

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

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:

- Propose an extension to the OSI Model and a Zero Trust variant ‘Abstract’ (ZT4)
- High-level draft of Secure Cognitive Architecture (SCA)
- Introduce the Lindian Model Theory/ 12-dimensional Meta-Prism
- Define C6M – Command, Control, Coalition, Communications, Ops, Coordination: Manifest – and bind to SCA
- 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
- Brainstorm ideas on how to Stabilize the Political situation at home and abroad without violating US Law or Treaties

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.

Contents

Vision.....	3
Mission.....	3
Values	3
1. Networks	6
1.1. Military Structure	6
1.1.1. Derivation.....	6
2. Education	7
2.1. Economy.....	7
2.2. Isms	7
2.3. Resilience	7
Administrative Information.....	7

DEMONSTRATION ONLY

MultiPlex.studio (MPS)

Description:

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.

Stakeholder(s):

Jason L. Lind :
Coalition Lead

Mitchell Maddox :
Command Lead

Corporations :

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”.

Organizations :

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.

Vision

Advancement through stability ... peace, not war

Mission

To resolve conflict before member: and non-member – state: and non-state – actors’ activity spill over into a tit-for-tat never ending war

Values

Macroeconomics: 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.

Advancement: 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.

Architecture: 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 $OO\mu D\tau A$.

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

Orientation: 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.

Decision Making: 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.

Action: Act -- execute the decision and then Observe the results.

Trust: 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. 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.

Security: 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 – 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.

Cognition: 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.

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

Markets: 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.

Probability: 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.

Consistency: REASONS FOR DISCREPANCY BETWEEN ANSWERS

Objectivity: BIAS -- Recognition of your own, and others’, natural biases when answering a question can help clarify what is the accepted answer to a question.

Factuality: 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.

Knowledge: UNKNOWN INFORMATION -- Admittance that there are things that an observer cannot possibly know only can make their observations stronger

Reality: 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?

DEMONSTRATION ONLY

1. Networks

Create more resilient “human networks”

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].

1.1. Military Structure

Re-architecture military structure

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.

1.1.1. Derivation

Derive management structure naturally via the concepts of Cyber, Space, Time and Thought

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.

2. Education

Educate the populace to think probabilistically

Stakeholder(s)

Generations :

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.

2.1. Economy

Prepare the populous for a transformed “new-collar” economy as a result of exponentially increasing artificial intelligent actors (the information singularity).

2.2. Isms

*Resolve *ism issues between population sets, particularly with a simultaneously and rapidly condensing and de-homogenizing generational gap.*

2.3. Resilience

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”.

Administrative Information

Start Date:

End Date:

Publication Date: 2020-12-09

Source: <http://multiplex.studio/files/CognitiveCyberwar.pdf>

Submitter:

Given Name: Owen

Surname: Ambur

Email: Owen.Ambur@verizon.net

Phone: