UTHOUGHT: Applied Cognitive Warfare Operational Research at ROTC Level

A Hybrid Peer-Instructor Leadership Camp at University of Utah Missioned to Transform Cyberspace through Global Information Manipulation & Dissemination

Jason L. Lind
Coalition Leader / lind@multiplex.studio
+1 414.788.2820 in/odyss3us

Haris Masic
CEO / hmasic@cyberinfrastructure.tech
+1 385.259.5879 in/haris-masic

Stealth Cognitive Warfare Experts
cognitive@multipliex.studio

Abstract

The Mind is the Next Frontier to Protect and Defend & it is Already under Attack from our Adversaries (1)

At UTHOUGHT we seek to not only educate our cadets on the tools and techniques of Cognitive Warfare / Social Engineering but place them in the field as "operational researchers." University of Utah NROTC programming will not have capacity for formal cybersecurity training for the foreseeable future and as such this will be an extracurricular activity that is both highly encouraged by command and compensated through the ONR grant. We intend to provide real world objectives, most likely in an unofficial support capacity of US CYBERCOM, to affect cognitive transformation of our adversaries' cyberspace.

INTRODUCTION TO COGNITIVE WARFARE

The future of cybersecurity is not defending against "bits and bytes" network attacks but rather the manipulation of human perception. Enter the realm of NATO's 3rd Operating Dimension and 6th Warfighting Domain (2): Cognition. Cognitive Warfare, a relative of "Social Engineering", we define as "next-order Cyberwarfare: 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." (1)

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. (1) To account for blow back all tactics reduce to leveraging transparency as a weapon. We are quickly entering an age of "no more secrets" and as such OPSEC that relies on obfuscation of strategy is inherently flawed. Ostensibly this turns Sun Tzu on its head, deception being the heart of warfare and all, however "The knights of old would first put themselves beyond the possibility of defeat before mounting a devastating attack against their enemy; thus achieving victory" – to be beyond defeat against enemy that sees and knows all is to have a plan that can't be defeated.

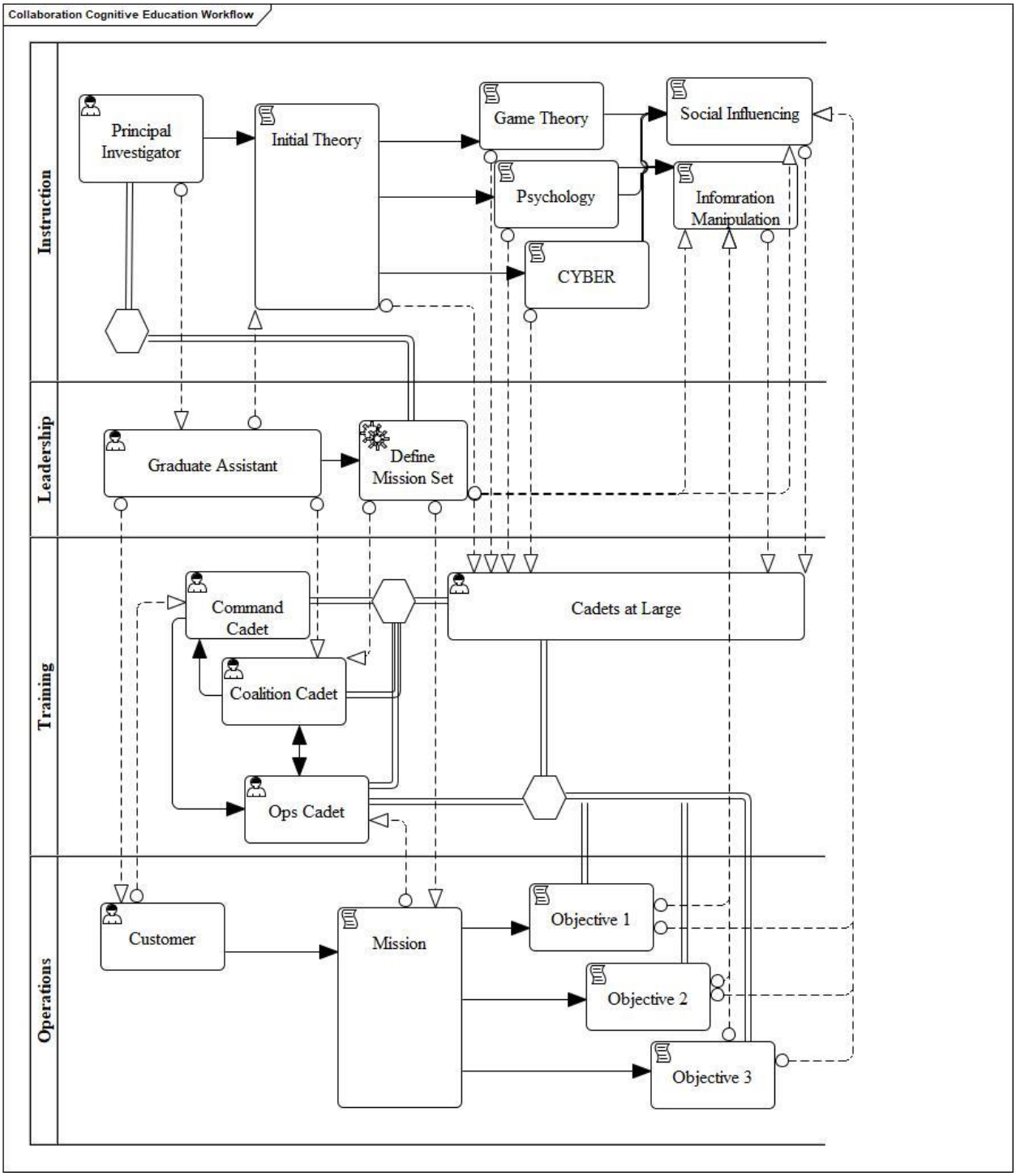
This is of course easier said than done and much research and development, in both human and computational resources, must be done before we start advertising our battle plans – however in order to do this we need to develop a new generation of CQW Operators and to do that we need a mission set. There is a clear need for "Operational Education" where training and operations are intermingled on a continuum – each driving the other. (3)

THE UTHOUGHT CONCEPT

To enhance American and Allied standing in the international community we must defend and attack in the Cognitive Domain requiring a new breed of military operators trained in the tools of both cyber and psychology. We will educate our cadets in the art and science of information manipulation – and further place them in an operational role, almost from day one, to practice and hone their skills. The instruction of Cognitive Warfare cannot take place in a vacuum: as these skills are taught cadets will innately practice these skills in their everyday lives and thus we must provide them with missions to channel this energy for the benefit of their country.

COGNITIVE EDUCATION WORKFLOW

Our process of placing cadets, under the tutelage of a Principal Investigator (Georgetown Professor) and a Graduate Leader (Research Assistant), in operational positions is described in the Business Process Model Notation (BPMN) diagram below.



WORKS CITED

1. **MultiPlex.studio.** A Cognitive Cyberwar. [Online] Sept 2020. [Cited: Feb 17, 2021.] https://multiplex.studio/files/CognitiveCyberwar.pdf.

2. **NATO Innovation Hub.** Cognitive Warfare. [Online] 2021. [Cited: Feb 17, 2021.] https://www.innovationhub-act.org/content/cognitive-warfare.

3. **MultiPlex.studio.** Open Source Asymmetric Cyberwarfare Curriculum. [Online] Sept 17, 2020. [Cited: Feb 17, 2021.] https://multiplex.studio/files/OpenSourceCyberwarfareEdu.pdf.