DECISION SUPPORT SYSTEMS, inc.

DSSI

METATEMPO: SURVIVING GLOBALIZATION

BATTLEFIELD OPERATING SYSTEM

INFORMATION OPERATIONS CODED COMMUNICATION SYSTEM

---

31 DECEMBER, 2001

DECISION SUPPORT SYSTEMS, INC.

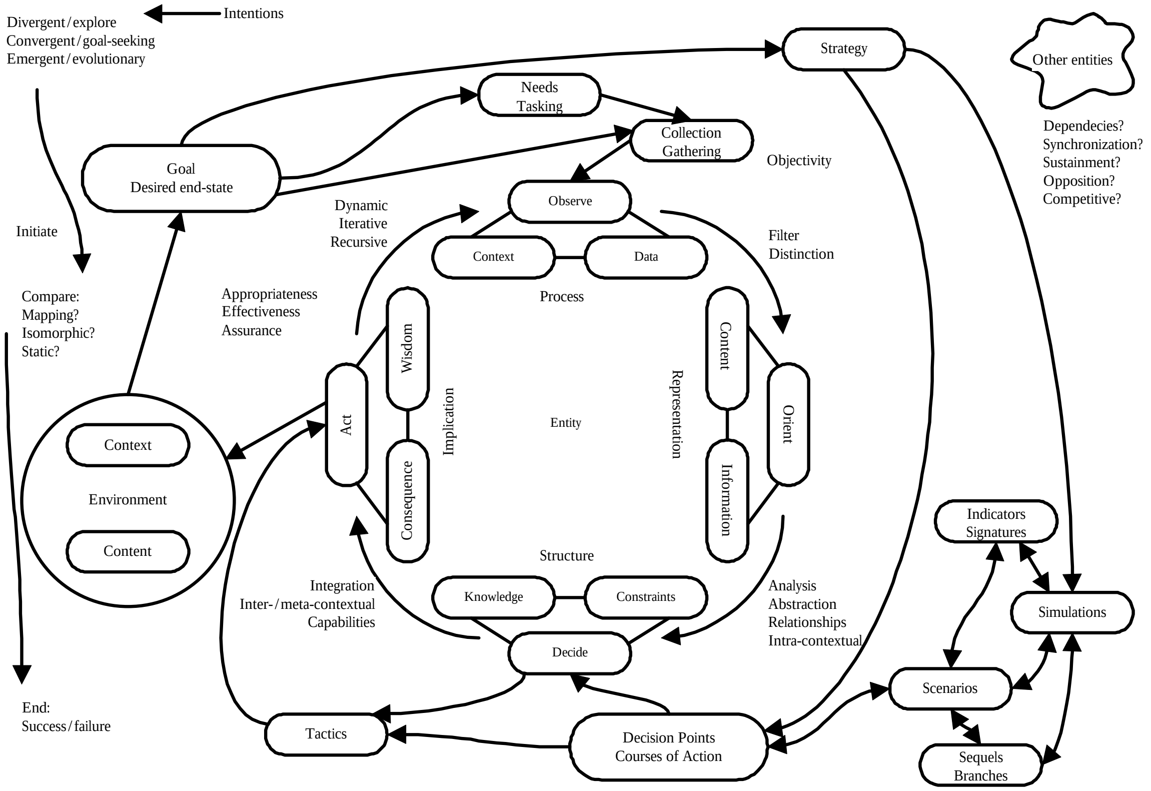
INFO@METATEMPO.COM

[HTTP://WWW.METATEMPO.COM](http://www.metatempo.com)

PURPOSE OF THIS DOCUMENT

This brief discussion of our extensive work on a ‘battlefield operating system’ for special operations and information operations is intended to provide an example that coding mechanisms can, with only a few bytes disguised in many ways, exchange an incredible amount of information.

THE DECISION CYCLE



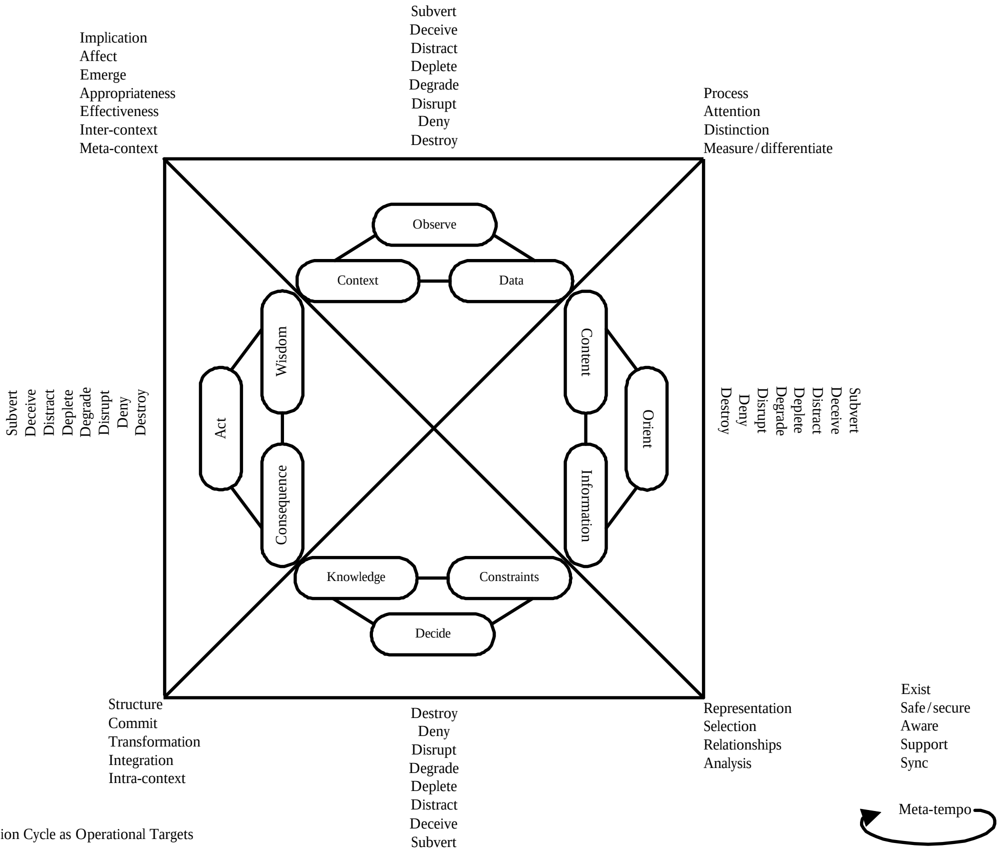
Decision Cycle: Monitor, Measure, Manage, Mitigate

This is a ‘roadmap’ to an entity’s decision cycle—an individual, organization, or movement falls fairly well inside the tolerances and flow established here. This is an essential tool in understanding an adversary, and with understanding comes the possibility of disruption or destruction. Explanation of this is available in detail in the paper **Toward an Ontology of Integrated Intelligence & Conflict**.

A ‘BATTLESPHERE OPERATING SYSTEM’

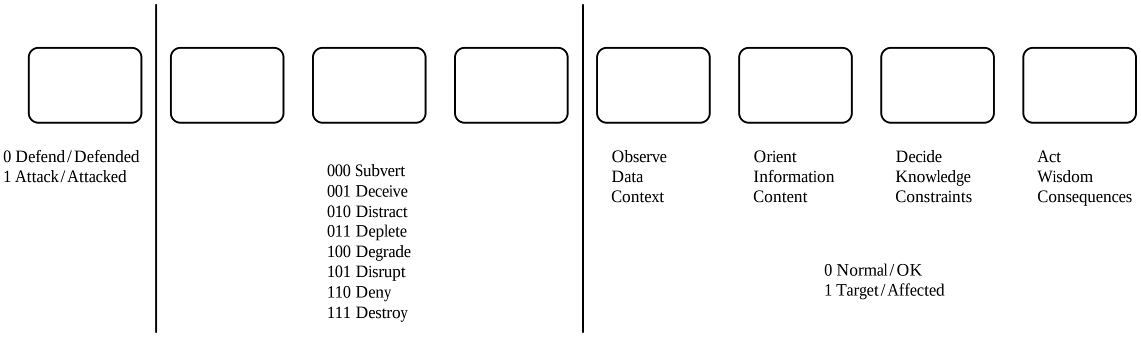
The complex process diagram of the decision cycle revolves around the decision cycle—the other elements are important, but as enablers or augmentation of the decision cycle. Looking at the core elements, there is a spectrum of attacks that could be launched on the cycle: subvert, deceive, distract, deplete, degrade, disrupt, deny, destroy.

Those familiar with the Boyd Cycle will often speak about “getting inside” the decision cycle—time-competitive decision-making, such as occurs between fighter pilots (the origin of the Boyd Cycle). This is distinctly different, and takes "getting inside" to mean conceptually rather than time-competitively—unconventional warfare broken into two disciplines, infrastructural warfare (IWAR) and information operations (IO).



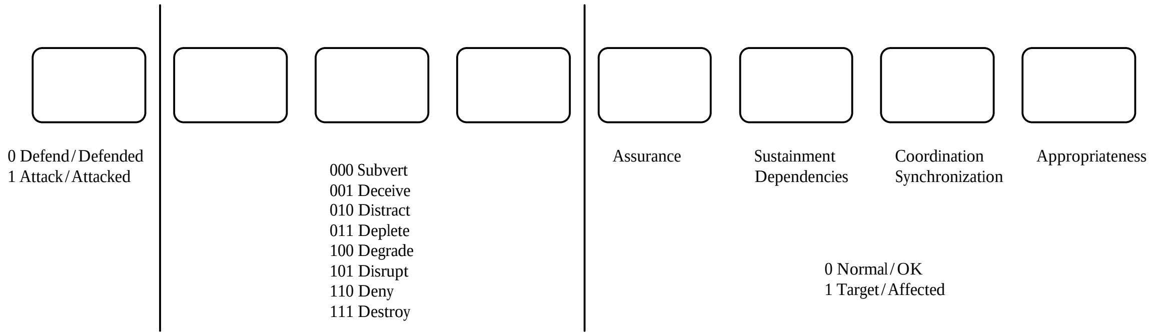
Attack Grid: Core Decision Cycle as Operational Targets

The definitions of the spectrum are detailed elsewhere (see **Toward an Ontology of Integrated Intelligence & Conflict**), but the application of the grid to a coding mechanism in a Battlesphere Operating System (BOS) was not discussed. Conceptually, the grid provides a useful tool in planning, mission orders, providing situation reports, and battle damage assessments. Coded for communication between parties with symmetrical knowledge (essential in interpretation), two (2) hexidecimal bytes are all that are necessary to exchange information:



This is the first byte of an IWAR/IO BOS communication code:

- The first bit (the high bit) is the mode of defend or attack
- The next three bits are binary coding of the attack spectrum
- The next four bits are which stage of the decision cycle targeted



The second byte of an IWAR/IO BOS communication code is similar except for the second 'nibble,' the last four bits of the byte, which describe which aspect of the 'meta-tempo' targeted. Meta-tempo is the "tempo of tempo," the decisions regarding the decision cycle itself. While individual elements of the decision cycle can be attacked and need to be defended, there are aspects of the cycle itself that require similar consideration:

- Assurance. Safety and security of the overall cycle, particularly OPSEC and INFOSEC/INFOASSURE

- Sustainment/Dependencies. Logistics, supply, interior/exterior lines, the resources necessary to keep the cycle functioning (material, information)

- Coordination/Synchronization. Interactive tempo—the relationships between decision cycles of various entities

- Appropriateness. Neither too fast or too slow, like driving at an appropriate speed for conditions. Being aware of the degree of trust in a context (e.g., landmines take advantage of a natural 'trust' in ground). Not overrunning information, knowing the certainty of information. Selection of information for its value and relevance

UNCONVENTIONAL ATTACKS

Using the grid as a planning tool rapidly turns into a way to code mission orders strategically:

- 1 111 0010 in the first byte would mean to attack, intending to destroy, decision-oriented targets (leadership-based targeting, C2, etc.)

- 0 000 1000 in the first byte would mean to defend against subversion in observation systems (sensors, C4ISR, forward observers, space-based assets, etc.)

- 1 111 1100 1 101 0101, using both bytes, would mean to attack observation and orientation capabilities (sensors, GPS, etc.), trying to create a 'fog of war' and have the target overrun their information (which would probably be accompanied by additional directions—rapid movement, changing the environment, or somehow making the last intelligence models of the opponent rapidly out of date after the attack on their systems; coupled with a loss of GPS in poor terrain, this would have devastating effect)

While the whole approach can be considered unconventional, some aspects are more conventional than others—attacking, with intent to disrupt, deny, or destroy, leadership or C2, in one of the examples for instance. Destruction is an inherent element of military force projection, so a focus of military operations on or near this end of the attack spectrum is a natural. The other end of the spectrum, subversion, is too 'target specific' to address in a general fashion. In between the two polarities, however, is a soft spot—altering the 'costs' associated with the decision cycle and meta-tempo, either against the adversary or to one's own benefit.