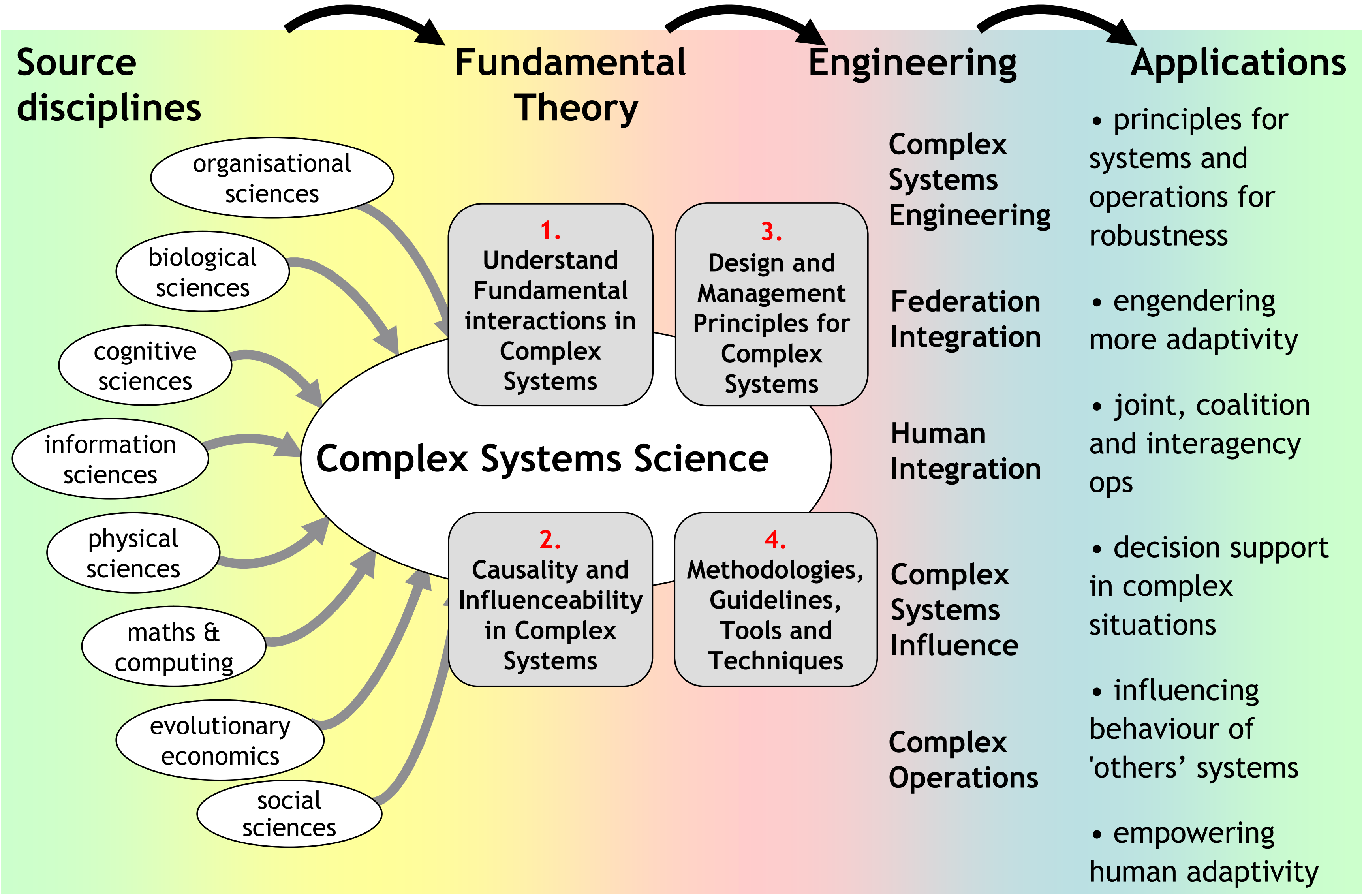
The abaci Partnership

Questions?
Comments?

patrick@beautement.com

Exploiting Complexity

Complex (Adaptive) Systems – from science to applications



Source disciplines

- organisational sciences
- biological sciences
- cognitive sciences
- information sciences
- physical sciences
- maths & computing
- evolutionary economics
- social sciences

Fundamental Theory

Complex Systems Science

1. Understand Fundamental interactions in Complex Systems

2. Causality and Influenceability in Complex Systems

3. Design and Management Principles for Complex Systems

4. Methodologies, Guidelines, Tools and Techniques

Engineering

Complex Systems Engineering

Federation Integration

Human Integration

Complex Systems Influence

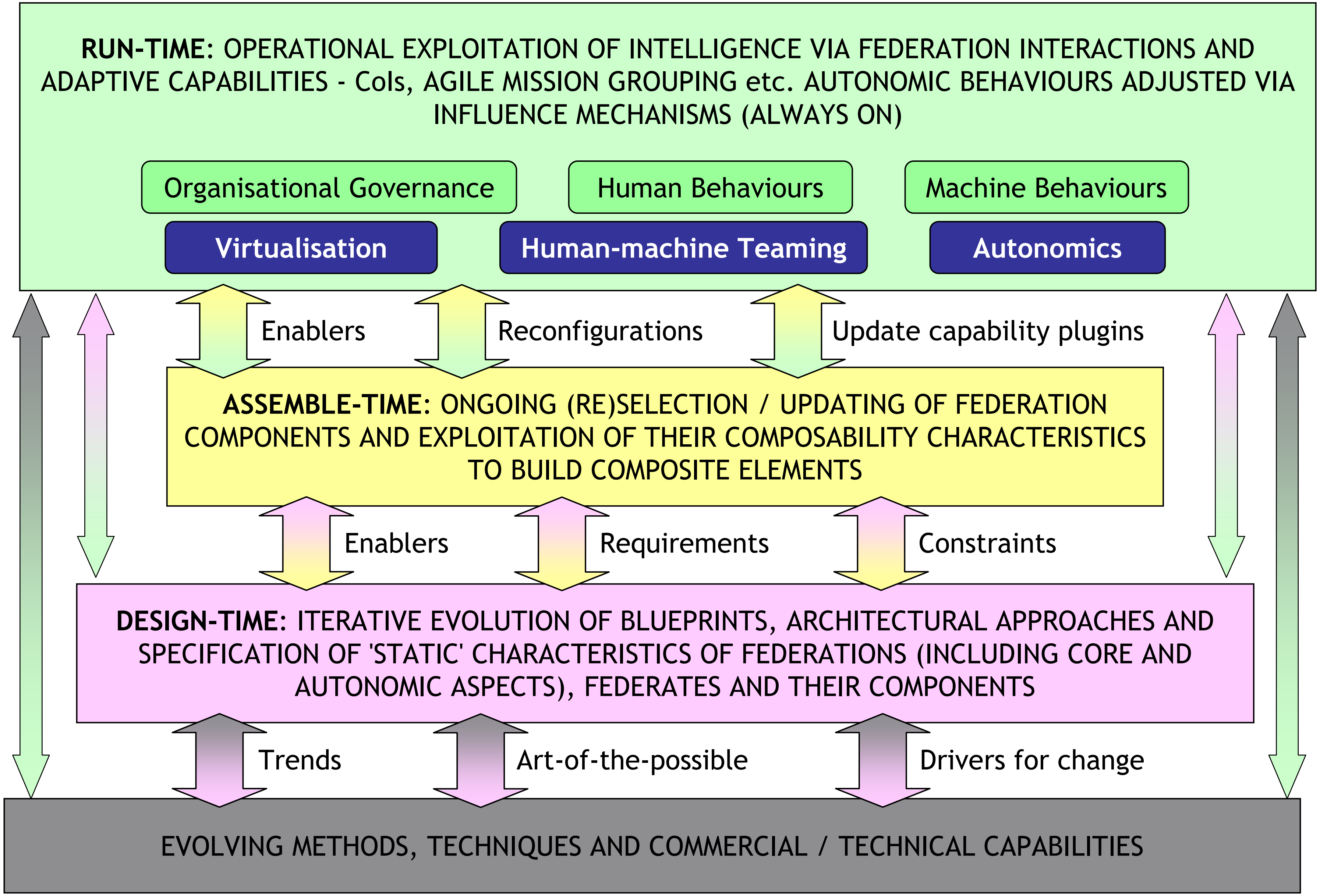
Complex Operations

Applications

- principles for systems and operations for robustness
- engendering more adaptivity
- joint, coalition and interagency ops
- decision support in complex situations
- influencing behaviour of 'others' systems
- empowering human adaptivity

After A. M. Grisogono, DSTO, 2007

Design, Assemble and Run-time (DART) activities for Federations



RUN-TIME: OPERATIONAL EXPLOITATION OF INTELLIGENCE VIA FEDERATION INTERACTIONS AND ADAPTIVE CAPABILITIES - CoIs, AGILE MISSION GROUPING etc. AUTONOMIC BEHAVIOURS ADJUSTED VIA INFLUENCE MECHANISMS (ALWAYS ON)

ASSEMBLE-TIME: ONGOING (RE)SELECTION / UPDATING OF FEDERATION COMPONENTS AND EXPLOITATION OF THEIR COMPOSABILITY CHARACTERISTICS TO BUILD COMPOSITE ELEMENTS

DESIGN-TIME: ITERATIVE EVOLUTION OF BLUEPRINTS, ARCHITECTURAL APPROACHES AND SPECIFICATION OF 'STATIC' CHARACTERISTICS OF FEDERATIONS (INCLUDING CORE AND AUTONOMIC ASPECTS), FEDERATES AND THEIR COMPONENTS

EVOLVING METHODS, TECHNIQUES AND COMMERCIAL / TECHNICAL CAPABILITIES