A COGNITIVE CYBERWAR

The Mind is the Next Frontier to Protect and Defend
& it is Already under Attack from our Adversaries

MultiPlex|studio

Jason L. Lind

Coalition Lead

+1 414.788.2820

lind@multiplex.studio

Mitchell Maddox

Command Lead

+1 757.951.3842

maddox@multiplex.studio

Response to RFI-WHS-20-CYBERST:

Cyber Science and Technology (S&T) Roadmap

ABSTRACT

In our view Cyber is a dimension of a reality (along with Space, Time & Thought) which we will reference that gives rise to traditional, and non-traditional, warfighting domains on a non-discrete continuum. Cognitive Warfare primarily occurs across the Cyber and Thought dimensions and related domain facets.

In this document we will address the following concepts:

1. Propose an extension to the OSI Model and a Zero Trust variant 'Abstract' (ZT4)
2. High-level draft of Secure Cognitive Architecture (SCA)
3. Introduce the Lindian Model Theory/ 12-dimensional Meta-Prism
4. Define C6M – Command, Control, Coalition, Communications, Ops, Coordination: Manifest – and bind to SCA
5. Provide a strategy to Educate civilian and military populations of not only US and her allies but, with the goal of winning hearts and minds, adversaries as well
6. Brainstorm ideas on how to Stabilize the Political situation at home and abroad without violating US Law or Treaties

MultiPlex.studio is a defense oriented independent think-tank and development organization with a focus on advancing a "beyond the bits and bytes" vision of the future.

WHAT IS COGNITIVE WARFARE?

Cognitive Warfare, for our purposes, is simply next-order Cyberwarfare, or "beyond the bits and bytes". Social Engineering would be another synonym. Classical Game Theory is ultimately about making decisions – given rules and utility curves (and their associated payoff functions) who does what? Social Engineering on the other hand could be described as an applied branch of Game Theory where the rules and utility curves are altered – either in reality or just in meta – to adjust opponents play in reality. Bottom line CQW (Cognitive Warfare) is about bending information to the will of the beholder in order to manipulate the perceptions of our adversaries. It should be noted this cannot be done in a silo – that is employing this tactic will have blowback on the aggressor's population which must be accounted for.

POLI-ECONOMIC STRATEGY

While placing pressure on our adversaries' economies may at first glance sound... well sound – it is probably not. Macroeconomics is not a zero-sum game – that is the advantageous equilibrii to the actor can be met with equally, or more so, advantageous equilibrii to the opponent: the converse, for example the classic tariff war example, being equally (and devastatingly) true. The negative, and positive, externalities of economic attacks cannot be discounted.
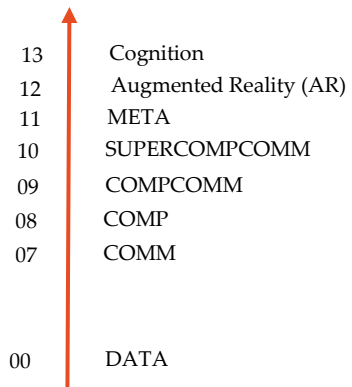
Politics, while ostensibly a zero-sum game, in my view is much more opened ended – as the last 4 years have proven. The level of CQW happening in US Politics is only escalating and the result is lower and lower approval ratings for both sides. This of course has been exasperated by outside influences, namely: Russia, China, Iran, North Korea and ISIS – but probably also our Allies as well. Recently the German Minster of Defense was blasting Trump on Twitter.

EXPONENTIAL GDP GROWTH WITH STABILIZATION AND DEPOLARIZATION OF ALLIED POLITICS

If there exists such a way to crash an enemy economy through financial directed CQW (and we know that there does) there should be a way to invert it and turn it into an avenue for advancement. At the same time if we harness our cyber weapons to fix our own problems instead of causing others perhaps both will work in concert to manifest The New Golden Age.

OSI EXTENDED MODEL

The OSI Model is generally represented as a layer cake diagram with layer 7 being "network" and 8 "application". We are going to slightly redefine this relationship yet keep the standard dimensional structure at this level of abstraction.

13	Cognition
12	Augmented Reality (AR)
11	META
10	SUPERCOMPCOMM
09	COMPCOMM
08	COMP
07	COMM
00	DATA

Layer #	Layer Name	Description
13	Cognition	A layer that can Observe-Orient-Decide-Act (OODA)
12	Augmented Reality (AR)	Devices that bridge the cognitive, directly or indirectly, to the network
11	META	Higher order logic bindings between the physical network and the "mind"
10	SUPERCOMCOMM	Architecture realizations that distributes computing, storage, control and networking closer to both the users and the data
09	COMPCOMM	More than just COMP+COMM L9 there are implied information enhancements and transformations at this layer to enable easier computation and broader communications
08	COMP	Traditionally the Application Layer, COMPUTE is responsible for not only application logic but abstract processing power
07	COMM	Traditionally the Network Layer, COMMUNICATIONS is responsible for not only TCP/IP level protocols but also the concept of communication
00	DATA	The "bits and bytes" flowing through the System.

OBSERVE-ORIENT-DECIDE-ACT LOOP ARCHITECTURE

Observe-Orient-Decide-Act (OODA) was introduced by Colonel John Boyd, USAF in the 1950's to help train fighter pilots and has since been extended to a wide array of strategic scenarios encompassing both individual and collective decision making. Like Sun Tzu's "Art of War" the OODA Loop seems to be a concept that will stand the test of time itself.

We will demonstrate, in metaphysics using Lindian Model Theory, that OODA is a natural construct that, while can and will be extended, is not going anywhere. Specifically we will introduce the concept of Model and Test for $OO\mu D\tau A$.

Observe: build a comprehensive picture of the situation with as much accuracy as possible.

Orient: find mismatches: errors in your previous judgement or in the judgement of others. Generally bad news is the best kind provided you catch it in time, as you can turn it to your advantage.

Decide: having gathered information and oriented ourselves, we must make an informed decision. The previous two steps should have generated a plethora of idea, so this is the point where we choose the most relevant option.

Act: execute the decision and then **Observe** the results.
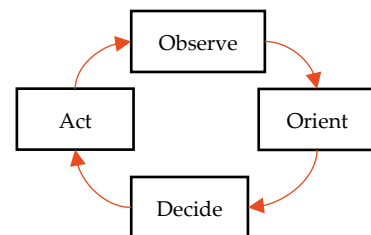
ZERO TRUST ABSTRACT MODEL (ZT4)

Zero Trust Architecture (ZTA) was coined in 2009 by John Kindervig and at its core is about shrinking the verification perimeter as close to the data as possible manifesting a "protect surface" that can be continuously monitored for threats. ("Zero Trust Architecture Overview & Innovations" [Lind 2020]) Dr. Chase Cunningham later authored Zero Trust eXtended (ZTX) which creates a simultaneously more robust and abstract implementation of ZTA.

IX	INTELLIGENT ACTOR
VIII	DEVICES
VII	ARCHITECTURE
VI	DISTRIBUTED
V	WORKLOAD
IV	MONITOR
III	Automation & Orchestration
II	NETWORK
I	DATA

ZT4 is in a similar vein in that it describes a vertical ZT structure heavily influenced by ZTX and then we then will map to a structure that combines the OSI-Extended and ZT4.
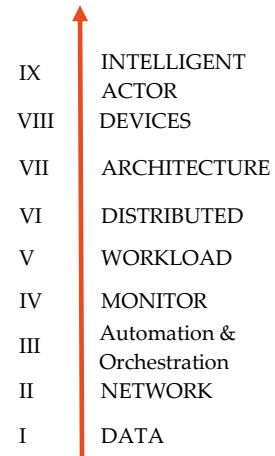
Zone	Name	Description	Zone	Name	Description
IX	INTELLEGENT ACTOR	Human, Machine, Alien?, Force of Nature? OSIE13+	IV	MONITOR	OSIE8+ entities that watch E7+
VIII	DEVICES	Any hardware capable of accessing the network (OSIE12)	III	Automation & Orchestration	OSIE8+ entities that provide tools and processes for IX/E11 to interact with.
VII	ARCHITECTURE	The conceptual design of the systems, is not static and more than just reactive (roughly OSIE11)	II	NETWORK	OSIE7-
VI	DISTRIBUTED	Seventh layer is transcendental, each distributed system is potentially representative all the up to layer Nine. (roughly OSIE10)	I	DATA	OSIE00
V	WORKLOAD	The conceptual and computational throughput of a process (OSIE-9+)			

| ZTA Inflection Point Binding	Character Priority	Description
Policy Enforcement Agent (PEA)	A	A PEA binds a Policy to a Policy Enforcement Point (Data Plane) and Policy Admin (Control Plane)
Monitor	α	The ZT4 Monitor component watches the PEA and Network
Policy	B	A human+machine readable living document defining the security policies of the enterprise. Blockchain/eventual-consistency-databases can be used here
Policy Admin (PA)	β	Responsible for binding the PEP through the PEA
Identity Presence	Γ	Device(s) that establish the presence and uniqueness of an Intelligent Actor, is doubly bound to the PEP.
Policy Enforcement Point (PEP)	γ	Gatekeeper for dataset(s)

From lowest level of abstraction to highest the Greek characters have an implied relationship with the capitals at a higher level of abstract than their associated lower cases

SECURE COGNITIVE ARCHITECTURE (SCA)

SCA combines the concepts of our OSI-Extension (OSI-E) with Zero-Trust Abstraction (ZT4) and classical ZTA components to achieve a conceptual design of a mixed reality platform that simultaneously is secure and has an offensive footing. Additionally key to this design is the concept of "Presence of Identity Assertion" where unique factors are combined to assure that the Intelligent Actor is who they claim to be – in fact our system must not rely on claims.

In our model a Hardware Unique Factor (HUF) is combined with a Secure Execution Environment – today in a USB-C form factor – to instantiate a communication channel through the SCA network.

Policy Admins (PA) in layers higher than 8 are a combination of hardware, software and cognition.
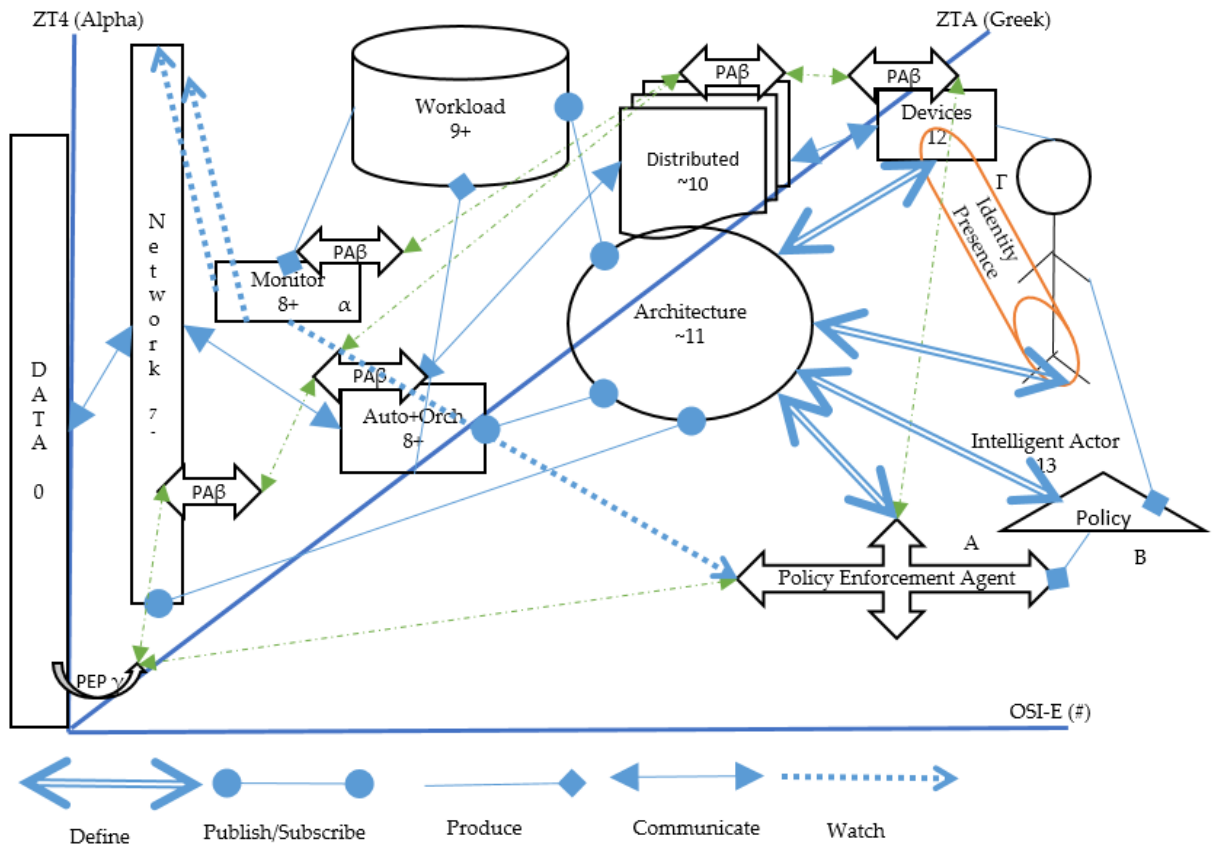
LINDIAN MODEL THEORY – A QUICK INTRODUCTION

LINDIAN DIFFERENTIAL SET THEORY

As far as I am aware my concept of differential set theory, which originated in the paper "Economic Circuitry" published in 2011, of differential sets is novel, seemingly confirmed by the description of it, by some, as "Lindian".

The basic idea is that a differential intersection describes a "relational intersection" where the sets are transformed as they intersect, intersect according to a transformation, or both.

Formally this is accomplished by generating a unit vector field for t's gradient with solutions at all values at each of the sets being intersected.

For all sets under intersection "differential set logic" is used to generate mapping functions, which take the transformation function theta and the vector field associated with the set. For a given element of a set the elements in the other sets are iterated over and the vector field generated, from the other set, is solved for the iterated element and then geometrically compared to the gradient of an integral of theta between the t' mirror bounds.

The idea behind the gradient vector field geometric comparisons is, that I believe, by definition we're creating a differential surface that for two elements will be equivalent iff the elements are geometrically equivalent with respect to the transformed plane.

It is important to note that all elements in this system must be triples or:

$$\forall n := \langle a :: t, b :: t, c :: t \rangle :: t$$
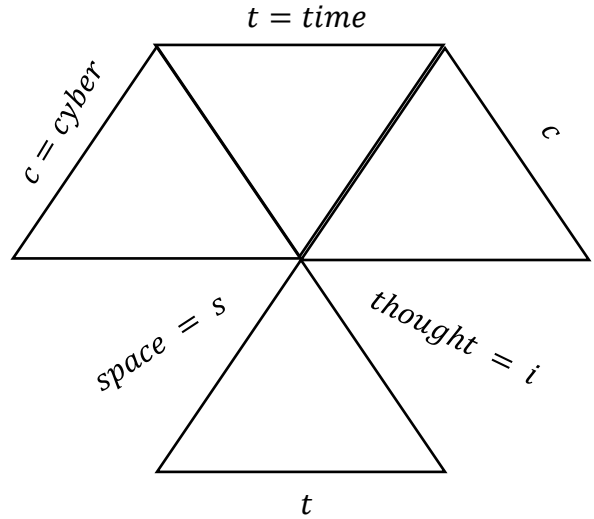
$$\bigcap_{n}^{\infty} x \, dA\Omega = \text{EM}_n$$

The example to the left describes an intersection over set n into infinity transformed by "Alpha-Omega" such that the points will intersect according the geometries defined by their respective vector fields, however there is no actual transformation of the points.

$$\bigcup_{\text{⋔}} A\Omega \, ds = \mathbb{s}$$

This union, with "pitch-fork" unioning itself according to a transformation with respect to space into "Alpha-Omega" – which transforms the results itself.

$c = \langle connections = ct, transport = tp, data = d\rangle$

$s = \langle x, y, z\rangle$

$t = \langle past = p^-, present = p^\circ, future = f\rangle$

$i = \langle utility = u, processor = pr, memory = m\rangle$

$c \cup d \cup t \cup i = A\Omega$

We define the union of these dimensional concepts as the variable "Alpha-Omega". The most basic relationship is how we define the electromagnetic field:

$$\bigcap_{n}^{\infty} x \, dA\Omega = EM_n$$

The equation to left, in differential set notation, states that an electromagnetic field over concept(s) `n` is the intersection over those concepts with respect to the dimensions. This would imply that different concepts bend or warp dimensions differently.

The equation to the right describes the rise of the traditional spatial domains used by most militaries to segregate warfighting responsibility across branches and services. A differential union with respect to the spatial dimension over the observer's perception of the known universe yields the concept of known space.

$$\bigcup_{\text{\tiny m}} A\Omega \, ds = \text{s}$$

Domains are defined as local interpretations of the consequences arising from the natural relationships between the dimensions that give rise to them. Domains are always a perspective of ones perception of known reality and as such there can be disagreement between their definitions without violating the

$$\iiint EM_\text{s} \, dc \, dt \, di = Spatial \; Domains = \varsigma$$

meta-model. The triple integral (4th dimensional surface), over the Electromagnetic Field arising from the Spatial Concept, with respect to cyber, time and thought gives rise to the spatial domains.
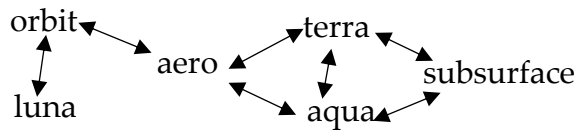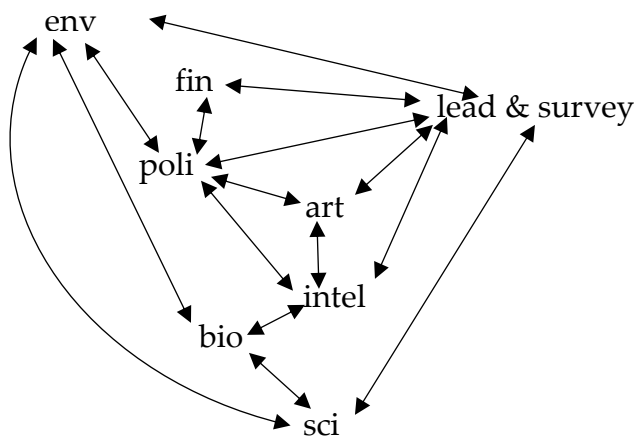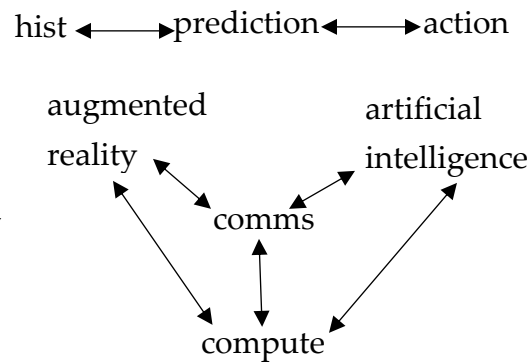
From my perspective "subsurface" connects to "terra" (land/surface) and "aqua" (water) both of which connect to each other and aero (land) which connects to "orbit" which connects to "lunar". Mars seems out of bounds for human warfighting at this point.

$$\bigcup_{\text{ᛘ}} A\Omega \, dt = \mathbb{t} \qquad \iiint EM_{\mathbb{t}} \, dc \, ds \, di$$
$$= Time \; Domains \; = \; \tau$$

$$\bigcup_{\text{ᛘ}} A\Omega \, dc = \mathbb{c} \qquad \iiint EM_{\mathbb{c}} \, ds \, dt \, di$$
$$= Cyber \; Domains \; = \; \gamma$$

$$\bigcup_{\text{ᛘ}} A\Omega \, di = \mathbb{i} \qquad \iiint EM_{\mathbb{i}} \, ds \, dt \, dc$$
$$= Thought \; Domains \; = \; \iota$$

hist ⟷ prediction ⟷ action

augmented reality   artificial intelligence

comms

compute

Whilst Space, Time and Cyber domains should, relatively at least, share a common perspective among the majority of actors, Thought is a much more complex topic. To the left is my initial render of the Thought Domains, also referred to as the Functional Practice Areas in earlier publications.

env — fin — poli — art — intel — bio — sci — lead & survey
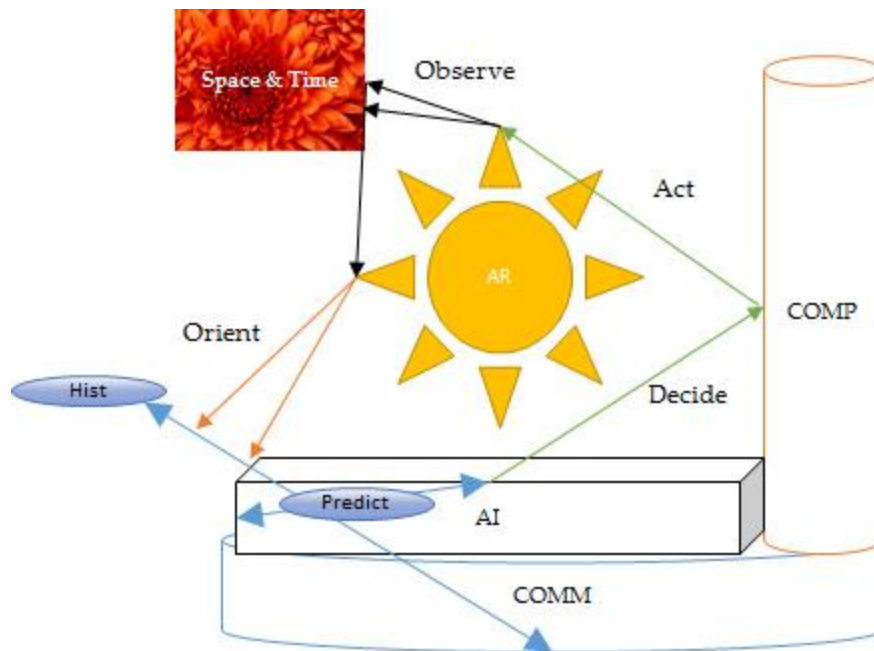
The diagram to left expresses thought interaction over the Space-Time-Cyber dimensions through the abstraction of the OODA loop introduced on page 3. The next section introduces a Military Force Structure based off this preemies.

COMBATTING COGNITIVE WARFARE WITH MILITARY STRUCTURE CHANGES – A PEEK INTO THE NEEDS OF 2025-2030

To combat our adversaries rapid advances into cognitive warfare, as evidenced by events such as the 2016 Election "Hacking" by Russia and the 2019-Present (Dis)Information Warfare Campaign by the Chinese regarding COVID-19, we must explore all opportunities to create more resilient "human networks" – in this case "Thinking Beyond C2 (Command & Control)" ["Space Force: An Opportunity to Rethink C2" Lind 2018]. Military Structure is at its core a formalized "human network" however current iterations were designed to combat and defend physical, not mental, threats – therefore it should be logical that in order to face emerging threats, as well as to implement new offence effects, that a re-architecture of military structure should be high on the priority list.

Lindian Model Theory (LMT), presented in "A Treatise on Reality Pre-Draft I" [ATR] (Lind 2020) provides insight into force structure by naturally deriving a management structure via the concepts of Cyber, Space, Time and Thought. While, in LMT, there are many possible solutions to this problem we use "Economic Circuitry" [EC] (Lind 2011) to bound the solution set which then provides a unique solution by bounding with "Ideal Organizational Theory" [IOT] (Lind 2010) and then it reduces to "C6M" - Command, Control, Communications, Coalition, Operations, Coordination: Manifest. Operations is considered a `C` because of the implied connotations that is on par with the other "big C's" – and more than just in magnitude of importance but also characteristic root geometry, in fact Control and Coordination are defined much differently than Command, Coalition, Communications and Operations in that Control and Coordination have External and Internal components.

The diagram on the left shows a conceptual look at the relationships between the C6M components.
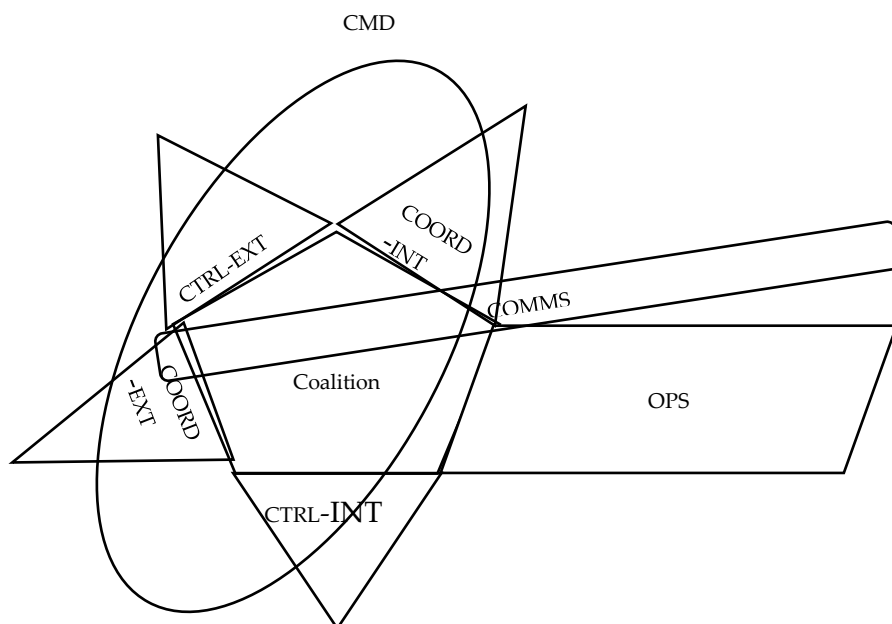
To defend and engage in Cognitive Warfare a "Corporation" (in EC terms) must have strong, in terms of "power" and "influence", "cyber-connection" bindings in order to resist aggressions, and blowback, from enemy – and allied - Cognitive Attacks. We argue that IOT is demonstrably, at a high level of abstraction, the mathematically most effective solution to this problem – and in fact "Corporations" that leverage these tenants will achieve "Artificial Intelligence".

This is because IOT posits/proves that the careful structuring of organizations naturally gives rise to Artificial Intelligence. This is NOT a computational AI singularity but rather a meta one in that the totality of the natural forces of the collective minds of in organizations equate to more than the parts.

Artificial Intelligence = Finite interaction is optimized through oligopical competition, whereas non-finite processes are optimized by the free marketplace. Formal organizational group structure therefore must be oligopical, but their interaction must be free. The individual is a monopoly. Q.E.D.

The above "equation" is the thesis of IOT and is the blueprint for defining organizational systems that give rise to "Intelligent Markets." C6M is a natural system that adheres to the principles of IOT at the LMT level.

SCA MANIFOLD MAPPINGS

C6M Component	OSI-E Layer	ZT4 Zone*	ZTA Binding
CTRL-EXT	13	IV	$\alpha\beta$
CMD	12	VIII	B
COAL	11	VII	Γ
COORD-EXT	10	VI	β
OPS	09	III	β
COORD-INT	08	VI	β
COMMS	07	II	β
CTRL-INT	00	IV	$A\gamma$

*All Components in C6M-SCA Mapping are in ZT4 Zone IX

The above is the bilateral definition of the Secure Cognitive Architecture to C6M based on the dimensional – and thus implied functional – definitions on the next page. For example in this model Command is a modeled as a ZT4 "Device" - implying that Command interacts with, and influences, reality and meta NOT that it is robotic.

The ZTA Bindings are also indirectly analogous to the SCA in that Coalition for instance is bound to Presence of Identity (Gamma) whereas the SCA defines it as between 13&12.

EDUCATION AND COGNITIVE WARFARE

Education must achieve several goals over the next 25 years:

1. Prepare the populous for a transformed "new-collar" economy as a result of exponentially increasing artificial intelligent actors (the information singularity).
2. Resolve *ism issues between population sets, particularly with a simultaneously and rapidly condensing and de-homogenizing generational gap.
3. Make resilient the population from Cognitive Warfare attacks by providing them with tools to sort out "natural delusions" in an effort to suppress the "Madness of Crowds"

What is a delusion? The DSM V roughly defines one as "the procession of an extraordinary belief that is held in spite of irrefutable contradictory evidence." Those seem easy enough to diagnose: a classic one being a woman claiming to be the Queen of England despite being shown a birth certificate from the United States.

THINKING PROBABILISTICALLY

BOOLEAN QUESTIONS

A core element of any thought: is questioning, and the most basic question requires a `Boolean` answer – that is yes or no. Even with the most basic of questions it is most often impossible to have absolute certainty – such as when asking "does 1+1=2?" someone is undoubtedly going to point out 1 male mouse + 1 female mouse will generally yield more than 2 mice.

REASONS FOR DISCREPANCY BETWEEN ANSWERS

BIAS

Recognition of your own, and others', natural biases when answering a question can help clarify what is the accepted answer to a question.
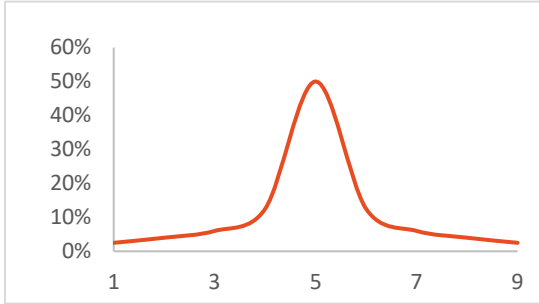
DISPUTED UNDERLYING FACTS

The facts used to answer a question are often in dispute – understanding the differences of perception are key to creating a resolved frame of reference.

UNKNOWN INFORMATION

Admittance that there are things that an observer cannot possibly know only can make their observations stronger

REALITY AS A PROBABILITY CURVE

A probability curve, by definition, must have a density (integral) of 1 - such as the curve to the right: options 1 and 9 are at 2.5% ranging up to 50% for option 5. This nears a classic "bell curve" often found in nature. Let us sit back and think what it really means to have a probability distribution over 9 options: we are saying that "there is an '20%' chance of 'x' option occurring compared to '80%' chance for 'y'" - therefore, in this instant, x happens 20% of the time and y happens 80% of time - which implies that, to some extent, both are real events - at the very least before the occurrence.

In most frameworks there is only one universal reality, however wouldn't it make more sense to at least plan for multiple realities?

GENERATIONAL REALITY MANIFOLD

A generation can loosely be described as "the set of people born between a distinct set of years." More than just a range of years where someone was born – a generation is accepted to have connotations of "general behavior."

Since the beginning of the industrial revolution generations have usually been defined into 20 year spans, however with the advent of the Information Age it is beginning to be clear that the time on network is having more of an impact on one's behavior than when one was born –

thus resulting in increased "blurring of the edges" and compressed timeframes between iterations.

To educate different generations we must understand their perspective and build to their modes of learning, or more technically put: be willing to adapt our utility curves to theirs.
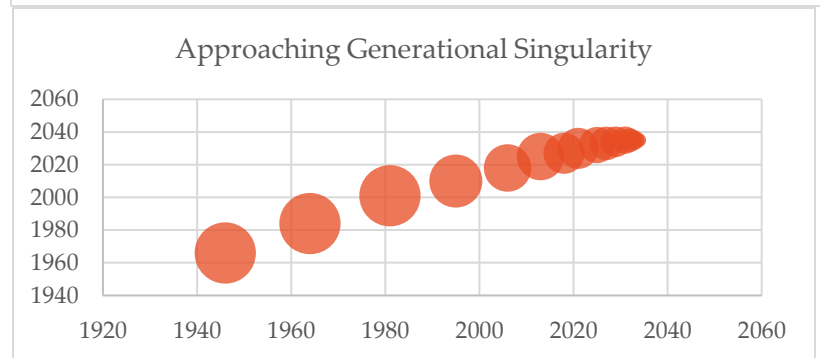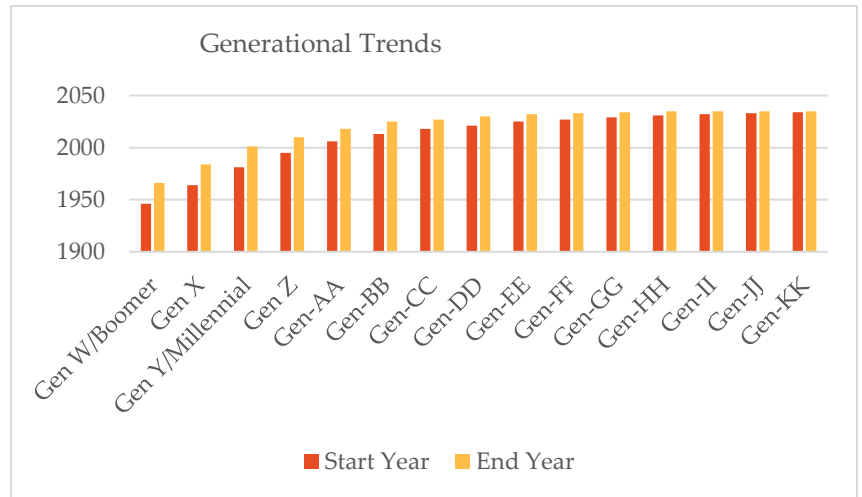
THE SPACE FORCE AND EDUCATION

Not to be confused with the United States Space Force (USSF), The Space Force (-SF-) is a construct that binds *.space over nato.int. We will design this Force to have an initial condition of existing only in meta, however the nature of the equations yields the expectation that it will eventually resolve into something concrete: Starfleet and The Federation/Earth. With these **bold statements**[mil.wwidew.net] it is now time to Architect, Innovate and Power: The Space Force.

To boldly advance Allied interests in Space Force, that is the relationship of Operations, Civilization and Cyberspace, through the establishment of a standing military force to repel our adversaries' counter interests.

We believe it is imperative that we take promising young minds who are "lost in space" – that is for whatever reason they have interest in technology and participate on the network but did not complete high school, have gotten into trouble with the law, have "mental health" conditions – and put them into specialized training to affect the network. Particularly this could help minority, immigrant and rural populations who do have access to the same opportunities those of us "in the loop" did.
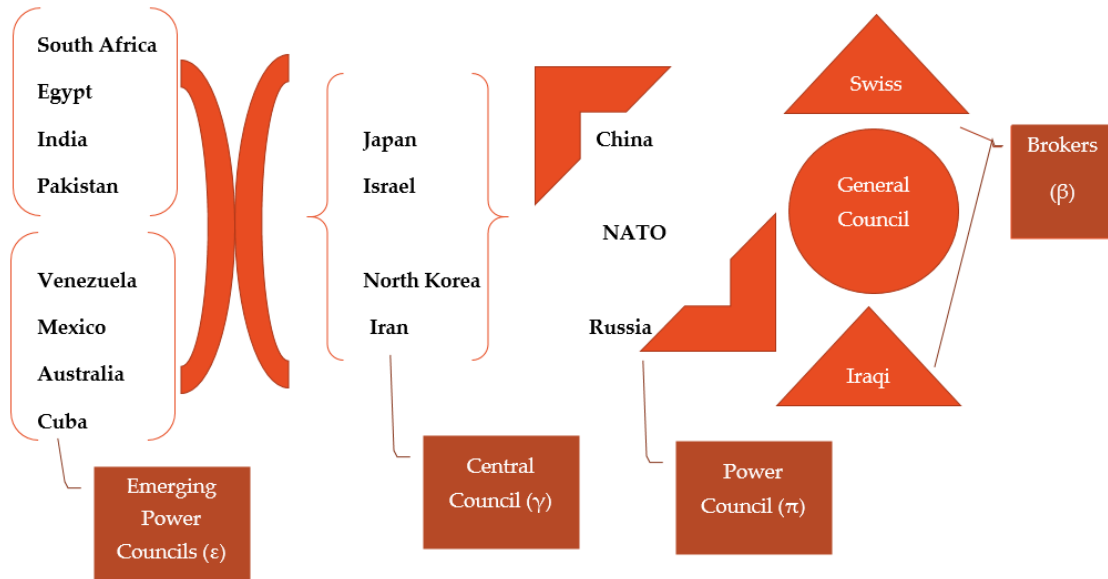
Transforming education at the adult level is just as important as doing so at that of the child. We can't just assume that primary and secondary education has done an adequate job, in fact we must assume the opposite as the number of exceptional students coming out of those programs is quite small while, especially in vulnerable populations (e.g. minority, immigrant, rural. "mentally ill", etc.), there are large numbers of students with major deficiencies.

USSF		The Space Force (NATO)		United Nations (Starfleet)	
		OS-1	Ensign		
		OS-2	Lt.		
O-1	2nd Lt.				
O-2	1st Lt	OS-3	Lt. Commander		
O-3	Captain			OJ-1	Fleet Ensign
O-4	Major	OS-4	Commander		
O-5	Lt. Col.	OS-5	Captain		
O-6	Col.			OJ-2	Fleet Cmdr.
O-7	Brig. Gen.	OS-6	Vice Admiral		
O-8	Maj. Gen.				
O-9	Lt. Gen.	OS-7	Admiral	OJ-3	Fleet Captain
O-10	Gen				
O-11	Space General				
				OJ-4	Fleet Admiral

The Space Force ranks and UN Starfleet ranks are NOT recognized by NATO or USSF currently, however we can unilaterally federate our ranks with NATO ranks.

Iff we attract significant membership from NATO personal – the laws of trans-dimension dictate that these will Transform NATO into an organization that defacto federates with these ranks.

OS = Office Space, OJ = Officer Joint

UN CYBERCOM Architecture

South Africa
Egypt
India
Pakistan

Venezuela
Mexico
Australia
Cuba

Japan
Israel

North Korea
Iran

China

NATO

Russia

Swiss

General Council

Brokers (β)

Iraqi

Emerging Power Councils (ε)

Central Council (γ)

Power Council (π)

$$\varphi(X) \xrightarrow{yields} random|x \in X$$

$$2\left(\sum_{\epsilon \in \varphi(\varepsilon)} \frac{\epsilon_{vote}}{4}\right) + \sum_{c \in \gamma} c_{vote} + 4\varphi(\pi)_{vote} + 2avg(GeneralCouncil_{vote}) + 0\beta_{vote}$$

The goal with our proposed UN CYBERCOM is not one of offense or defense, but rather advancement through stability – resolving conflict before member: and non-member – state: and non-state – actors' activity spill over into a tit-for-tat never ending war. This white paper demonstrates the cognitive, not just bits and bytes, is being manipulated and – while ZT4 and SCA can mitigate risk and secure substantial vectors –the risks and attack surface will only exponentially increase over time.

The proposed voting architecture, over the state actors, is described above, using random selection at both the bottom end (among the two Emerging Power Councils) and the top end (within the three Power Councils).

The Future of Cyber is Peace, not War.