



DECISION SUPPORT SYSTEMS, inc.

D S S I

METATEMPO: SURVIVING GLOBALIZATION

TOWARD AN ONTOLOGY OF INTEGRATED INTELLIGENCE & CONFLICT

A PRIMER

APRIL 2001

MICHAEL WILSON

DECISION SUPPORT SYSTEMS, INC.

WILSON@METATEMPO.COM

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

COPYRIGHT 2001. ALL RIGHTS RESERVED

PURPOSE OF THIS DOCUMENT

An 'ontology' is a specification of a conceptualization, a representation of processes and relationships. For purposes of sharing, an ontology is an essential communication tool; for purposes of use, a specification provides a doctrine, and in this case, introduces a meta-doctrine (a doctrine of doctrines).

My personal experience, as an inventor and pioneer in what is currently referred to as infrastructural warfare, information operations, and open source intelligence, is that the domains of intelligence and conflict are merging. What I wish to present in this, a primer on an ontology of integrated intelligence and conflict, is how the merger of the two domains is not additive, but synergistic—the scope and scale of potential operations widens dramatically.

In order to support the argument for an integrated ontology, it is necessary to first explore the existing intelligence cycle, the failures of the conventional intelligence cycle, and the changes in the world that have negatively impacted on the intelligence cycle. I will then present the decision cycle which, as both force multiplier and operational target, embodies the integrated intelligence and conflict processes. To further the reader's understanding, I provide a number of definitions, as well as analysis and assessment tools that are elements of the ontology.

[31December2001: This document is being made available as a companion to **Hunting the Sleepers**: <http://www.metatempo.com/huntingthesleepers.pdf>

Hunting the Sleepers is a 'companion' piece to **An Analysis of Al-Qaida Tradecraft**, which can be found at <http://www.metatempo.com/analysis-alqaida-tradecraft.html>.

In the process of preparing this document for public consumption, it became clear that an earlier document, pre-11Sept2001, would need to be made available. **Toward an Ontology of Integrated Intelligence & Conflict**, which can be found at <http://www.metatempo.com/DSSIOntology.PDF>, is a theory of special operations, with a particular focus on information operations. Regarding the 'war on terror,' a theory and doctrine are emerging, and we've made considerable headway toward a structure for what used to be referred to as the 'revolution after next.'

Three additional documents are supplementary to **Hunting the Sleepers**:

Al-Qaida Threat Brief available at:
<http://www.metatempo.com/AlQaidaThreatBrief.PDF>

Battlefield Operating System: Information Operations Coded Communication System available at:
<http://www.metatempo.com/BOSCode.PDF>

Secure Communications Operational Tradecraft available at:
<http://www.metatempo.com/SecureCommo.PDF>

Readers interested in Al-Qaida may also find **Al-Qaida's Endgame? A Strategic Scenario Analysis** of some use. It is available at:
<http://www.metatempo.com/alqaida-game.pdf>

Information is the best defense, as well as the most viable weapon in any conflict, this being no exception. While a large body of material, the author feels the availability takes the fight out from behind closed doors and into everyday life—where it's being fought already.]

THE CONVENTIONAL INTELLIGENCE CYCLE

The conventional intelligence cycle is a 'legacy' process—an ontology that has followed an 'organic growth' path over the centuries, with 'forced growth' in the last half century. As with any emergent process, the intelligence cycle has 'abstract principles' or 'rules' that are context-independent, and that generate context-dependent elements.

If intelligence were actually thought of and taught as such by the involved professionals, the domain would have evolved in the direction suggested in this ontology, in all probability. Context shifts have dramatically impacted on context-dependent thinking about intelligence and conflict; this is why abstract principles are still relevant, while many of the specifics of the conventional intelligence cycle are failing.

THE PURPOSE OF INTELLIGENCE

The purpose of intelligence, and the intelligence cycle, is to provide adequate, accurate detail to the decision-makers in order for them to make an informed decision.

Intelligence may come from many sorts of 'sources':

- Signal intelligence (SIGINT), such as monitoring communication channels
- Image intelligence (IMINT), such as satellite observation
- Technical intelligence (TECHINT), such as network sniffing
- Human intelligence (HUMINT), provided by human sources
- Open source intelligence (OSINT), which relies upon 'legal' sources
- Espionage, which involves breaking the local laws in order to obtain information

Most intelligence organizations take an ALLSOURCE approach, which utilizes any and all means and methods to obtain the most accurate and highest quality information.

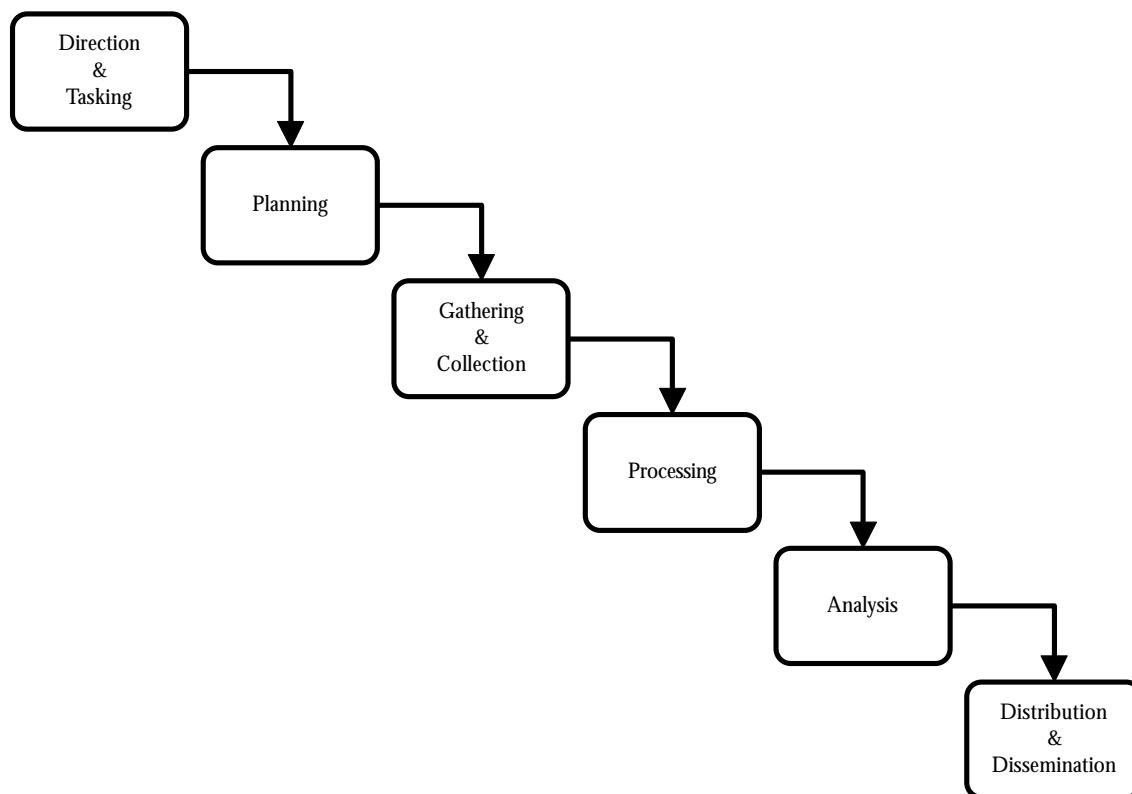
Most intelligence organizations, particularly those of the Nation-States, have concentrated on 'capability' intelligence (things you can count, like tanks and missiles), rather than 'intentions' intelligence. This is largely a product of the Cold War mentality, and has resulted in incredible intelligence failures, notably the collapse of the Soviet Union, and the Iraqi invasion of Kuwait. The two are distinctly different sorts of intelligence, but technology is less capable of looking into the human mind and human heart.

THE CONVENTIONAL INTELLIGENCE PROCESS 'FLOW'

The intelligence process is under considerable 'pressure' to evolve—this approach is no longer effective, since the 'threat model' of groups regarding whom Nation-States require intelligence has changed dramatically.

Nation-States are well aware of the problems with the conventional intelligence cycle, but the 'major' players (most industrialized nations) have considerable trouble shifting intelligence approaches. As an example, the United States intelligence community has 50+ years of inertia to overcome ("we've always done it this way"); tens of thousands of personnel in the intelligence community, many of whom are 'career' and thus difficult to alter the behavior of or 'retire'; and billions of U.S. dollars appropriated from the budget every fiscal year that keeps things pretty much as they are. It is, therefore, important to know how the conventional intelligence cycle works, simply because so many of the players are going to be 'stuck' using the approach for some time to come.

The conventional intelligence process 'flows' like this:



- Set the direction, which is known as 'tasking,' of the intelligence cycle. This establishes the purpose of the cycle, driven by simple questions such as "What is the need?" and "What is the intention, what do we want to accomplish, with this intelligence operation?"
- Planning then takes the proposed tasking (the 'intention') and figures out which 'capabilities' would best be applied—how to gather the intelligence, using what sources, etc. This plan is then communicated to those groups in the intelligence community that command and control the capabilities—who, what, where, when, and how
- Gathering and collection involve actively operating to obtain the intelligence and passively 'working' the existing intelligence database and existing capabilities to see what

may already be known or opportunistically available. The 'output' of these processes is then communicated back to the requesting elements of the community

- Processing receives the gathered and collected intelligence, essentially 'centralizing' the various materials produced under the tasking. While this aspect is supposed to 'make sense' of the materials, it is also compartmentalized—access to the materials is restricted to 'cleared' personnel that have permission from the intelligence bureaucracy of the community
- Analysis takes the body of available materials and provides a 'value add' that creates the intelligence product—review of the sources, looking for meaning, discussion of the possible implications
- Distribution and dissemination then takes the produced product and delivers it to the approved and (hopefully) relevant decision-makers

The conventional intelligence cycle is a 'legacy' approach—developed in a time when it may have made perfect sense, but now an artifact that no longer functions terribly well, but that those in the community are still required to use. Briefly, the conventional cycle was generated out of a 'command & control' mindset—hierarchical, top-down, conservative, assuming a linear world. That's no longer how the world works, and the conventional cycle doesn't cope well with the new and novel.

It may also be of historical interest that this cycle, which is essentially the same as the 'waterfall' model of product and software development, was rejected by the larger technology world decades ago as inefficient and ineffective.

PROBLEMS WITH THE CONVENTIONAL INTELLIGENCE CYCLE

There are a number of problems that have been evident with the conventional intelligence cycle; these are presented in no particular order—the intelligence process being what it is, different problems have more or less significance under different circumstances:

- The cycle is limited, with a defined 'start' and 'finish,' a defined duration, and constraints on how the intentions can be accomplished. Particularly problematic is that the cycle ignores tempo as a factor, and thus loses a competitive advantage
- Similarly, the cycle is 'discrete'—various taskings are generally isolated from each other. This leads to redundant efforts, considerable sunk costs, and incredible opportunity costs. Because of the way the process is structured, it just isn't responsive or flexible
- Scale and scope issues are poorly handled by the cycle—there is too much detail about too many things, with miserable information management, and so 'information overload' is present at every stage of the process
- You don't know what you don't know. Most intelligence operations are explicitly tasked, and thus dependent upon knowing that you need to know something. Moral and material surprise continue to plague adherents to the conventional cycle
- The structure of the cycle inhibits completeness; no 'area of specialty' is isolated from any other in the current context, but compartmentalization in intelligence forces severing domains from 'connectionist' thinking. Attempts to cross specialization boundaries perturb the intelligence community, because they are completely unprepared to make

such structural shifts. This is one of the critical pressures driving military intelligence toward OSINT—since the intelligence is open source, it isn't restricted by specialist or compartmentalization boundaries

- Thresholds in the cycle are set inappropriately—there is little acceptance outside of military intelligence for a 'minimum necessary product' that is improved upon continually. Individuals in the intelligence community also struggle with two critical questions: "When is more just more?" and "When does having more information become confusing, counter-productive, or actually mean knowing less?" The first question is a product of information overload—capabilities overwhelming the community—and the second question is increasingly important with active deception and subversion, not to mention poor management of complexity
- The intelligence process produces 'product' with great limitations—what I refer to as the 3Fs: freezing, flattening, and forgetting. Product isn't dynamic, so once it leaves the cycle, it becomes dated—and the 'expiration date' in some domains can occur very rapidly. Distortions creep into the product—assumptions, skewed connections and associations. Great levels of detail just aren't included in the product—for compartmentalization reasons or for brevity, there's a loss of context that helps the decision-maker reach an understanding. Also intelligence product is highly 'source' dependent, creating issues of credibility and trust, which is why there is a distinct preference for technical methods over the human (information operations, however, directly takes advantage of this misunderstanding of trust)
- Compartmentalization also means that there is a disconnect between the 'consumer' or decision-maker and the intelligence cycle. There's a lack of feedback that could be used to be more effective; 'intention' is set at the initiation of a cycle and thus becomes static; intelligence that doesn't meet the needs of the decision-maker means that no informed action can be taken; ultimately this can lead to a lack of iteration in the cycle
- Tradecraft, the means and methods associated with intelligence, is dogmatic—it's taught as a set of ways to do things, but without the rationale or 'why' things are done that way. As tradecraft becomes less effective or ineffective, field officers and assets lose the ability to generate their own tradecraft because they aren't connected to an understanding of why things are done a certain way. This leads to a loss of flexibility, a directly negative impact on security, a disconnected product, etc. It also leads to 'echoes' as even basic principles such as 'triangulation' are no longer understood, adhered to, or validated. The consequence cascades of dogmatic or ineffective tradecraft are considerable; for example, 'dead drops' (an asset leaving intelligence at a neutral safe location for later pick-up by an intelligence officer) have evolved to include the Internet, and the conventional community is experiencing great discomfort because they can't use the existing counter-intelligence capabilities against new approaches effectively
- The legacy approaches—cognitive, technical, social—are leading to bad decisions about how to make decisions. One example is the on-going preference for the 'tangible'—things you can count or measure, capabilities—which leads to a focus on technical, signal, and image intelligence. This, of necessity (sunk costs and opportunity costs), leads to decreased emphasis on the 'intangible'—intentions, motivations, cognitive approaches, emotional states—the sorts of intelligence that comes from HUMINT
- The intelligence community, and those involved in the cycle, are monolithic; this leads to a loss of speed, tempo, timeliness, accuracy, and comprehensive products

TRADE-OFFS IN INTELLIGENCE

The existing conventional intelligence cycle is also continually faced with decisions regarding trade-offs in how to manage and operate the cycle:

- Emergent, divergent, and convergent products require different processes. Emergent tasking requires a wide-open view of the world looking for what might be interesting or essential to know, and subsequent pursuit of those things. Divergent tasking starts with an initial 'area of interest' and expands out across associations and connections. Convergent tasking is intended to come to a conclusion, or at least a set of potential courses of action and probabilities. Some sorts of intelligence, then, are exploratory, with no pre-determination, while others are looking for explicit detail on specific domains—again, the issue of the unknown vs. the known
- Quantity, what's referred to as 'production' is preferred because it is measurable, but it has little to do with 'quality' coverage, which defies easy measurement
- Current reporting isn't in-depth intelligence, but they are in fact complimentary products, both of them essential. Current reporting provides a rapid view of indicators and tripwires, but it's opportunistic, not directed or comprehensive. Emphasis on current reporting means there are gaps in intelligence coverage
- Objectivity is difficult to achieve—there is bias in assumptions, interpretation, analysis, dissemination, complicated by specialization and compartmentalization. When the product gets to the consumer, bias and politicization are even more damaging to the intelligence process
- Analysis and operations are under different pressures, and so there is considerable friction between the two functions. Military intelligence cycles are better at a balance between the two functions, because of the more 'concrete' and life-and-death nature of the intelligence product

THE CONVENTIONAL INTELLIGENCE CYCLE IS INADEQUATE

The conventional intelligence cycle is decreasingly effective at what it is intended to do—inform the decision-makers so they can make effective decisions. In large part, this is because the world is no longer conventional—too many risks and threats coming from too many new and novel places. This will lead to increasing numbers of intelligence failures—and in the current and future contexts, that means increased vulnerability to potentially catastrophic consequences.

Dramatic failures of the conventional intelligence process have led the Nation-States to look elsewhere for a 'next generation' of intelligence, one that doesn't fall prey to the illusion of omniscience. As previously mentioned, there are considerable structural limitations to an evolution or revolution in intelligence affairs, so many of the Nation-States are turning to technical quick-fixes, playing for time, while trying to figure out how to solve the many problems.

IT'S A CHANGED WORLD

The conventional intelligence cycle is functionally constrained and context-dependent—largely a set of processes and a community that emerged under circumstances that are no longer operative.

INTELLIGENCE IS CHANGING

Intelligence is changing, or at least the intelligence community is trying to change, because the world is a different place. The existing, 'legacy' agencies and organizations are having great difficulties, and because the intelligence products they produce are decreasingly useful, the community will have either to evolve or die.

While the primary problem with the community is that the 'opposition' has changed dramatically, that isn't the only change facing agencies and organizations. What is worth noting is that while the community is having difficulty making the necessary shifts, the opposition is having minimal problems, and thus is enjoying strategic and tactical advantage.

The other primary forces driving real and proposed changes are well worth considering, and are the subjects for analysis below.

GLOBALIZATION

The world is now 'local'—continual and completely connected communications infrastructure means that the other side of the world can, if it's 'media hot' enough, get more coverage and attention than what's right next door. This is also more than just media—financial networks and markets of every sort are increasingly impossible to cleanly separate. Certainly there are explicit interactions that have connected the markets, but complex financial instruments such as derivatives have made the connections incredibly complex and almost beyond comprehension. In fact, everything is becoming connected in ways not very well understood, and not just financially. One example is how global transportation has changed biological vectors and epidemiology in ways that human society and ecosystems may not be able to cope with, as disease takes advantage of sociological vectors of contagion, and agri-business creates catastrophic mechanisms for propagation into animal and plant populations.

A consequence of 'everything is local' is, oddly, everything is also non-local. With the entire world competing for attention, very little is actually paid attention to. The economic 'tragedy of the commons'—if everyone owns something, then nobody does—is playing out in social structures and the social contract, leading to the individual feeling disenfranchised and disenchanting. Perhaps this wouldn't have been quite so important in previous time periods, but with the capacity for mayhem and destruction having 'devolved down' to the individual, and the willingness of individuals to engage in violent behavior to demonstrate their displeasure with the state of things, this is increasingly problematic. It's also complicated by the fact that a displeased individual can engage in destructive behavior, sometimes catastrophic, against targets anywhere on the planet.

Another consequence of the complexity and connectivity is that 'tempo' is increasing, as well as the meta-tempo, the tempo of tempo—the rate of change, as well as the rate of change in the rate of change.

In other words, the world and the interactions around it will keep changing, increasing in complexity, faster and faster.

GLOBAL POWER SHIFT

After the Cold War and the collapse of the Soviet Union, the world has become ‘monopolar’—one Superpower, namely the United States. This situation will not persist for long, both because the position is unsustainable if history is any proof, and because other Nation-States don’t wish the situation to continue. A number of ‘second tier’ Nation-States have programs in place to run operations, so-called ‘active measures,’ in order to enhance their position. One example has been the proliferation of nuclear weapons, simply because being in the ‘Nuclear Club’ is a symbol of world status.

Some of the same Nation-States, as well as a number of others, are betting that if they can maintain continuity, if they can just persist and survive the mistakes made by others, then they will ascend to a dominant position. This explains large internal programs in certain Nation-States to suppress subversive activity and maintain the status quo for the existing power structures.

DECAY OF GOVERNANCE

There are also significant trends toward ‘Balkanization’—large Nation-States and organizations are hitting diseconomies of scale, creating significant inefficiencies that impact on the society. Large Nation-States and organizations are also running into problems with heterogeneous populations and memberships, which has led to movements for cultural independence, ethnic cleansing, and schisms in most large organizations.

At the same time, as previously mentioned, there is a devolution of power, particularly in the capacity for violence or damage. The fact that the scale of force projection has decreased, coupled with a massive increase in the scope of organizations and operations with both the intent and capabilities, explains some of the significant erosion of the strength in Nation-States.

POLARIZATION

Everyone is taking sides; the numbers of ‘non-aligned’ have been decimated, since non-committal has been an invitation to disenfranchisement, an opportunity to take over the property controlled by the non-aligned, and on occasion has led to ethnic cleansing with attempts at genocide.

Political and economic systems are going to have to cope with self-interested and actively challenging groups, the most mild of which are causing market forces to no longer operate as they have previously, while others are waiting for their chance to make a bid for control. There are also less active, but no less destabilizing, issues of ‘haves’ vs. ‘have nots’—the growing divide between the wealthy and the poor, those with technology and those without, etc.

TRANSPARENCY

There is increasing pressure for ‘public’ or at least more available disclosure, particularly in politics and in the financial markets. Such efforts at transparency would have distinct benefits, particularly as an essential ‘check and balance’ against abuses of power, or financial manipulation or fraud. In addition, disclosure of such decision-making tools like risk models, will allow the public to make better decisions and investments themselves. Many recent global financial crises originated with risk models that had ‘fallen out of step’ or no longer accurately reflected the real world situations. A large and looming potential catastrophe exists because there is no distinction in global markets between ‘hedging’ and

'speculation'—and financial instruments used for risk shifting and sharing in a completely connected world may well lead to uncontrolled market collapses.

ADVANCES IN TECHNOLOGY

Progress continues, in both scale and scope, and this only exacerbates all of these trends—more change, more frequently, with increased interactions, and incredible emerging complexity. Many technological trends lead directly to radical consequences that moral and ethical structures, as well as the social contracts that make civilization possible, just will not be able to cope with. Biotechnology, massive increases in computational power, the emerging field of nanotechnology, just as a small set of examples, will be incredibly destabilizing. These three in particular will convey great power—political, economic, military, etc.—upon those capable of making the significant breakthroughs first.

ADVANCES IN 'OPPOSITION'

Many of the individuals and organizations that set themselves in the 'opposition force' role have made a significant behavioral shift. While many prior opposition forces followed a doctrine of 'the ends justify the means,' the emerging opposition accept no rules of engagement, and have adopted a 'by any means necessary' approach. This means no constraints, no restraint, no limitations on operations or targets, and all-out 'unrestricted warfare.'

There are profound implications to this, including the potential for use of Weapons of Mass Destruction (WMDs). Size no longer matters, even the 'little guys' will have access to chemical, biological, nuclear, and informational weapons. Use of WMDs is now largely a matter of 'when' and not 'if,' and the Nation-States have yet to think through what their range of potential responses might be. In many cases with WMDs, there may well be no valid response or opportunity for reprisal—the opposition force that uses WMDs may be anonymous, totally unknown, and beyond reach.

Opposition forces are also much more able to adopt and adapt to the availability of new and advanced technology. Information technology has driven a considerable revolution in opposition forces—organization, coordination, intelligence, fund-raising, recruiting, communications, etc. In many cases, opposition forces have better capabilities due to 'commercial off-the-shelf' or COTS technologies than the Nation-States they are opposing.

DEPENDENCY

As noted previously, the world is increasing in complexity, inter-connectedness, and in the sheer number of interactions.

A combined downside of advances in technology and movements toward transparency has been an increasing awareness, particularly among opposition forces, of the vulnerabilities in physical and virtual infrastructure. In many ways, the defining characteristics of the major Nation-States are the advanced elements of infrastructure, those things that provide an economy of scale and the quality of life enjoyed in such societies. This includes everything from efficient markets to transportation systems—whether of physical goods, or of information. The consequences of a catastrophic failure—whether through natural disaster, accident, or through deliberate hostile action—in such infrastructures would be considerable, as cascading failures propagated throughout the 'value web' or dependency webs that make up the modern political economy.

The risks (passive, a potential problem) and vulnerabilities (active, an opportunity for a hostile or opposition force to target) associated with dependency infrastructure are considerable, and intelligence regarding them is easier than ever to obtain, particularly through OSINT, and the tools and technology to

attack them are also incredibly simple to obtain. The major Nation-States, because of their heavy reliance upon advanced infrastructure, are the most vulnerable.

FORCE MAJEURE

Catastrophic events are taking on a new meaning—disaster for one can mean disaster for many. As an example, a number of significant biological events are looming, including an ecological disaster on a scale that merits the term ‘die-back.’ Both Africa and Southeast Asia are facing crises of disease—HIV, TB, old diseases that they can’t afford treatment for, new diseases for which there is no treatment—that will cause massive fatalities on a scale beyond the influenza Pandemic early in the 20th century. This is pure, inescapable trending—a matter of ‘when’ and not ‘if’—as incubation or latency periods are approaching their maximum possible length, people will become sick and start to die. Both Africa and Southeast Asia are highly manpower dependent to support their populations, and as the numbers of sick and dead increase, the probability of total societal collapse approaches certainty.

As such a point, there will be an opportunity, a ‘power vacuum,’ that is going to be exploited—too much land, with too many valuable resources, and in too strategic a position to be ignored will become available. This will have global impact—politically, economically, biologically, and probably militarily. To say that it will be destabilizing is an understatement.

FRAGILITY

Given the levels of risk and vulnerability among the major Nation-States, and even with a growing awareness of the potential for catastrophic failures, little has been done to generate solutions. There are no ‘fall-back’ systems or positions, no integration of safety and security systems to improve the situation, largely because those responsible don’t have the ‘mindset’ or understanding necessary to solve the problems.

Because of this, denial and subversion are rapidly becoming incredibly potent tools for opposition forces, and so the ability to use them is increasingly common. One of the few limiting factors is a lack of ‘will’ or intention to cause such catastrophic damage among the current opposition forces—they’re more interested in taking their turn at running things, rather than destroying it all—but the ‘next generation’ of opposition forces that are emerging do indeed have damage on such a scale as part of their motivation.

INTELLIGENCE & CONFLICT

This brief discussion of some of the significant changes in the world will help the reader to understand why the intelligence community is under great pressure to evolve—and it is, with the leading edge players.

The new emphasis in intelligence is turning to the 4Ms: monitor, measure, manage, and mitigate. Intelligence will eventually need to be delivered continually to all decision-makers, and it is an increasing trend that everyone in an organization is making decisions.

What is becoming clear, however, is that intelligence and conflict have become integrated, and this is being proven by the rapid expansion in domains such as infrastructural warfare, information operations, and psychological operations. Open source intelligence is a rapidly growing ‘specialty’ because it’s becoming a more powerful tool in many ways than espionage was in the previous era, particularly against more open, more transparent Western targets.

Future areas of conflict will be well-integrated with intelligence:

- Infrastructural warfare (IWAR) is conflict based on dependency and infrastructure, particularly unconventional warfare on 'soft' targets that can cascade and affect 'hard' targets
- Information operations (IO) are elements of conflict directed at decision cycles and infostructure (information infrastructure, such as communication systems, information technology, the Internet, etc.), a sort of 'virtual manoeuvre warfare' than can decapitate the opposition, and remove political, military, and economic command structures
- Psychological operations (PSYOP) are direct actions or counter-operations aimed to subvert social, political, and military will, and this is particularly effective in Western or democratic societies where popular support is necessary for political decision-makers, who have command authority over military and intelligence capabilities

In the changed world, where even more change will be occurring, the intelligence community is poorly structured and positioned to evolve in the necessary direction in order to exploit the new opportunities, vulnerabilities, and capabilities. It is for this reason that a number of 'crash' or emergency programs are being put into place, and why some odd relationships—particularly between 'old school' Nation-States' intelligence communities and 'new school' opposition forces, including the computer underground.

THE DECISION CYCLE: FORCE MULTIPLIER & TARGET

The decision cycle is the first glimpse of the synergy possible with an integrated ontology of intelligence and conflict.

WHAT IS DECISION SUPPORT?

While the conventional intelligence cycle is mainly concerned with providing details to the decision-maker (the 'consumer') in order to make informed decisions, this approach is rapidly becoming inadequate.

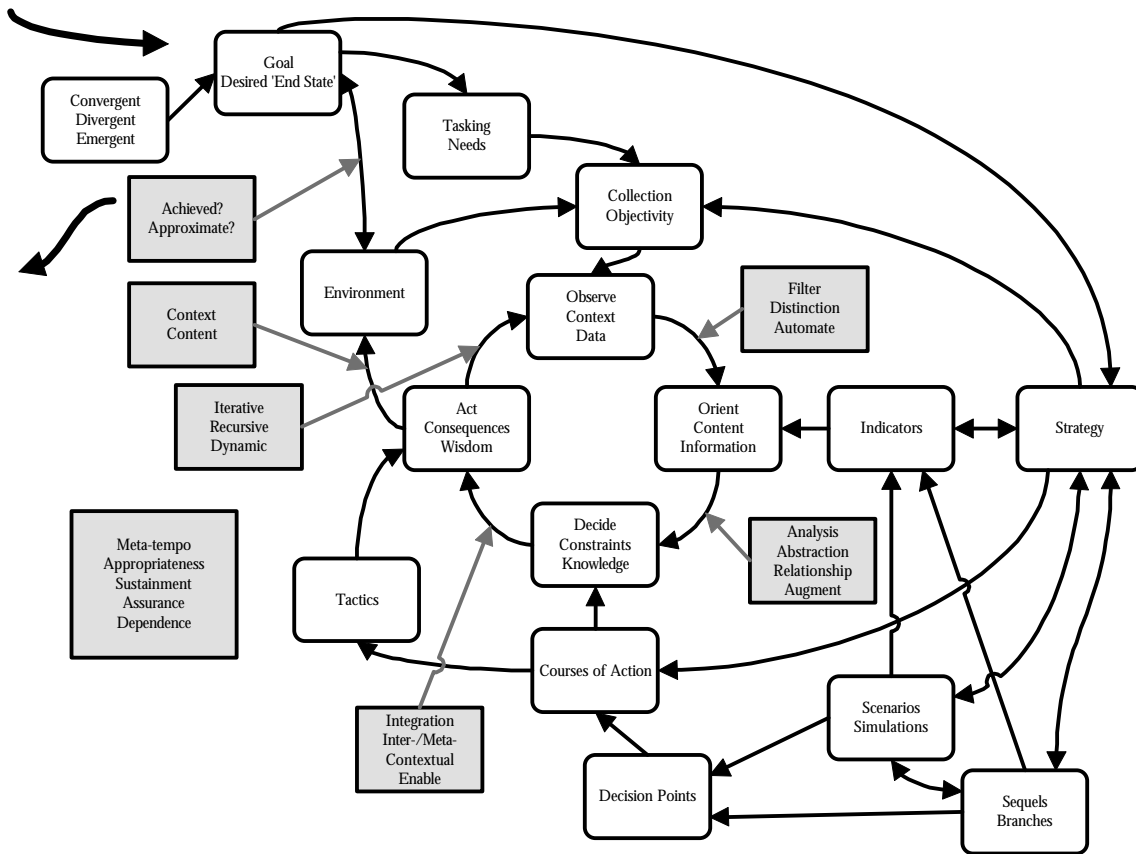
What is necessary now, and into the foreseeable future, is the construction and delivery of adequate and accurate models to every aspect of the decision cycle, rather than just the decision-maker. This also allows the decision-makers to be better informed in many ways, particularly the '4Ms': monitor, measure, manage, and mitigate.

In short, the key differences are as such:

- Models are more comprehensive than 'details'—the best models are those which provide a direct 'one-to-one' correspondence to whatever system is modeled. The more complete the correspondence, the more useful the model. This is not to say that models need to be comprehensive before they can be delivered and of use; models should, in fact, be delivered as soon as a 'rapid prototype' is available, and continually improved
 - Intelligence is a continual process—the world is high tempo, and if you slow down or stand still, the product delivered to the consumer rapidly expires
 - Decision-makers, the consumers of intelligence models, are now at each and every level of an organization. To leave support of these consumers out of the decision-process is an invitation to disjointed decision-making and a schizophrenic organization
 - The author makes his 'Continual & Complete Intelligence Course' available, and it is highly recommended that the interested reader of this report refer to the courseware for more information and an introduction to this new intelligence approach
 - Integration of intelligence into conflict, particularly as seen in support of the decision cycle, means end-to-end integration, including in support of operations and direct action. This aspect in particular has been largely ignored by the conventional intelligence process, much to the detriment of those requiring intelligence support in the field
-

THE DECISION CYCLE

The decision cycle is best introduced through the following diagrammatic representation:



The Decision Cycle

Development of an understanding of the decision process has been an on-going project for almost two decades, and so this is a necessary discussion because I believe, from practical experience, that it is critical in any understanding of the direction military and intelligence operations are moving toward. I am only presenting a 'primer' lever of detail, cursory at best, because of the depth of the domain.

THE CORE OF THE DECISION CYCLE

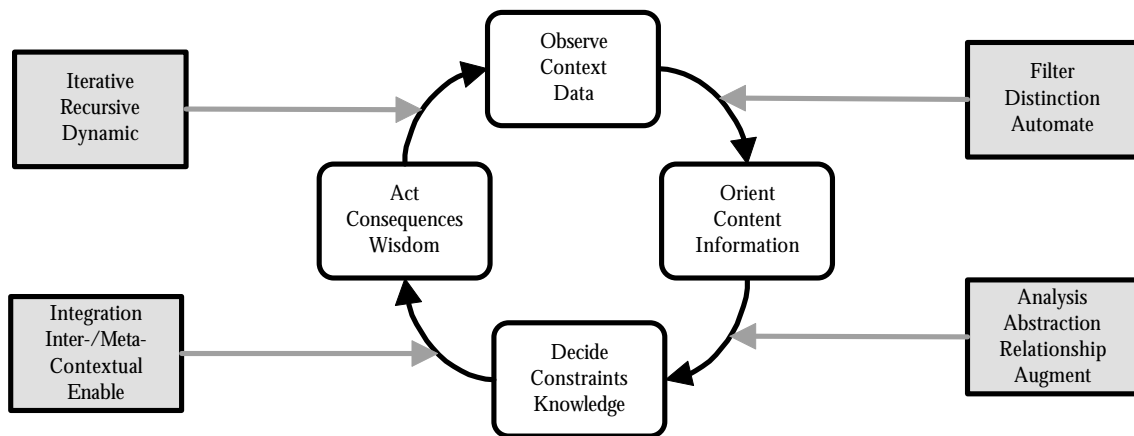
At the 'core' or center of the decision process are three 'isomorphic' or near-replaceable cycles. This is a significant conceptual breakthrough, since it means that tools from one of the domains of the cycles can be adapted to use in the other two domains to great advantage.

The three isomorphic domains and cycles are:

- Observe-Orient-Decide-Act, known as the 'OODA Loop' or 'Boyd Cycle.' This cycle comes from Colonel John Boyd, who attempted to understand why he won an aerial dogfight in the Korean War. He discovered that two factors were critical to his having survived: the canopy of his fighter was larger, thus giving him a greater field of vision; and his aircraft, while slower, was more maneuverable, allowing him to make more frequent adjustments. The results of Boyd's breakthrough in understanding led to improved pilot training for combat ("Top Gun"), the F-16 fighter, and the OODA loop. This could just as easily be represented by the cybernetic decision model as well, but the OODA loop has additional 'weight' over control systems—it's intended to be time-critical, time-competitive, and enable the human user to survive in and thrive on chaos

- Context-Content-Constraints-Consequences, which I've developed out of complexity theory. These elements are critical in understanding emerging, evolving, or dynamic systems, which is a very abstract way to refer to the real world. More important, as many military commanders have commented, no plan survives contact—this is because, once the shooting starts, all the assumptions have become inoperable, and the battlesphere is an emerging context that Darwinian, evolutionary pressures are rapidly unfolding within
- Data-Information-Knowledge-Wisdom, the basic elements of the cognitive science and cognitive psychological approach to the world, and how human beings model it internally. This is largely an area of cognitive transformation of models through analysis and application

Some definitions of the cycle elements will be helpful in a basic understanding.



'Core' Cycles

The

OBSERVE-CONTEXT-DATA

Observe, context, and data are what and how we experience, directly or through proxy, the real world. Immediately this means that we're operating on models of the real world that are already suffering from the 3Fs—freezing, flattening, and forgetting. Proxies further complicate matters—they may be 'objective' such as scientific instruments, video cameras, sensors, etc., or 'subjective' such as other human observers communicating with us somehow. This means that it's almost impossible to be truly, objectively aware of context, circumstance, setting. From an intelligence standpoint, this greatly complicates the process, because it may be flawed, corrupted, or subverted from the initial tasking and gathering.

ORIENT-CONTENT-INFORMATION

These three cycle elements are very 'clean' in how they are isomorphic. Orientation is where attention is directed. Context differentiates into content—entities, relationships, messages. Data reduces to information by a process of filtering or exclusion. All three domains have extensively worked out means and methods for defining boundaries, looking for distinctions, and measuring 'deltas' or differences. It's worth remembering Gregory Bateson's definition of information as any difference that makes a difference—this is an apple, that is an orange; this apple is here, that apple is there; this apple is now, that apple was/will be then.

In intelligence and decision support, this is an incredibly important area—knowing what's important, the management of complexity and information overload. It's important to know how to look for

indicators (hints or 'signatures' of what may be occurring), to have 'tripwires' prepared (use of indicators to provide early warning, but also to navigate the potential future through scenarios, sequels, and branches, which have been 'gamed out' during extensive simulation).

DECIDE-CONSTRAINTS-KNOWLEDGE

Information becomes knowledge through processes of analysis and abstraction, or through reduction to practice and application. This means knowledge is still largely 'intra-contextual' or still inside its originating domain, constrained. Constraints are the limits, boundaries, and relationships that provide structure. Making decisions remains a function of selection among options; the available options are defined by an understanding of the world, and limited by knowledge of it.

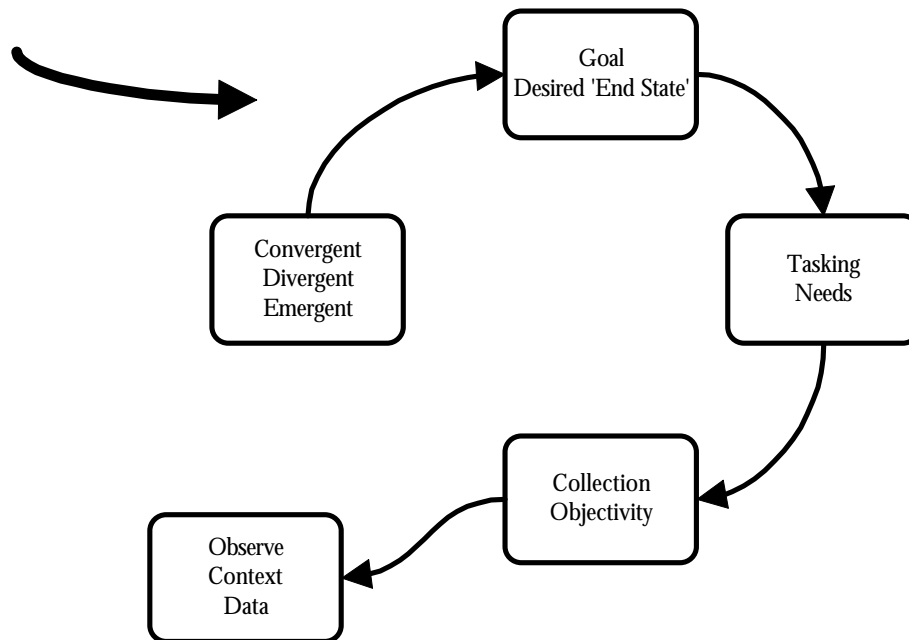
Intelligence and decision support are clearly essential here—to provide comprehensive models generated by the previous cycle elements, but also to support the decision-maker by providing the options, the potential strategies and tactics. In particular, this means a detailed composition of any and all potential 'scenario networks,' with the navigation points down scenarios, known as decision points, clearly delineated. Decision points are critical, and the more frequent, or 'higher resolution' of decision points, the more frequently the decision-maker can select for effective action. These potential options at decision points are known as course of action, which require considerable intelligence support, and are constrained by the intentions and capabilities of the decision-maker.

ACT-CONSEQUENCES-WISDOM

With an intelligence and decision support infrastructure in place, act moves beyond command & control (C2) communicating out orders to 'the troops,' but instead becomes delivery of decision models for coordination among potentially many different distributed elements working cooperatively toward a common outcome. Intentions, purpose, and desired outcomes are what the effects or implications of action are directed toward, transforming the existing world into the desired world. Achieving these ends requires understanding of the relevant concepts, systems, interactions, and relationships, many of which may be inter-contextual, given the complex and connected world, as well as 'meta-contextual' or 'higher level' systems of thinking such as IWAR, IO, PSYOP, and OSINT. While not generally appreciated, 'wisdom' on the battlefield is critical—it's the factor of novelty, doing the unexpected or impossible, providing moral and material surprise.

Finally, this set of aspects of the cycle are, ultimately, the overall purpose of the cycle—to support operations or application of capabilities in order to affect change on the context/content to achieve intentions, assure the process of the cycles, and sustain every aspect of the cycles.

The cycles are just that—an iterative, and at times recursive, set of processes that affect incremental, progressive transformation in the context or content, until the context/content matches the intentions of those involved in setting the direction of the cycle.



Initiating the Decision Cycle

Immediately upon initiating the decision cycle, it's necessary to decide which is the more appropriate approach based on the intention or purpose:

- Emergent intentions means having a 'wide-open' look at the world, because the areas of interest or importance are not yet known; this is a unbounded seek, best for being dynamic, evolutionary, and responsive to a changing world
- Divergent intentions means having a specific area of interest, but not knowing all the aspects of that domain or subject matter that require specific attention; this starts with a 'seed' as a search, and rapidly develops into a number of 'branches' of desired models, a comprehensive spectrum in scope and scale
- Convergent intentions are intended to narrow onto a specific detail or analysis to support a specific decision—particularly metric-based (how much, how many) or probability-based (what are the chances of X occurring)

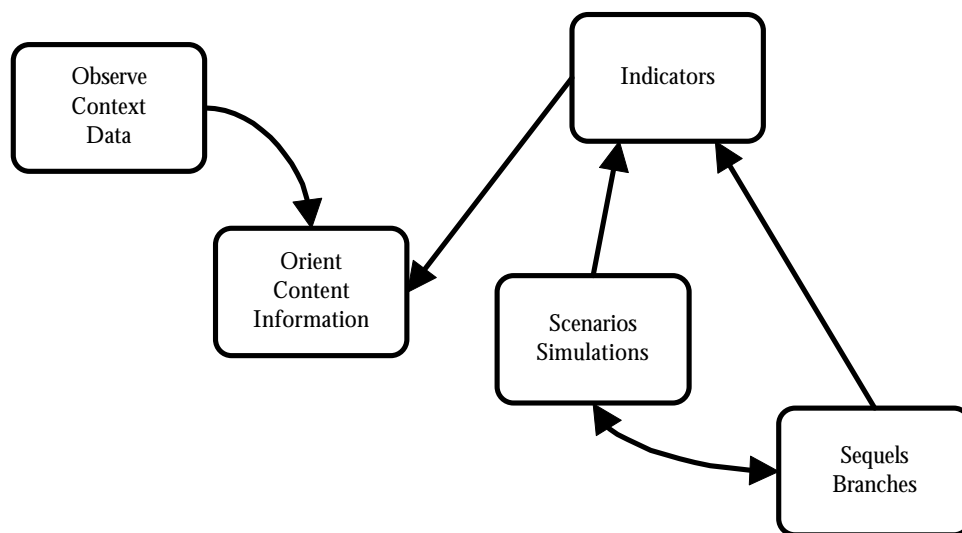
It's critical to have an image or impression of the desired 'end state' if the cycle is going to be 'goal-driven'; this requires that the cycle focus on making incremental changes until the real state of the context or content matches the desired state. It is also possible to be purely cycle-driven, particularly for the emergent approach, when it may be necessary to be entirely exploratory at times. Regardless of the approach, it remains crucial to survive and remain viable, because termination of the cycle pre-completion is failure—wars aren't won by dead heroes. Assessing and communicating the needs and tasking have been addressed in a number of different fashions, many of them quite useful at assessing the context in order to provide intelligence support to the decision cycle and operations:

- Modeling the potential approaches, problem and solution spaces, leverage points, relationships in the battlesphere and infosphere, the decision models of any possible entity that can affect the context, and the structure and integration of the various elements (like the roles/niches in an ecology)

- OPORD or 'operations order,' concentrating on: situation (context); mission (intention); execution (areas of support to decision and action); support, supply, and sustainment for the entire cycle; and 'command & control' (who sets the intent, who makes what decisions)
- METT-T: mission; enemy; terrain (context, battlesphere, infosphere); troops (resources in support of the cycle); time available (the 'window of opportunity,' synchronization)

Collection needs to be concerned with capabilities: sourcing and real-time monitoring (thanks to collection methods such as SIGINT and IMINT) that feeds into current reporting, tripwire notification, and in-depth/exhaustive acquisition of intelligence raw material. At this basic level, it is critically important to be accurate in the models of 'areas of interest,' 'areas of operations,' the information environment, and the core decision cycle requirements.

SUPPORT IN INFORMATION MANAGEMENT



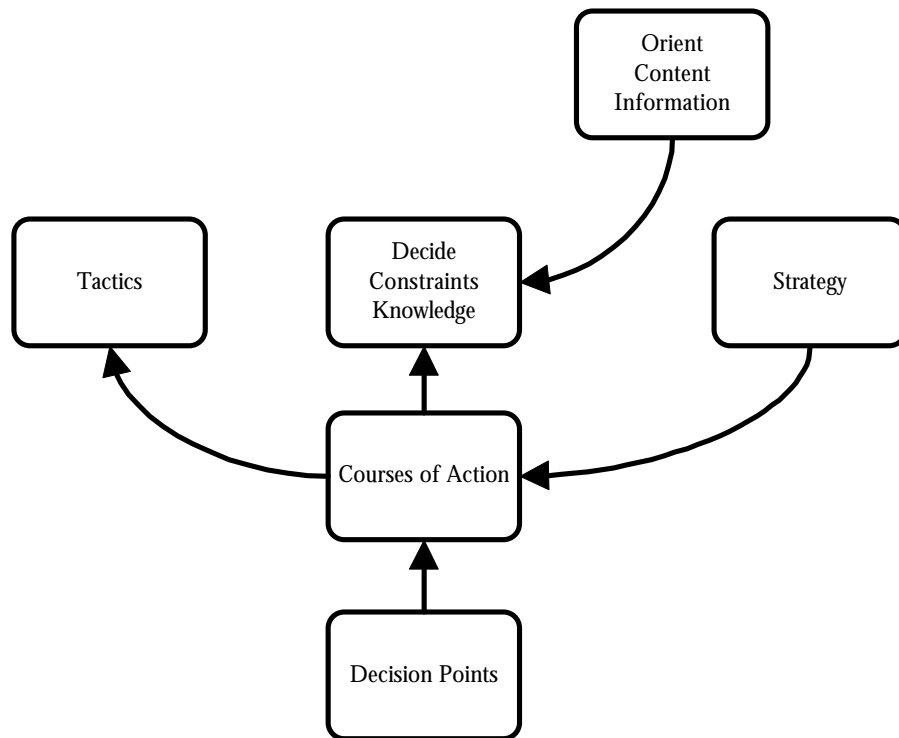
Cycle Information Management

Indicators are crucial—they're the means to decide what's important, and what affects what. Improper or ineffective use of indicators leads to information overload, the inability to distinguish what should be paid attention to in the volume of data and models. Intentions indicate the approach to achieve the objective, and provide selection among analysis methods and analytical products—what's the context/situation when viewed against cues and patterns of possible intentions, capabilities, courses of action, and decision points? In particular, indicators are the 'danger signals' that allow navigation through scenario networks.

Scenarios are detailed models of possibilities, options, opportunities. Scenarios, because they encompass potential sequels (what to do at decision points if an action is successful, in order to further pursue goals) and branches (what to do at decision points if an action fails, in order to correct, manage the consequences, and regain the initiative), are actually cascades, networks of subsequent cycles and their associated probabilities, priorities, indicators, strategies & tactics, further decision points with sequels & branches, and what support is necessary.

Simulations are a critical tool in scenario development—the 'active gaming' of conflict in a context, in order to fully develop rich models of all the potential scenarios. This too is an iterative process—as the cycle progresses, it will always be necessary to maintain a function exploring scenarios through simulation, and passing key indicator and tripwire models along to others in order for scenarios to truly be effective.

SUPPORT IN CONVERGING ON A DECISION



The Decision-Maker Commits

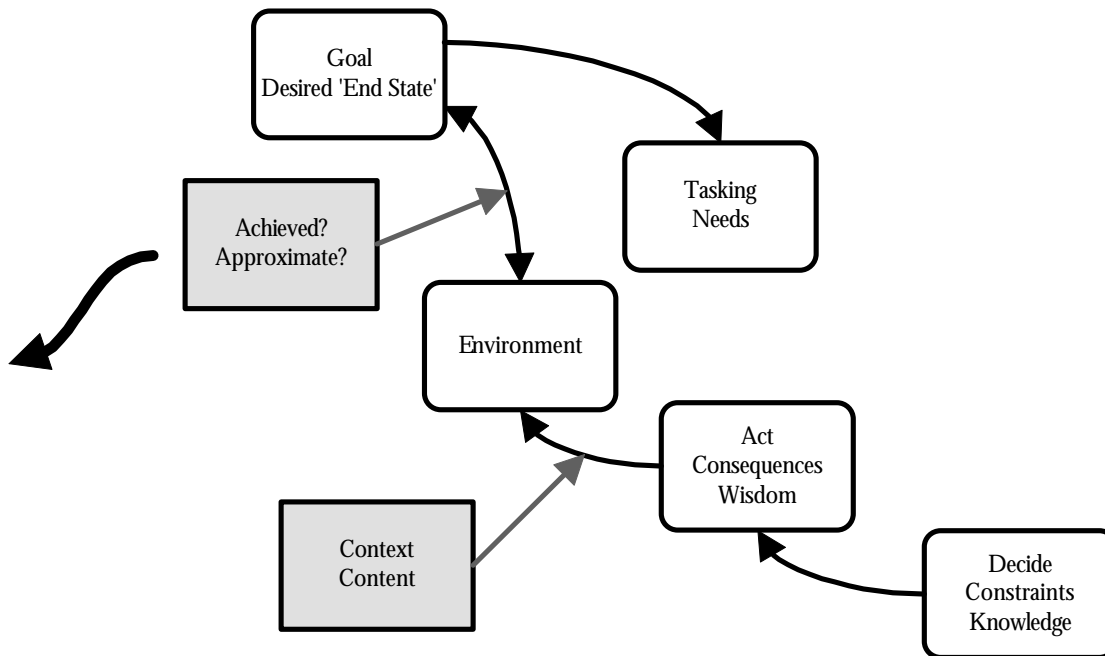
The decision-maker selects among a number of options (choosing not to take an action is still making a decision, just perhaps not a very effective one). The guiding principles in generating decision points and potential courses of action, as well as how to select among them are thought of as strategy. Strategy provides the means and methods, the approach, analysis, and methodologies necessary, and establish the thresholds required to converge on a decision.

Decision points are of variable granularity (frequency of occurrence of 'nodes' in the potential scenario network)—the more decision points available, the more frequently the decision-maker can affect a situation. This is particularly critical in contexts where tempo provides a competitive advantage, or the situation itself is so rapidly changing that a large number of decision points are necessary to survive. Decision points are generally 'internally' directed—oriented at those elements inside the intentions and capabilities for influence or control of the decision-maker.

At decision points, there are generally a large set of potential courses of action—the possibilities, options, and opportunities for action to be taken or that are available for exploitation. Obviously, in order to 'weigh' the potential options, it is also necessary to view the potential consequences (in other words, this area is intensively interactive with the scenario and simulation function to provide sequels and branches). Courses of action are also constrained by intentions (and refinements, such as the rules of engagement, order of battle, synchronization, etc.) as well as capabilities (what is actually possible with the resources and support available) and dependencies (an 'order of operations,' as well as the dependency web involved in sustainment and assurance).

Tactics are the 'methods of execution' of the decisions, as well as a way of navigating the available decision points and scenario networks. Communication from the decision-maker to those responsible for carrying out the decisions can be simple and secure representations or messages (orders, advisories, perspective), through complex models that would make the entire decision process (including scenario networks) available to those actually engaged in operations.

SUPPORT IN OPERATIONS



Operations to Achieve the Objective

Operations involve the use of capabilities to affect context or content in order to shift the situation toward the intended goal or end-state. This means the cycle is iterative—converging on the intended end-state through continual, progressive transformation.

It's important to remember that the cycle needs to be dynamic and responsive—tempo in the cycle needs to be appropriate to the situation, and the cycle needs to be sustainable until the objective is achieved or the decision-maker changes their position. If adequate models are delivered from the decision-maker to those responsible for operations, then there is considerable flexibility and potential for initiative through independent decisions, constrained inside the overall mission objective. Bi-directional communications between decision-makers and operators is crucial—complex, active, responsive models from decision-makers gives the operator the initiative, and feedback from the operator provides the decision-maker realtime assessment of effects on context and content. This allows more effective application of the entire cycle, and leads to more rapid goal-achievement through the potential for retasking and continual improvement inside the cycle. One caveat, however, is that the use of novelty is critical—the more intelligent the opponent, the more important it is to break potential patterns of behavior and avoid 'standard operating procedure.'

IWAR, IO, OSINT, PSYOP

Infrastructure is comprised of processes, representations, and structures that provide an economy of scale or 'force multiplier.' The conceptual process of the integrated intelligence and decision cycle is a decision support infrastructure, and so a key point of leverage in modern conflicts. Because the system is effective, it's obviously a target for opposition to the intentions and goals of those utilizing the infrastructure and cycle. Because most of the elements of the cycle are so poorly understood by those applying them, and because technology is integrated at every element, the vulnerability of the cycle is enormous.

Intelligence and conflict are integrating in key areas, both offensively and defensively:

- IWAR, infrastructural warfare, looks at conflicts based on dependency and infrastructure. Using the IWAR conceptual tool, it is possible to understand conflicts crossing the technology spectrum and focus of operations
- IO, information operations, looks at a subset of IWAR conflict, specifically targeting decision cycles and 'infostructure' or information infrastructure. This is the modern, high-technology equivalent of the old 'unconventional warfare' or UW
- OSINT, open source intelligence, provides intelligence and decision support services without resorting to espionage—critical in high-tempo conflict
- PSYOP, psychological operations, can be 'direct action' (DA) or counter-operations to IWAR, IO, and OSINT through subversion

IWAR is the overall conceptual strategy that unifies a number of approaches to conflict. As the inventor and pioneer in IWAR, I've developed a number of crucial tools necessary to apply the strategy and tactics. One of these tools, the Boyd Matrix, looks at the core cycles of the decision cycle and explicitly targets them. As there are four steps in the cycle, there are 16 possible combinations of attack upon them or process failure by those operating the cycle. This leads to a simple binary notation, with attack or failure of a step indicated by a '1,' and a complete good cycle represented by a '0000.'

Use and escalation of IWAR, IO, OSINT, and PSYOP are interesting. My own personal interactions with a large variety of non-State 'opposition forces' as well as military and intelligence organizations for Nation-States allow me to conclusively state that, no matter what the intentions, as soon as a capacity to run such operations is available, it will be used, continued, and escalated. I will discuss this in greater detail later in the report, but it's important when looking at this section to understand that this is the expanding and probable area of operations in most future conflicts that are not purely force-on-force State-against-State affairs.

THE BOYD MATRIX & CONFLICT TYPE

0010	Manoeuvre warfare, assassination
0011	Management/command failure
0100	Guerrilla warfare
0110	Terrorism
0111	Political warfare
1001	Attrition warfare
1100	Propaganda
1110	PSYOP, propaganda
1111	Weapons of Mass Destruction, UW, IO

Conflict types by attack or failure in the decision cycle.

Briefly, to understand how the attacks or failures delineate conflict type:

- Attacks on Command & Control (C2) such as in manoeuvre warfare, or commanders directly on commanders using assassination would be conceptualized as a 0010 under Boyd Matrix notation
- Guerrilla warfare concentrates on opportunistic attacks, particularly where not expected, and thus where 'attention' isn't focused
- Terrorism is similar to guerrilla warfare, but will also target command, commanders, or operate in ways intended to attract attention
- Political warfare targets attention, decision, and action; this may be direct action (attacks), attention (PSYOP, demonstrations, rioting), or subversion of will
- Attrition warfare attempts to collapse the observation and action elements of the cycles through inflicting mass casualties. This sort of warfare remains devastating in 'low-technology' or 'Third World' regions because the social support infrastructure is so manpower intensive in order to remain functioning
- Propaganda works to alter the perceptions of the observation and orientation elements of the cycle
- PSYOP may also include propaganda, but is also directed at an effect in the decision-maker, such as an alteration of intention, perceptual shifts, or subversion of their judgment
- Weapons of Mass Destruction, unconventional warfare, and information operations can have catastrophic consequences upon every element of the decision cycle, which is a significant reason for the growing interest in the fields

BOYD MATRIX & INFRASTRUCTURE TYPE

1111	Communications, infostructure
1110	Media
1101	Power, air/rail/public transport, shipping, bridges/tunnels
1001	Fuel
0011	Schools, spiritual institutions, Emergency Management Systems, governance
0001	Water supply, business, financial services, economy

Infrastructural elements that support conflict, and thus become targets, by attack or failure in decision cycle.

Various aspects of infrastructure, both physical and 'virtual,' support the decision cycle, and thus are targets:

- Communications and data networks are essential to every aspect of the decision cycle

- Media generally has little effect upon operations; the lessons of Vietnam have been learned by Nation-States, and journalists and the cameras are kept away from anything that might be critical. Terrorists and guerrillas generally desire media coverage, and so don't target media 'at large,' even if they might attack individual journalists
- Power, transportation, and choke-points have a large effect upon any aspect of the decision cycle that requires mobility and electrical support
- Fuel has smaller direct impact on the specific process of 'attention,' other than observers not being able to get in place at all. Note that fuel is inversed in the view of decision-makers—without fuel, everything grinds to a halt
- Schools, spiritual institutions, emergency services (police, fire, hospitals, etc.), and governance are 'soft targets' and so have direct impact on decision-makers (generally through public pressure) and thus shift priorities in operations. Governance is directly attacked (on command structures and commanders), as well as the symbols of governance (flag burning, Embassies, etc.)
- Water is critical in support of operations and life-sustainment. Financial warfare—attacks on business, financial institutions, financial systems, markets, etc. has dramatic impact on operational capabilities in sustained, 'slow burn' conflicts

CONFLICT TYPE EXAMPLES

0010	Manoeuvre warfare, assassination Attack or cut off command
0011	Management/command failure Attack C42I, command support
0100	Guerrilla warfare Opportunistic attacks on military orientation (GPS)
0110	Terrorism Car bombs, targeting of civilians
0111	Political warfare Rioting, social subversion
1001	Attrition warfare Mass killings, friction of war
1100	Propaganda Subvert the will to fight, public support

1110	PSYOP, propaganda Subvert command authority, command judgment
1111	Weapons of Mass Destruction, UW, IO NCBW, 'Pearl Harbor' scenario

Brief examples of attacks, per attack type.

INFRASTRUCTURE ATTACK EXAMPLES

1111	Communications, infostructure Attack satellites, sensors, switching, Internet (DNS), etc.
1110	Media Subvert media, Internet as entry point to media cycle
1101	Power, air/rail/public transport, shipping, bridges/tunnels Power grid, maintenance, monitoring, switching, market; attack coordination of transportation system (e.g. traffic control)
1001	Fuel Unrest or instability in the Middle East; disrupt supply chain; manipulate market
0011	Schools, spiritual institutions, Emergency Management Systems, governance 'Soft' targets, critical support mechanisms, social contract
0001	Water supply, business, financial services, economy Supply systems; economic warfare, manipulate markets

Brief examples of IWAR attacks, per attack type.

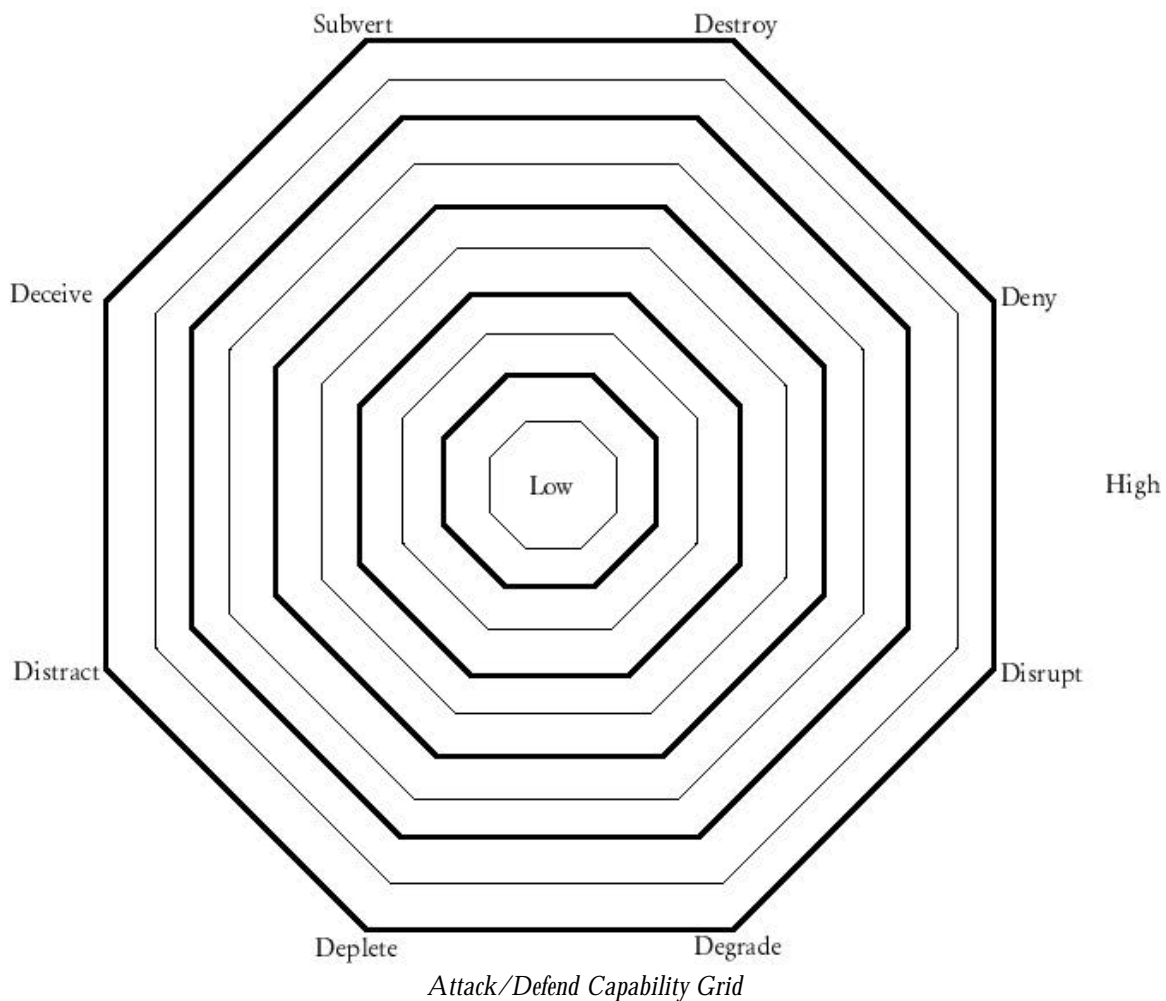
CONCEPTUALIZING ATTACKS

There is a spectrum that is useful when thinking about attacks:

- Destroy is outright elimination
- Deny impacts on capabilities by removing options
- Disrupt is chaos, confusion, or other difficulty in the cycle

- Degrade is slowing down or reduction in effectiveness of capabilities
- Deplete impacts on support, necessary capabilities, limited attention
- Distract is misdirection as well as media events that shift attention priorities
- Deceive is providing false or faked detail to elements of the cycle
- Subvert undermines will, priorities, judgment, command authority, or other elements necessary to be effective

Each of these elements can have a 'metric' assigned, and be linked to offensive intentions and capabilities, as well as defensive efforts and vulnerabilities. Graphical representation, such as on the diagram below, can be useful for rapid assessment and comparison between players.



OPEN SOURCE INTELLIGENCE

Intelligence without espionage is rapidly becoming more powerful; OSINT is, however, much more effective against the West and other 'open' countries. Some Nation-States, such as China, have taken great advantage of this fact, even to the point of having written a comprehensive manual on how to engage in OSINT against the U.S. Various Nation-States have also engaged in competitive intelligence programs taking advantage of 'compound' information—assembly from multiple sources of all the necessary materials to support various programs, from intelligence and decision support to economic expansion.

An example I like to show that demonstrates the power of OSINT is the vulnerability of the U.S. military. It is possible, and in fact easy using the Internet, to obtain a list of military bases and military facilities around the world; using such a list, the coordinates of these bases can be found in a number of locations. Once the coordinates are known, a number of satellite photographs of bases and facilities can be downloaded. Interpretation of this IMINT is possible by going to the U.S. Army's Digital Technical Library and downloading the educational and training materials available—they've restricted access to field operations manuals, but all of the support and logistics field manuals are available. Just one, Petroleum Supply In-Theater, can be used to interpret the satellite images and tell what is what in the entire fuel supply for the base or facility, even to the point of knowing the pipe diameter. 95% of attack planning can be supported using OSINT against U.S. military targets—and civilian targets are in even worse shape.

PSYCHOLOGICAL OPERATIONS

Psychological operations can be 'direct action,' or initiated by decision-makers, or to counter the PSYOP initiated by an opponent. PSYOP can be used particularly effectively against the West and other open Nation-States in a variety of ways:

- Subversion of will. Most Western or Western-influenced Nation-States have established political authority over military and intelligence objectives and forces. Subversion of the public and public perceptions impacts on politicians and policy makers, who are generally also the decision-makers. Such actions can stop or even prevent intelligence or military operations, to the detriment of the Nation-State
- Subversion of command authority. Undermining trust in command requires a significant understanding of the opponent and profile/mindset, but again, undermines the ability of intelligence and military decision-makers to be effective in their operations
- Operations such as 'diversionary diplomacy' and other deception operations. In the decision cycle, these attacks are oriented at data gathering, attention and focus, options and priorities, and what actions are appropriate. This can be accomplished by subverting sensors and proxies, including human observers, attacks on the Global Positioning System (GPS), disguising indicators (which is what camouflage does in a primitive way), providing false 'effectiveness' intelligence (such as faking damage, and thus subverting the Battle Damage Assessment), and attacks on trust and assurance necessary in the decision cycle

PSYOP is poorly utilized by Western Nation-States because it 'feels unfair' or other such nonsense. Modern and future opposition forces are expanding their own intentions and capabilities, and PSYOP is becoming a critical aspect of all operations.

THREAT SPECTRUM

It's worth knowing the 'threat spectrum' or range of potential operations that can have immediate and negative impact on the decision cycle. The spectrum is best considered by threat, probability of occurrence, the scale of potential negative consequences, and the required sophistication to possess the capability:

[31December2001 note: this grid indicates levels as of the time of April2001, not post-11Sept2001.]

THREAT	PROBABILITY	CONSEQUENCE	SOPHISTICATION
Terror	2↑	3↑	6↓
Blackmail	2	2	7↓
Subversion/sabotage	3↑	6↑	4↓
WMD	2	10	4↓
Information Operations	4↑	8↑	6↓
Insider Trading	2	2	8
Dependency Attack	7↑	8↑	8↓
PSYOP/Reputation Attack	8↑	10	8↓
Industrial Espionage	8	9	5↓
Theft	10	10	9↓
OSINT	10	7↑	7↓
Viral Attack	10	10	8↓
DoS/DdoS	8↑	5↑	5↓
Hacktivism	10	2	5↓
Competitive Intelligence	9	10	7↓
Net Probe/Map	10	9	6↓

Threat Spectrum

- denotes an increase; - denotes a decrease

These threats will be defined and discussed in great detail later in the report, but for now it is sufficient to note that the variety of threats (the scope of potential threats) is increasing, the probability of being attacked is increasing, the consequences of being attacked is increasing, and the sophistication necessary to launch most attacks is decreasing.

THREAT SPECTRUM BY COMPETENCE

It is worth considering the threat spectrum by player as well:

- The Nation-State with the 'best practice' in offensive (threat) capabilities is China
- Middle-tier Nation-States, those working diligently at putting comprehensive capabilities in-place, are the U.S., Australia, France, Germany, India, Pakistan, Israel, the Palestinian National Authority, and Russia

- The 'Opposition Force' best practice occurs in a range of capabilities, but includes groups such as Al-Qaida (Osama bin Laden's network), Hamas, and the Zapatistas
- Middle-tier opposition forces include organized crime and FARC (the Colombian narco-terrorists)

[**31December2001**: Note the Al-Qaida/bin Laden reference in the original.]

DEFINITIONS, ANALYSIS, & ASSESSMENT

It is important to reinforce that the conceptual basis and tools presented here are critical in understanding and utilizing the content of this report, as well as to be a player in the emerging conflicts.

A note on language: some of these concepts may not 'translate' well outside English, or may be unclear even within English. There are large concepts behind many of these simple terms, and hopefully the nuance will not be lost. This obviously occurs with translation of concepts into English. The German 'wirkung im ziel,' translates in English to 'effect in target,' which in a simple translation would appear to simply mean the damage caused by a weapon system. In fact, there are a number of psychological overtones associated with the German original that are critical in understanding; for example, during Desert Storm, the Coalition Forces used U.S.-made cluster bombs, which are far more effective than mortars or artillery shells. Survivors (and there were very few) of such attacks were highly motivated to surrender, and generally tried to do so as soon as possible. Even less effective weapon systems such as the B-52 had similar 'effect in target,' which became a factor in Coalition PSYOP. I will attempt to communicate the nuance as best able in the explanatory text, and I hope that suitable equivalents will be possible across the linguistic boundaries.

The critical factors used here to analyze and assess the players and targets have been developed over a considerable length of time by the author, and has been refined or expanded as necessary. Field operations have been critical in our development of this toolset, because those factors that looked important during the planning stage have proven to be meaningless, and 'minor' factors have turned out to be quite significant.

MOTIVATION/WILL

This is the overall set of factors that generate behavior and constrain selection among available options. Profiling, the intelligence function used to 'map' an individual's motivation and 'construct space,' is important because it can help in understanding the operations of other players, but profiling is dangerous to use predictively—the world, and entities within it, are not linear constructs (at least, there are a few people that can exhibit radical shifts in behavior that will make linear predictive profiling meaningless, and lead to the potential for moral and material surprise).

An extensive discussion of motivational elements is available in the the author's **Continual & Complete Intelligence Course**, and so will not be presented here. What we don't discuss in the 'public' materials, however, is that motivation is not entirely a 'post-fix' operation for most individuals, but can in fact be structured in an 'anticipatory' construct. In other words, some sets of behavior are engaged in by individuals because they've worked in the past, and have every possibility of working again in the future. This is crucial in profiling, because it provides areas where 'linear' thinking of an opponent can be used against them—which is the heart of deception operations.

MISSION/INTENTIONS

Decisions about a mission—what end-result the operator wishes to accomplish—and intentions—the over-all principles (similar to motivation, but more ‘pro-active’) under which an operator functions, are the ‘entry points’ to the decision cycle discussed previously.

This can largely be an area of ‘business as usual’—most of what is going on in the world is reasonable, acceptable, and doesn’t need any dramatic change for the operator. Operators can, however, be ‘goal-driven’ and want to change what is ‘now’ into something envisioned as a possible future. Events can also occur which make ‘now’ unacceptable, and so the decision cycle is initiated to ‘restore’ things to the way they were. Understanding the ‘goal’ of the opposition, or their acceptable ‘baseline,’ is critical in understanding their decision cycle.

COGNITIVE APPROACH

This is the mental toolset with which the operator approaches the world; some toolsets are very narrow (conventional warfare, attrition warfare, etc.) while some have been explicitly structured to provide cross-domain, cross-context effectiveness (IWAR). It’s also important to distinguish whether an operator is goal- or event-driven, because those provide the thresholds that trigger decisions in an operator’s cycle.

In addition, there are three overall approaches to operations that are worth categorizing: initiative, responsive, and reactive. Initiative, which is commonly seen in goal-driven operators, means being pro-active in transformation of the context or content, or perhaps alteration of the range of constraints. Responsive operators straddle the initiative and reactive approaches—they ‘look forward’ to potential changes that they would consider unacceptable, and undertake operations to prepare or pre-empt the changes from occurring. Reactive operators are purely affected by events, and then initiate operations—and the operations that are initiated are generally ‘standard operating procedure.’ This latter category are particularly trapped in their mindset—if it worked before, it will work again; if the only tool you have is a hammer, every problem looks like a nail.

OPPOSITION

These are two important categories: who does the operator consider to be ‘the enemy,’ and who considers the operator as their ‘enemy’? While mapping the space of players that an operator considers ‘friendly’ or ‘neutral,’ much more can be learned from the clean and clear lines drawn by what is opposed.

It’s important to note that the two categories may not be identical, and that is crucial from an operator’s perspective. Those defined as opposition are forced into their own cognitive approaches to cope with a hostile operator; some boundaries can’t be crossed back over, and so defining an opposition may force them into shifting their own position to ‘reciprocal-hostile.’

AREA OF OPERATIONS

Originally, the area of operations (AO) was the region within which an operator would be engaged. An AO may be ‘smaller’ than an ‘area of interest,’ but the two are getting blurred and indistinct in the modern, interconnected world. An AO makes more ‘sense’ when view as those things that are critical, important, or affect the operator. Even this is poorly defined by most operators, as they have little understanding of their position in the global dependency web and ‘value web’ (political-economic exchange networks).

The expanded definition of an area of operations now must include ‘cognitive’ and ‘virtual’ domains along with geographic regions—markets, human rights, the information environment, ‘cyberspace,’ etc. are all potential AO’s for the modern operator. Proper definition of an AO is important to prevent being overextended—trying to be all things to all people.

AUTHORITY, RESPONSIBILITY

Authority and responsibility are not the same thing, even though many hierarchical structures ‘seat’ the two concepts as linked elements.

Authority is what an operator may have control over (or may perceive they have control over); this can be conceptually connected with an earlier point over being ‘goal-driven’—those in authority get to set the goals, and ‘give the commands’ that commit to a course of action (what we refer to as the decision-maker). Responsibility is what an operator is accountable for, and is willing to be a ‘source’ or take the initiative regarding; most hierarchies concentrate on the first aspect (accountability), and this connects to being ‘event-driven’ in approach. Operators in a position to be flexible (because they are independent, or because their organization is structured appropriately) can in fact be ‘a source’ or leader.

This, for most operators, particularly those that are organizations, is a true muddle; there has been a great deal written on organizational issues, and I have done considerable work myself in this area. The friction and inefficiencies in an organization are critical targeting points, and breaking down cohesion and inter-operability is generally a ‘soft’ target. Many failures viewed in the Boyd Matrix are organizational failures and process failures that have their origin directly in this confusion.

CAPABILITIES

Commonly confused with intentions (just because you *can* do something doesn’t mean you are going to—most social contracts that allow civil society to function rely upon this distinction), capabilities are the range or spectrum of actual options available to an operator. They may be ‘real’ or material/materiel, such as the capability to utilize an available weapon system; or ‘virtual,’ such as the capability to think through a problem or having an available skillset.

Intentions and capabilities interplay. Having certain intentions can lead to capabilities being developed or acquired. Having an available capability makes the ‘ease of use’ much more possible. The confusion about intentions and capabilities is understandable, and the complexity can be managed by having clear models of intentions, capabilities, and the interplay as three separate domains.

STRATEGY & TACTICS, APPROPRIATENESS, EFFECTIVENESS

There are many definitions of strategy and tactics; some have even attempted to simplify the issue to the point where strategy is ‘what occurs before the conflict starts’ and tactics are ‘how the conflict is waged.’ The defining line is not so clear, and the over-simplification leads to information management issues during the decision cycle. Strategy can perhaps best be thought of as how an operator thinks about problems, and particularly how they make decisions (particularly when presented with a range of options across decision points, and a variety of courses of action—how those are prioritized and selected). Tactics can be thought of as the transformative processes—real and conceptual—used during the decision cycle to change the context and content toward the goal or desired ‘end-state.’

Appropriateness and effectiveness are ‘meta-tempo’ issues in the decision cycle. They are issues that are used across iterations of the cycle to correct the various elements. Appropriateness is the level of ‘fitness’ of the cycle elements to what is going on. An example of appropriateness would be in tempo—faster is not always better. When driving an automobile, there are places where driving as quickly as

possible might seem reasonable (a straight road, no other drivers on the road, a safe and reliable automobile, etc.), but driving at high speed is inappropriate around sharp turns, in heavy traffic, around pedestrians, etc. Effectiveness is another fitness issue, but it is a measure of how well the cycle is performing at transforming the context or content in the desired ways. To return to the automobile example, the driver could be enjoying a rapid and safe journey, and admiring the view along the way, but be heading in the wrong direction.

Appropriateness and effectiveness, which are how strategy and tactics are continually improved, are not 'linked' concepts—something can be appropriate but ineffective, and something can be effective but inappropriate.

These are very complex spaces to model regarding operators, but they provide critical insight into assessing how 'introspective' an operator is, and thus how well they can survive and thrive in chaos or to other changes in their environment.

COURSES OF ACTION

Courses of action (COAs) are 'fed' by detailed scenario networks (all the potential things that may happen, and the potential things that may happen after that, and so on) that have been 'gamed out' using simulations. These scenario networks are 'navigated' using intelligence provided to the decision cycle, particularly indicators and signatures that provide information as to which 'paths' of the scenario network are probably currently in process (like reading street signs to navigate while driving). Scenario networks are constructed from 'decision points'—literally any time a decision could be made. Resolution or 'granularity' of decision points (DPs) is critical—the more frequent the DPs, the more frequently a decision can be made, or *has* to be made—if an operator's decision cycle is 'higher tempo' and has a higher granularity of DPs than their opposition's decision cycle, then the operator can transform the context or content more rapidly than the opponent can, and faster than the opponent can cope with (the opponent's decisions have less and less to do with the actual situation).

Decision points in the scenario network provide an available selection of options among which the decision-maker selects—these are the courses of action. In high-quality scenario networks, each DP and set of COAs are also connected to sequels (what network of potential options become available if the COA is successful) and branches (what network of potential options become available if the COA is unsuccessful, to correct, manage the consequences, and regain the initiative) in a continually expanding network. The decision-maker selects COAs that will lead to a successful conclusion of the decision-cycle—achieving the goal or desired end-state.

Since no emergent process can be adequately 'gamed out' in advance—it's impossible to decompose out all the potential events and options of the real world—this is an on-going function that is continually in support of the decision-maker.

TRADECRAFT, TOOLS, TECHNIQUES, MEANS, METHODS

Related to, but more specific than tactics, these are the real and virtual tools that are used throughout the decision cycle to accomplish the necessary process at each step.

Tradecraft is an intelligence term used to describe the processes used by human assets and officers to engage in the intelligence cycle. This includes everything from using 'dead-drops' to escape and evasion. Intelligence tradecraft is largely taught as a dogmatic process—do this, then do this, then do this, etc.—rather than discussed in terms of why things are done, and why they work (or why and when they might not, which is of critical importance). A more expansive view of tradecraft education would empower the individual operator to be more flexible, inventive, and survive longer.

Tools are generally thought of as the physical elements that enable the process—intelligence-gathering technology (sensors, satellites, etc.)—but the supporting information technology is obviously a ‘blend’ of conceptual tool and physical representation.

Techniques are the ‘higher level’ approach that can provide a more abstract approach to intelligence. For example, one technique is ‘pre-texting’ or operating ‘as if.’ This is also sometimes referred to as ‘social engineering’ because it largely relies upon assumptions and expectations. Wearing a jumpsuit, carrying a clipboard, and walking around like you belong somewhere (perhaps to pick up a package, or some other ‘normal’ function) is pre-texting, and can provide access to many restricted areas because it takes advantage of the assumptions and expectations of those that may perhaps question the operator. This is a complex field, generally referred to as ‘deception operations,’ but it can also include domains such as camouflage.

‘Means and methods’ are a single concept, but generally refer to a compound of the previous elements—what is it that will be relied upon to achieve the purpose of some element of the decision cycle, or support to it.

COMMAND & CONTROL

Command & control (C2) refers to a decision-maker in a position of authority making decisions (selecting among COAs at DPs), giving orders, and knowing the situation (sitrep, or situation report) of those under such command. This is a hierarchically-driven approach, top-down, bureaucratic, and prone to a great number of problems.

A new approach, almost the inverse of the C2-mindset, is through communication and coordination. Distributed operators independently acting, under their own initiative but under a common intention and set of motivations, can be incredibly effective, and are much less prone to ‘single points of failure’ or attacks on the C2 function (maneuver warfare, assassination, ‘decapitation’ of C2 support networks, etc.).

Also relevant are some additional structures that have converged and created compound acronyms:

- C4: command, control, communications, and computers
- C4I: command, control, communications, computers, and intelligence
- C42I: command, control, communications, computers, intelligence, and interoperability
- C4ISR: command, control, communications, computers, intelligence, surveillance, and reconnaissance

What this reflects is a move upon military forces and command structures to integrate what they have been learning in their own operations—the support infrastructure is essential to the decision process, the need to move away from centralized command structures, the integration of intelligence into conflict, and the need to coordinate among many different types and locations of forces.

DISCRETE/CONTINUOUS, SHARING

Among the many failures of conventional intelligence and decision processes, maintaining ‘discrete’ or constrained cycles (compartmentalized, limited duration, bounded scope, non-iterative and thus not correcting or improving) is important to gauge in an operator. Some operators are running limited or completely continuous processes, and this coherence provides a competitive advantage.

Sharing is a factor to note. The 'DIKW' (data, information, knowledge, and wisdom) of an operator, particularly organizations, can be strictly limited in distribution (intentionally, such as through compartmentalization, or unintentionally, such as when critical elements are human-centric and thus not digitally portable). Such internal constraints severely limit effectiveness and improvement; 'best practice,' innovations, and outright invention that doesn't positively impact on an entire organization is, literally, mostly wasted.

DECISION PROCESS

The decision cycle is discussed in detail previously in this report. The more comprehensive a model of an adversary's decision process an operator may have, the potentially more effective operations can be at targeting it.

Scale and scope are critical issues here. The individual operator has a number of drawbacks (limits in time, attention, energy, etc.), but has the advantage in a unified decision cycle. Organizations encounter scale and scope problems—too many people with too many different ideas about what should be done, across too many boundaries (functional, language, regional, etc.). Association of who has authority and who has responsibility for what domains, aspects, and elements throughout the process map of the decision cycle can provide insight into friction and interoperability issues that are encountered by every organization.

TEMPO

Tempo is literally the rate at which the decision cycle turns over or passes through iterations. More important is the use of tempo as a measure of the rate at which effective decisions are made. Tempo, particularly the turnover of COAs at highly granular DPs by the decision-maker or operator, provides a significant competitive advantage.

Tempo isn't the only essential view of cycle turnover, there is also 'meta-tempo' or the tempo of tempo. This means the 'rate of change' in the 'rate of change,' which may be intentional (to maintain an appropriate tempo for the circumstances, or for synchronization purposes when acting under command or cooperatively) or unintentional (such as losing capabilities through loss, attrition, lack of supply and sustainment; security issues and assurance of the decision cycle). Monitoring of the meta-tempo is critical in achieving appropriate and effective operations.

STRUCTURE

Structure is actually three linked concepts:

- Process, which is represented mostly by the decision cycle, but includes all the functions and inter-related functions of the operator
- Representation, which is the profile, mindset, and symbol-set (linguistic) out of which the operator's information environment and 'infosphere' are composed
- Structure, which is how the processes relate (the dependency network and 'value' network), how the representative structures relate (cognitive spaces), and the organizational structures or networks which the operator functions within (external to an organization, internal to an organization)

RECRUITING, TRAINING, RETENTION

While mostly applicable to organizations, these areas do also apply to individual operators (only they become 'internal' questions, where the operator self-selects certain behaviors).

Recruiting is identification of potential recruits (including criteria for selection), the argument made to obtain an individual's cooperation (or compulsion), and the 'initiation' or 'enrollment' phenomenon which inducts an individual into an organization.

Training provides skill-sets to individuals, as well as education and indoctrination into the relevant structures. Note that training of individuals in the organization sustains or expands capabilities for the decision-maker, as well as providing a 'metric' that provides the decision-maker with some trust that the tasked COAs can and will be accomplished.

Retention is keeping individuals inside or accessible to the organization. Experience is a critical factor in effective, high-tempo decision cycles, and so retention is an extremely important factor in assessment of potential future performance. Training is generally at odds with retention—while some skill-sets may not have 'free market' application and thus value, many in fact do. This leads to higher losses among the most highly-trained operators with skill-sets applicable outside the intelligence and military communities, the very operators that are most important to retain.

DISCIPLINE, COMMITMENT, LOYALTIES

Discipline is adherence to command authority—willingness to conform to the requirements of the structure and follow the orders from the chain-of-command, particularly under circumstances that may encourage less-than-rigorous behavior (such as being ordered to hold a position under heavy fire). Self-discipline is adherence to an internal standard of behavior or action, largely identified with sacrifices to comfort and 'normal' behavior in order to pursue priorities considered more important.

Commitment is what an operator is prepared to do in order to achieve certain objectives. Those objectives are generally considered loyalties, and they may be to abstractions (a deity, a concept such as liberty, etc.) or concrete things (a country, a religion, family, friends, etc.). The spectrum of commitment varies across cultures—some cultures consider the height of commitment to be self-sacrifice of survival (and the basis of heroism), while others put a greater value on living under pressures in order to enact change.

Intelligence and military operators have a considerable range of behaviors; high levels of discipline and commitment are considered the metric for professional forces that gain significant 'force multipliers,' while low levels of discipline and commitment lead to a collapse of organizations. These factors can also be disjointed or operationally-specific; many 'allies' have found that as situations shift, so do loyalties.

COMPOSITION, ELEMENTS

This is a decomposition of what makes up an operator or organization. In military terminology, this can be referred to as the 'order of battle,' which breaks out the various sorts of forces and their area of operations. An order of battle (OB) is decreasingly helpful in assessing and modeling operators as a primary approach. The levels of complexity, inter-operability, and inter-changeability of forces makes this a temporary (and in some cases, arbitrary) distinction. For example, a battlegroup assigned to an area of operations may not possess the relevant and necessary training and experience to function effectively in an AO, which is just not reflected in an OB.

For this reason, it makes much more sense to model the composition and elements of operators, and the associated decision cycle, with particular attention to the details of the 'core' cycle.

DISPOSITION, ATTITUDE

Disposition and attitude can be thought of as the structure of an operator with explicit emphasis on the 'orient-content-information' elements of the core cycle—how is the operator arrayed (relationships in space) and what is being paid attention to.

This is also a worthwhile place to note what is referred to as 'morale'—which can be thought of as a metric or representation of how the operators feel or are coping with their disposition and attitude, as well as their effectiveness (or lack thereof). Being 'out of place' or in an area of operations that is strange, for which an operator hasn't been trained and isn't in possession of the cognitive tools to cope well, and not being effective in operations, will quickly impact on the future ability of the operator to function. It's the addition of negative feedback into a cybernetic cycle—it rapidly moves to a 'runaway rundown.'

STRENGTH

This can be a simple metric—what is the number of effective operators, perhaps with the number of support personnel (generally reflected by number of support per different sorts of elements). Use of 'pure' metrics can be misleading—it assumes a certain judgment in the assessment of 'effective' operators as an abstraction, and can have little to do with overall performance under a well-operated decision cycle.

PLANNING, RESOURCEFULNESS, OPPORTUNITY EXPLOITATION

Assessment of an operator's planning ability is mapping out support functions (or how well an individual accomplishes the same necessary and complex tasks). Plans are composed out of comprehensive intelligence models, detailed scenario networks (including indicators; the scale and scope of scenario cascades, including detailed sequels and branches; the resolution/granularity of decision points; and array of options presented as potential courses of action), and meta-tempo support functions (particularly sustainment, but also assurance, and dependence such as synchronization). Building a comprehensive decision cycle and support infrastructure is also representative of a solid planning function.

Resourcefulness is, in many ways, the inverse of planning—how well does the operator handle the situation when their planning functions are inadequate, or when confronted with the new and novel?

Opportunity exploitation straddles the two positions—how flexible can an operator be in adjusting or shifting plans to pursue a scenario path not initially forecast, or that doesn't have a great deal of granularity on decision points?

EMBEDDEDNESS, IMPROVEMENT

Embeddedness is linked to structure and meta-tempo. An inability to improve, adapt, or alter a process or approach is to be embedded or inflexible and 'over-embedded.' Being totally detached from any particular process or approach is to be 'under-embedded.'

There are many aspects that an operator can be embedded regarding: region, mindset, social network, process, etc. Operators may only function in a specific, limited region or area of operations, and that is a form of embeddedness. An operator may view the world a certain way, and be incapable of changing that mindset; this is what Thomas Kuhn, in his Structure of Scientific Revolution discusses as a 'paradigm.' To

be structurally embedded, or limited in social networks, an operator has a limited range of human interactions; this can particularly occur because of linguistic issues, and is used to reinforce as well as limit group or organizational membership. Process embeddedness exhibits as “it always worked before” and “do what you’ve always done,” which may or may not be appropriate to the situation.

An embedded, particularly over-embedded and thus totally inflexible, operator loses the ability to evolve—improve, adapt, and over-come. Increasingly so, this is a world of ‘live-and-learn’ or you don’t live long.

META-TEMPO

While mentioned in associated and component points, let me again mention the essential nature of meta-tempo:

- Appropriateness—the tempo of tempo, the rate of change, making certain that the tempo fits the context
- Dependence—timing issues such as synchronization, which is essential because operators acting under command or cooperatively need to be aware of other operators; scenario networks generally also require an ‘order of operations,’ where certain objectives need to be accomplished before others can be attempted; dependence is also critical in a ‘dependency network’ and ‘value web’ sense, which is more specifically expressed as sustainment
- Sustainment—everything necessary, from intelligence to materiel, to maintain operations. More intensive operations or more chaotic contexts may increase the ‘burn rate’ of support, supply, and logistics. There are also concerns of near- and extended-lines, as well as interior and exterior lines; these are how well supply can be managed from the support infrastructure to the ‘front.’ Impact on sustainment is a crucial factor, from degraded support along exterior lines, to infrastructure attacks to deny sustainment. Infrastructure attacks on the decision cycle (such as communication or data networks) through information operations should be viewed as impacting on virtual sustainment, which cascades to ‘real’ sustainment
- Assurance—security issues are critical in every intelligence and military operation, and assurance is generally supported, inadequately, through secrecy measures

Intelligence is a critical factor in meta-tempo because it supports every aspect of the decision cycle. Counter-intelligence is the set of operations undertaken to prevent, degrade, or subvert (through deception campaigns) adversarial operators in their task of constructing comprehensive models of the operator or organization.

Communication, networking, and coordination are all critical ‘infrastructure’ functions supporting the decision cycle, and so also essential to consider as a factor in meta-tempo. The effects of a continually, completely connected world are contributing factors to why this improved approach to intelligence and conflict is essential. Assessment of the importance and priorities afforded to these functions by operators can provide an indicator to how well the operator may be prepared for future conflict.

PSYOP, PERCEPTION MANAGEMENT

PSYOP campaigns are operations undertaken to subvert the elements of an adversarial decision cycle—subvert the will of those involved or supporting the process, subvert or create deception measures

to degrade intelligence models in the cycle, impact on the judgment of the decision-maker, undermine the command authority of the decision-maker(s), etc.

Perception management, like counter-intelligence, is concerned with the models created and maintained by other operators, as well as the public, the media, etc. Operations in perception management are intended to subvert the assumptions, expectations, and interpretation of actions regarding the operator.

Understanding the next sections: the author uses a proprietary approach in building models and profiles of operators. The following points are what can be thought of as 'tensions'—a number of vectors that have 'poles' in opposition. Operators will fall somewhere along the spectrum represented on the vector, including heavy polarization by being at one of the extreme ends in approach. Individual vectors can be constructed into complex and interacting models of compounded vectors, and such models are greatly specific to an operator. The uniqueness of models has application in the inverse—when looking at the actions or events occurring without attribution to an operator, the models can suggest probable operators.

INTENTIONS: TENTATIVE/PERSISTENT

Some operator organizations, particularly command & control or hierarchical structures, are persistent in their intentions—they're in it for the 'long haul.' There are also operators that are cooperative, heterarchical, and exist more on a 'spot' basis—mission or constrained-goal oriented.

This is a scale and scope issue—tight focus and constraints only require a tentative set of intentions, while commitment to 'larger' issues requires a persistent decision cycle.

INTENTIONS: TASK/GOAL

Initiation in a cycle can be driven by a 'future-orientation'—the desire to achieve a goal, and transform the context or content until it matches the vision of the potential future. Other operators have a 'baseline' that, once certain thresholds of difference are achieved, they will initiate a set of decision cycles to 'restore.'

Understanding the 'goal' of an operator can be useful in mapping out much of their decision cycle, particularly their scenario network, decision points, and courses of action. Perception of the accepted baseline for an operator can help in understanding the trigger points of the operator, as well as the potential for managing operations under the threshold—either slowly changing the situation such that the operator doesn't notice, or making sufficient changes outside the sphere of attention (or concealed by deception operations) until it may be too late for the operator to effectively return to the original state.

WILL: SOFT/STRONG

An assessment of the level of commitment, and what those loyalties are to, can provide an understanding of the operational parameters of the operator, as well as what 'costs' they would be willing to incur. A soft will, particularly in political or command authority, undermines any operations potentially engaged in by their organization. Strong willed operators can make irrational commitments, including 'spoiler' strategies that can prolong conflicts indefinitely, or have catastrophic consequences (such as the Mutually Assured Destruction scenarios of nuclear warfare).

WILL: SLOW/RAPID

Some operators can rapidly or immediately form their will, at which point, there is little room for discussion or alteration of perceptions. Will can also take a great deal of time to form, which delays operations, keeps operational tempo fairly low and constrained, and may never solidify to the point where the operator is truly effective. The longer it takes an operator the form their will, the more potential to subvert it through PSYOP and perception management.

SCALE: MASSIVE/INDIVIDUAL

Size matters. Some operations just cannot be undertaken by operators without enough mass, economy of scale, or other essential resources. Some things are also negatively impacted by scale, such as cohesion, inter-operability, unity of force and approach, etc. Scale has many potential dimensions—strength in manpower, available resources and materiel to draw upon, computing resources to apply to a problem, available time for operations, etc.

SCOPE: TIGHT/DIVERSE

Diversity is important—diversity of forces, diversity of approaches, diversity of viewpoints, etc. There are drawbacks to diversity, however—specialization can be more effective, a tighter focus is easier to maintain, information overload is distinctly probable, etc. Tight scope can be just as problematic—specialization comes at the cost of flexibility, it can ‘fall out of step’ and no longer be current with the ‘now,’ understanding of a complex world is much harder to achieve, etc. This is a difficult tension to balance well, and it is generally accomplished using ‘value webs’ or dependency networks—specialized groups provide their ‘value add’ and pass along their output product to the rest of the web/network. Such an arrangement can be specifically targeted, and failures of critical dependencies can cause cascading failures throughout the web/network.

THINKING: LINEAR/COMPLEX

Operators and organizations can, particularly if specialized, only handle one thing or one sort of thing at a time, and are very linear. Others will be very complex, capable of multi-tasking, and handling a wide variety of decision cycles simultaneously. Much like the scope issue, there are times when one approach is more appropriate than another, and prioritization and ‘load balancing’ or trade-offs among decision cycles can be problematic.

INITIATIVE: EMBEDDED/AUTONOMOUS

The ability for completely independent action can have a dramatic effect on operations tempo, and provide considerable competitive advantage. Embeddedness in an organization, or any other sort of embeddedness, will have dramatic negative effect on operations tempo, the decision cycle, and survival of the operator. Hierarchical organizations are particularly troublesome in this fashion, where an operator may have to decide between ‘asking permission or asking forgiveness.’

OPERATIONS: SERIAL/PARALLEL

While complex thinking requires operation of multiple simultaneous decision cycles, the ability to initiate and manage more than one, particularly simultaneous and dependent operations, is a separate

matter. Parallel operations require complex thinking, but complex thinking does not imply the capability to handle parallel operations.

OPERATIONS: EFFICIENT/EFFECTIVE

This vector is complex, involving an operational emphasis from productivity, through efficiency, to effectiveness. Productivity is purely activity-based, sort of a “don’t just sit there, do something” approach. Efficiency is activity with some metrics, units against time; efficiency is a measure of the ‘fitness’ between components of a structure or process (the greater the mismatch, the higher the ‘friction’). Effectiveness is appropriateness, fitness (which is appropriateness over time, also known as ‘persistence’) between the structure/process (content) and the context. The differences can be explained by using a group of monkeys on typewriters, turning out reams upon reams of paper (productivity); a group of monkeys being monitored by a monkey with a stopwatch, with how many keystrokes they manage in a unit of time (efficiency); and finally, a monkey holding up a single sheet of paper with ‘ $E=mc^2$ ’ written on it (effectiveness). Most intelligence and military organizations confuse productivity and efficiency with effectiveness, because effectiveness is difficult to apply a metric to.

OPERATIONS: REFLEXIVE/REFLECTIVE

Just as with a biological reflex, some operators function with unthinking actions, just to be doing something. Other operators will be deliberate and consider their options (literally a comprehensive review of the available scenario network) prior to undertaking actions. One of the benefits of extensive simulation is to reach a comfortable middle-point—engage in the necessary cognitive process (reflection) during simulations, when the consequences aren’t real, until the ‘right thing to do’ becomes the reflexive action. This approach has been very successful in automated simulation systems training for complex tasks such as being a fighter pilot, but more ‘cognitive’ simulations have yet to approach to level of realism and variety necessary.

OPERATIONS: PLANNED/EMERGENT

Operators, particularly goal-driven ones, may be conducting actions based on their planning abilities; such plans may be appropriate and effective, or not. Other operators rely upon resourcefulness and capabilities to manage complexity ‘under fire,’ and try to manage situations as they emerge; this approach is particularly favored by politicians and the politically-oriented, for whatever personality and character reasons.

OPTEMPO: LOW/HIGH

Operations tempo, when viewed from a meta-tempo (tempo of tempo) perspective, may be set inappropriately, either too low (and thus not truly responsive to the context and content, and ineffective) or too high (and thus burning resources and straining the operators and support network necessary for sustainment). Value judgments in the trade-offs are essential to assess here—the more ‘wealthy’ operators (those, literally, with resources to burn) may choose to operate at inappropriately high and expensive optempo in order to gain a rapid conclusion or less ‘lethal’ conflict.

GAME PERSPECTIVE: SHORT/LONG

Decision cycles can ‘nest’ within decision cycles. In a ‘game’ perspective, the turns taken by players are a complete cycle, while the game itself is viewable as a ‘thread’ of cycles or a larger cycle. Intelligence and military decision cycles can have very long and extended meta-cycles (the cycle of cycles, wherein various

decision cycles are operating), while other players cannot sustain a 'long game' perspective (particularly because of continually shifting political structures, where political authority sets the intent and missions for the intelligence community and military organizations).

Long-game operators can have distinct advantages over short-game operators, simply because short-game operators will lack the necessary perspective, and ability to sustain their own direct actions and counter-operations.

CONTEXT: DEPENDENT/INDEPENDENT

Embeddedness of various sorts—regional, social network, mindset, process—limit the operator's area of operations, as represented in the decision cycle, their context. Mapping out areas and degrees of embeddedness can provide advantage by conducting operations outside an opposition's context, but that affects the dependencies and value web of the opponent. This fact is one of the reasons why the global players are expanding their areas of operations and spheres of influence—complexity and inter-connectedness make them vulnerable, and this necessitates the more comprehensive view of the world.

CONSTRAINTS: RIGID/FREE

One pole of this vector is represented in the mindset "by any means necessary"—a willingness to do anything at all to accomplish the desired intent. Close, but still recognizing constraints, is the position of "the end justifies the means," which recognizes certain constraints, as well as moral and ethical factors than may limit operations. Rigid constraints are represented in operators with set doctrine, limiting rules of engagement, concerns about human rights, an unwillingness to suffer casualties in their own organization, etc. History presents a number of examples when "by any means necessary" was a position that led to an operator successfully achieving objectives, but the situation then required on-going ruthlessness to maintain what was achieved.

OFFENSE: MASS/SURGICAL

Operators that are uncertain of themselves, have unreliable intelligence, or desire a 'swift and painless' conflict will rely more upon mass—overwhelming use of force and materiel—as the deciding factor in a conflict. The 'surgical' approach requires a much more professional decision cycle—solid and reliable intelligence; accurate models of the opponent; decision-makers with insight; and an operational capability that either has the best in technology or special operations forces (SOF), preferably both. While not in direct correlation as a general rule, reliance upon mass can be seen as an indicator of weakness in an operator—will, commitment, intelligence support, judgment, and/or capabilities.

OFFENSE: CLUELESS/SOPHISTICATED

The decision cycle is a 'cognitive machine'—a way of taking data and energy and making effective change in the world. As with most machines, it is only as good as the people that built it, operate it, and direct it. One of the critical flaws in Marxist theory was that 'work' or effort was automatically seen as the equivalent of 'value add,' or improvement to whatever was acted upon. This is clearly false, and the more complicated or sophisticated the machinery, the greater the requirements upon those involved. Decision-makers that are unprepared to utilize the complex machinery of the decision cycle will only be enabled to reach catastrophe more rapidly—the 'clueless' use. The more capable the decision-maker is without the leverage provided by the machinery of the decision cycle, the more effective they will be as a sophisticated user.

RESOURCEFULNESS: LOW/HIGH

While those involved in the decision cycle will be attempting to create comprehensive models for the scenario networks, it is impossible to adequately anticipate the real, complex world. Conflict in particular is the most extreme of emergent systems, with interactions unseen under 'normal' circumstances, and Darwinian pressures of evolution (where fitness is appropriateness and effectiveness over time—and since a battlesphere isn't a stable context, this implies considerable abilities to cope, manage, and thrive on chaotic change) rampant. The ability to continue effective functionality—lacking intelligence, planning, support, etc.—is an indicator of an operator with considerable resourcefulness. Operators with detailed and comprehensive support but low resourcefulness will be challenged by rapid change and chaos, resulting in decreased probability of survival.

TOOLS: SCRIPTED/ORIGINAL

The cost of entry into the emerging domain of integrated intelligence and conflict is such that it is easy to do poorly, and difficult to do well. Most operators looking to bootstrap their efforts or remain current—since hierarchical, bureaucratic organizations have significant problems keeping pace with high-tempo domains, and aren't innovative in this field—are relying upon 'scripted' or automated toolsets developed by others. Similar to the 'open source' software movement, the various aspects of the computer underground and hacker communities, as well as other operators in this domain, will provide a wide variety of tools that automate attacks, exploits, and take advantage of vulnerabilities. Reliance upon scripted tools again fosters a dogmatic approach in operators' means and methods. Entirely original and sophisticated attacks have been a competitive advantage of a small set of operators, but the more interesting trend is for operators to use scripted tools with original or novel tradecraft.

ORGANIZATION: DISCRETE/CONTINUOUS

Operator organizations can be 'discrete,' functioning as mostly or entirely independent elements with defined areas of authority and accountability. This approach leads to little cooperation generally, and can even lead to competition (but not the sort of competition that leads to improvement; rather, the sort that leads to nothing being accomplished at all), and certainly impacts on inter-operability inside the structure. Continuous, well-integrated organizations function much more effectively, but need to be diligent about security and assurance issues to prevent cascading failures because of subversion or denial.

ORGANIZATION: HIERARCHY/HETERARCHY

Hierarchical organizations are those that define authority by structural position ('top down'), and by the dependency of subordinate nodes (the 'top' maintains control of information, control of decision-making, etc.). Hierarchies are the classic 'tree' network, the 'cell' structures used by opposition forces. Heterarchical structures are non-linear, potentially non-local; from a network analysis perspective, nodes in a heterarchy can all be considered co-incident. Heterarchies confer authority by knowledge and function. 'Many-to-many' network models, typified by the virtual communities of the Internet, are examples of heterarchical organizations.

ORGANIZATION: CENTRALIZED/DECENTRALIZED

Regardless of authority and responsibility structures—hierarchies and heterarchies—an organization can be independently located spatially. Hierarchies have historically tended to be centralized—power coalesces—but the fact that centralized command authority can be a 'single point of failure,' a great deal

of effort has been taken by some hierarchies to decentralize command & control. Heterarchies tend to inherently be decentralized, but some aspects of heterarchies may in fact centralize—markets, for example, will centralize exchanges in order to gain certain economies of scale.

ORGANIZATION: STRUCTURE/FITNESS

Organizations can act similarly to organic organisms and act conservatively, with self-interest and self-protection as an overriding concern. Confronted by certain sorts of options, these sorts of organizations will favor continuity of structure over the sorts of changes that would improve appropriateness and 'fitness' to the evolving context. Other operators will select fitness over continuity, even though this can cause considerable internal disruption. This aspect in organizations can also lead to schizmogenesis—one set of elements of the operator selecting continuity, while another set of elements will 'break off' to form another operator that has selected the 'new' ways as its initial conditions.

ORGANIZATION: FORMAL/INFORMAL

The structure of an organization may be formal—a charter, mandate, order, contract, etc. that dictates the specifics of function, particularly with respect to authority and responsibilities. 'Organic' organizations, which start as an individual or cadre and 'grow' as an emergent process, are generally informal up until a threshold, when formalized structure will either be imposed or rejected. Informal structures may have growth advantages, but higher potential for friction over authority and responsibility boundaries. Formal structures tend to accrue further formalization to the point of structural over-embeddedness, with the accompanying drawbacks in tempo and survivability.

PROCESSES: HEAVY/LIGHT THREADING

Process and systems analysis can focus on the entities and processes (such as the decision cycle represents) or that which the entities and processes function upon. If a system is viewed from the perspective of the content being processed, it would be progressively transformed by a sequence of entities and processes, and that progressive sequence can be viewed as a 'thread.' Heavy-threaded cycles are highly structured as to the 'flow' of the content, and that structure is rarely altered. This affects the decision cycle in terms of meta-tempo—prioritization, dedication to certain threads over others, etc. Lightly-threaded models are more flexibly structured, and can 'float' the associated requirements of threads fluidly—multi-tasking, different queuing, etc.

INTERACTION: FRICTION/SMOOTH

Inter-operability of the elements of the decision cycle is crucial in enabling high-tempo when appropriate. Independent operators have the advantage of unified elements of the decision cycle, while organizations have to worry about 'friction' or resistance to cooperative/coordinated processing throughout the cycle. Smooth interaction is an indicator of a well-integrated and cohesive operator. The reasons for smooth interaction are worth modeling—unified support systems and language, homogeneity of culture, etc. can also indicate exploitable flaws such as a lack of diversity or a potential for reflexive operations.

COMMUNITY: COMPETITIVE/COOPERATIVE

Many operators are actually only responsible for a sub-set of elements in the decision cycle; this makes them part of a 'community' acting like an integrated structure or economy. Unlike in a market economy, where competition can be the impetus to continually improve, competition in these sorts of communities

leads to increased friction, arguments over responsibilities ('jurisdiction'), and generally ineffective provision of services. Cooperative communities are either tightly integrated and under unified command or coordination, or have very little overlap in service provision (in other words, competition is avoided by forced specialization). Redundancy of services to the decision cycle, with a 'market competition' mechanism that lets the decision-maker benefit from a wealth of models, is the ultimate goal of many competitive community organizations, but has yet to be truly achieved.

COHESION: STRONG / WEAK TIES

The level of 'connection' between individuals in an organization or community can be high, with people being emotionally and socially 'close' to one another, and these are 'strong' ties. Individuals can also be 'distant' from one another, and these are 'weak' ties. Strong ties in organizations and communities can lead to much higher cohesion. Strong ties, however, also translates to low 'novelty' (differences in data-information-knowledge-wisdom sets, referred to as meta-information, or any difference that makes a difference in the difference that makes a difference) and a homogeneous culture. Weak ties, while potentially suffering in cohesion, have diversity as an advantage, and higher levels of novelty to draw upon operationally.

FLEXIBILITY: STATIC / DYNAMIC

Many aspects of the decision cycle, and the cycle itself, can be viewed as 'static'—unchanging, and perhaps unchangeable. This is being mindset and process embedded—loss of flexibility in how the world is viewed, and how attempts are made at transformation of context and content. Being and remaining 'fluid' or dynamic requires additional effort, but generally pays off. It's important to make a distinction, however, in self-transformation—just because something is 'old' doesn't mean that it is 'wrong' or 'bad'; just because something is 'new' doesn't mean that it is 'right' or 'better.' One key to appropriateness is using the right tool for the right job; the decision cycle is a 'meta-tool' that provides an abstraction in management of the overall process, and supports any effective tool, old or new, within a dynamic framework.

RISK MANAGEMENT: SHIFTING / SHARING

Risk can be viewed as negative opportunity or consequence; how risk is managed by an operator is critical—every action entails risk, and not engaging in risk management means exposure to every negative opportunity or consequence. Risk can be shifted onto others, making them responsible (accountable); risk can be shared, particularly into risk pools, making all participants partially responsible (but factoring of the potential risk consequences may be more manageable as a collective).

As an indicator of planning, models of risk management of operators can be crucial. It is also critical for any operator to maintain current risk models (and threat models, which combine potential adversaries with potential vulnerabilities); when risk models 'fall out of step' with the actual risk complexities, risk exposure occurs.

KNOWLEDGEBASE: SCARCE / PORTABLE

Operators, particularly organizations, have internal knowledgebases—data, information, knowledge, and wisdom—as part of the core of the decision cycle. Such knowledgebases may be scarce or non-portable—for example, they may be human-centric and thus require extensive training to 'transmit' from one operator to another. Other knowledgebases may be 'digitally' represented in a transmissible format that can encapsulate the portable knowledgebase and provide for improvement throughout an organization.

It's worth noting that "some things can be taught, while others have to be learned." Even with transmissible knowledgebases, the newly educated are lacking in practical application and experience. This can lead to the 'aha!' factor—many aspects of portable knowledgebases defy adequate symbolic representation (particularly subjective or abstract elements), and will only make sense when the same or similar situation as described in the 'courseware' is encountered by the operator in the real world.

INTELLIGENCE: MINIMAL/DETAILED

Intelligence, as with any 'knowledge-intensive' field, will vary in degree of detail and accuracy dependent upon the desired area of interest and the capabilities developed and available regarding that domain. There are distinct process differences in operators, however. One sort will deliver nothing or little 'now' and try to provide 'everything' later; this may not be of much use to a decision-maker that requires models as the basis for an immediate judgment. Another approach is to provide 'rapid prototype' intelligence models to the consumer, and to continue assembling detail and checking accuracy over iterative cycles. This meets the consumer's immediate needs as a decision-maker, supports the on-going requirements, and also allows for feedback from the decision-maker as to prioritization of what aspects of the intelligence models would support the decision process most.

APPROACH: CAPABILITIES/INTENTIONS

Many operators, particularly the more technologically-adept, have concentrated on 'capabilities'—sensors, satellites, etc. that provide 'objective' or metric-based intelligence. Other operators have focused on 'intentions'—what are others thinking, feeling, and likely to do? Capabilities-based intelligence can help count the tools and materiel, but doesn't express what is in minds and hearts of men—the initiation, function, and conclusion of the decision cycle. Intentions-based intelligence is much harder to develop, is uncertain, and doesn't create the volume of 'production' that capabilities-based intelligence does. Both are essential sorts of intelligence, but operators are very polarized one way or the other.

SUPPORT/LINES: EXTERIOR/INTERIOR

Critical for operations and sustainment, exterior or extended lines can be difficult to supply, while interior lines can be directly supported. The larger the area of operations for an operator, the more complex the support issue; if any area can be one in which operations occur or conflict may be an issue, planning and provisions will need to occur well in advance. This leads to sunk and opportunity costs, as well as the losing game of trying to be everywhere at once and being all things to all people. Strong interior lines can mean superior sustainment, but limits the area of operations considerably; this may translate to regional strength, with reduced areas of interest.

'Virtual' lines are a very different issue. The increased connectivity of the world, and availability of communication and computational resources and assets makes this less of an issue. Additionally, 'virtual' operations can be launched from any point to any point (non-local conflict), so proper pre-planning can provide the equivalent of completely interior lines.

EXECUTION: POOR/EFFECTIVE

Metrics on execution are largely an issue of analysis and judgment. Many operators, more so with politically-controlled operators, will 'define down' objectives of the decision cycle in order to claim effectiveness and success.

One factor that leads to more effective execution is 'clustered combatants.' Some operators will be in opposition to each other, and initially both may have very poor execution. Two things may occur: one

combatant continually improves while the other does not, and the 'static' operator will eventually lose (or shift emphasis in operations in order to compensate, to their increased cost); both (or more if it's a complex cluster) will continually improve and 'trade' positions as to which is most effective in execution (no 'knock out' blows, but an increasingly complex conflict). As with most things, but integrated intelligence and conflict, particularly IWAR, UW, and IO, most of all, assessments are very time-dependent and can be subject to rapid change and revision.

Understanding the next sections: The following sections briefly explain the 'check-lists' used by the author to rapidly assess operators in different areas.

SPECTRUM OF OPERATIONS & VULNERABILITIES

As discussed previously, the 'spectrum' of operational capabilities, and what an operator may themselves be vulnerable to is:

- Destroy is outright elimination, if possible
- Deny impacts on capabilities by removing options
- Disrupt is chaos, confusion, or other difficulty in the cycle
- Degrade is slowing down or reduction in effectiveness of the cycle or of capabilities
- Deplete impacts on support, necessary capabilities, limited attention
- Distract is misdirection as well as media events that shift attention priorities
- Deceive is providing false or faked detail to elements of the cycle
- Subvert undermines will, priorities, judgment, command authority, or other elements necessary to be effective

OPERATIONS & VULNERABILITIES

These are various process elements in the decision cycle or associated support and infrastructural elements that can be the target of operations or vulnerabilities:

- Reliability-Availability-Serviceability (RAS)—meta-tempo issues regarding the decision cycle. Is the cycle reliable, will it continue to function, and will corrections be possible?
- Access—particularly a technology system issue, access can be 'penetrated' (providing intelligence to potential opposition) or denied (thus leaving the decision-maker unsupported)
- Integrity—trust factors are complex. What is sourcing, what is the accuracy of the models, have alterations been made, is active deception a possibility?
- Communication/Coordination—essential to every aspect of the decision cycle, communication and coordination are vulnerable to the entire spectrum

- Visibility—any point that media focus can be focused on or is already a point of concentrated attention is at increased risk, essentially as a ‘message relay’ point as part of PSYOP or a hacktivist campaign
- Governance/Civil Position—subversion or destruction of the ‘opposing’ social contract is essential to any opposition’s operations. Such elements can also be used to further an operator’s intention through social or technical means
- Competitive Advantage—portable knowledgebases can be portable to the opposition as well (espionage)
- Infrastructure/Infostructure—any element of physical or virtual support networks can be vulnerable to the spectrum. Any impact on the provided economy of scale will have an effect on the target
- Financial—financial warfare, the obvious being economic sanctions, but also manipulation and the elements of the spectrum can be applied

PROXIMITY/DEPENDENCY NETWORK CASCADES

Operations and vulnerabilities can be broken across two approaches: penetration and denial.

Penetration can be ‘deep,’ which leaves the target vulnerable to great degrees of subversion in their decision cycle; penetration can also be ‘shallow’ or ‘casual,’ which is far more common, with the intention of distraction, or if the target has visibility, for PSYOP purposes.

Denial can be direct, with operations focusing specifically on just the target. Denial attacks can also be of the ‘cascade’ variety, where the real target of the attack is ‘down’ or subsidiary in the dependency network or value web. Cascade attacks, because they ‘branch out’ and cause cascading failures from the target onward through the subsidiary points, are much harder to identify the ‘real’ target of (since so many targets suffer loss).

INTELLIGENCE INTENTION/CAPABILITY

As discussed previously, intelligence models can be used for the ‘4Ms’: monitoring, measuring, managing, and mitigating.

Monitoring is continual collection and gathering to be informed, construct on-going models, and look for indicators.

Measuring is an analytical function, some of it ‘metric-based’ or actual measurement (how many of these, the magnitude of those), while other ‘measurement’ is ‘fuzzy’ (intentions, profiles, probabilities, etc.).

Managing is an interaction between internal decision cycles for an operator and the external world. Internally this is the overall functionality of the cycle (‘information management’), but also initiation points for decision cycles—is there a goal to accomplish, is the world shifting in some way outside the ‘tolerances’ established by the decision-makers?

Mitigating is the transformational process—in particular, ‘crisis management’ or otherwise handling events of the world in such a way that the operator survives and thrives.

BOYD MATRIX

The Boyd Matrix, utilization of the core elements of the decision cycle to understand targeting in operations, as well as to assess an operator's vulnerabilities (or internal vulnerabilities), has been discussed previously. Note that extremely complex models can be built by mapping the Boyd Matrix against the operational spectrum, and these can be extremely useful in building operational scenario networks.

THREATS

A consideration of the abstract threat categories is also helpful, in order to 'turn the problem around' and consider it from this direction rather than operations and vulnerabilities:

- Theft— theft can be physical (such as the risk posed by 'insiders' or through 'dumpster diving' (going through the garbage of a target)) or virtual (hacking, industrial espionage, or competitive intelligence targeting knowledgebases)
- Denial— attacks can be physical (sabotage) or virtual (system attacks, such as 'denial of service' or 'distributed denial of service' network attacks; or cryptographic attacks, that turn the security and protection measures of communication networks against the users)
- Signal— signal intelligence (SIGINT) can come from a variety of sources (surveillance, collection technology, covert channels, TEMPEST intercepts, taps, bugs, traffic sniffers on networks), and signals can be denied (jammed, overwhelmed, packet flooded, etc.)
- Social— pre-texting and other techniques of 'social engineering' are difficult threats to address, as well as targeting of weak links (blackmail) or insiders
- Subversion— for both physical and virtual knowledgebases, alteration and manipulation can be serious threats, particularly because authentication is not integral, and subversion occurs prior to some knowledgebase being essential or below the threshold of detection
- PSYOP— propaganda subverts the judgment and valuation criteria, and thus impacts on the decision cycle; attacks on will or command authority also undermine critical dependencies in the decision cycle. Externally, reputation can be attacked, which can seriously impact on perception and valuation of targets in dependency, value, and social networks
- Political Warfare— social aspects, such as hacktivism, protests, disturbances, or rioting can affect the political, and thus intelligence and military decision cycles. Guerrilla warfare and terrorism (including 'no retreat' scenarios where the operator has no clear means of extraction from the situation, and 'no contact' scenarios where the operator uses indirect methods of attack) have more direct intelligence and military implications, and are more complicated to prevent or counter, because of the social system involvement and implications (particularly in contexts where political control explicitly limits the actions of intelligence and military decision-makers regarding the supporting social system)

RISKS

While 'threats' are more active (vulnerability + opportunity + operator + capability + intentions = threat), risks are more simply thought of as exposures. For example, risks can be spatial or domain-based:

- Regional—various geographic locations have accompanying risks (and the ‘resolution’ of spatial location is important; resolution shifting is assumption shifting, from the abstract (higher level) categories down to the more specific (lower level)). The Middle East as a region has associated risks, with specific countries having different (and some a large number more) risks, and so on to cities, and even one street to the next. Risk exposures, however, can be categorized at the more abstract level: Middle East, Asia, Former Soviet Republics, Europe, Central America, South America, North America, Transnational, etc.
- High Risk—some domains are much greater in risk-levels, but different sorts of risk. As a pure metric (considerable risks associated with the domain), there are the sectors of manufacturing (petrochemical, pharmaceutical, technology, biotech among the highest risk), finance (banking, brokerage, trading with the greatest exposures), transportation (air, rail, shipping, mass transit with different sorts of risk, but generally catastrophic or ‘media hot’), utilities (infrastructure support systems such as power/fuel generation/transportation/storage, water supply), food (production, distribution), entertainment (media, parks, and resorts are ‘soft’ targets with ‘media hot’ potential), communications (satellite, ground, cellular, Internet, because of the ‘ease’ of disruption and denial, and the cascade effect), and defense (weapons, force projection, WMD; these, however, are the direct ‘hard’ targets)
- Medium Risk—domains in the medium risk category are either ‘harder’ to target or considered ‘off limits’ for operators (the support consequences make such operations counter-productive). These areas include healthcare (hospitals, clinics; these are, however, targets for specific sorts of operators), emergency services (police, fire, ambulance; social services are generally ‘off limits,’ but representatives of target governments or symbols of Nation-State power (such as police) are considered by some to be valid targets), international and government agencies (governance, offices, Embassies, personnel; these are supposed to be ‘hard’ targets, but the opportunistic operator can select soft and vulnerable targets—it’s an example of being over-extended, that it’s difficult to harden every potential all of the time)

CONCLUSIONS

I hope this has provided a satisfactory 'primer' level of an adoptable ontology. While highly simplified and abstracted, context- or operation-specific systems can be generated from the materials presented.

Integrated intelligence and conflict, as I've been practicing it for two decades, is no simple thing to attempt to understand fully, even in such a streamlined and minimalist form. What I've discussed herein is based on what I've found essential and effective, and I hope that is appreciated by the reader.

Questions, comments, and discussion are always welcome.

Michael Wilson
Managing Partner, 7Pillars Partners
partners@7pillars.com
<http://www.7pillars.com/>

[Principal, Decision Support Systems, Inc.
wilson@metatempo.com
<http://www.metatempo.com/>
31December, 2001]