SYM-AM-21-092

EXCERPT FROM THE PROCEEDINGS OF THE EIGHTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

Developing a Threat and Capability Coevolutionary Matrix: Application to Shaping Flexible Command and Control Organizational Structure for Distributed Maritime Operations

May 11–13, 2021

Published: May 10, 2021

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

Developing a Threat and Capability Coevolutionary Matrix: Application to Shaping Flexible Command and Control Organizational Structure for Distributed Maritime Operations

Dr. Ying Zhao—is a research professor at the Naval Postgraduate School (NPS). Her research is focused on data sciences, machine learning, and artificial intelligence methods for defense military applications such as semantic and social networks, common tactical air pictures, combat identification, logistics, and mission planning. Since joining NPS, Zhao has been a principal investigator (PI) on many projects awarded for DoD research projects. She received her PhD in mathematics from MIT and is the co-founder of Quantum Intelligence, Inc. [yzhao@nps.edu]

Abstract

The mission of the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S) is to quickly and cost effectively deliver and sustain secure and resilient capabilities to warfighters and international partners. There are urgent requirements to develop adaptive acquisition framework (AAF) to speed up software development and acquisition processes that strengthen the concepts of operations (CONOPS) such as distributed maritime operations (DMO). It is imperative for the Department of Defense (DoD) to shape the AAF using data-driven analysis linked to the National Defense Strategy and the nature of global threats, and scale new capabilities to counter new threats. The threat and capability coevolutionary matrix (TCCM) addresses the requirement. A threat is a problem a capability tries to deal with. A capability is the solution to the problem that represents a threat. Coevolutionary algorithms explore domains in which the quality of a capability or combination of capabilities is determined by its ability to successfully defeat a threat or combination of threats. TCCM has the potential to systematically optimize, recommend, and coevolve capabilities and threats in new and contested environments. We show a use case regarding helping a program executive office (PEO) to wargame capabilities and threats against a specific domain DMO using unclassified data compiled from open sources.

Introduction

It is necessary not only for the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S) to shape the acquisition strategy but also for the whole Department of Defense (DoD) to apply data-driven analysis and innovative and adaptive concepts of operations (CONOPS) linked to the National Defense Strategy and the nature of global threats and to scale new capabilities for warfighters.

For example, to enhance total force readiness and project combat power across the wide range of operations and spectrum of conflict at any time, the Navy needs flexible command and control (C2) organizational structures to meet the CONOPS. For example, DMO is a CONOPS for the Navy, and expeditionary advanced base operations (EABO) is a CONOPS for the U.S. Marine Corps (USMC). Both DMO and EABO are emerging operation concepts for modernization of naval warfare. PMW 150, PEO C4I's Program Office for C2 Systems and preeminent provider of C2 solutions, focuses on acquisitions to transform operational needs into effective and affordable operational and tactical C2 capabilities for the Navy, Marine Corps, Joint and coalition warfighters. PMW 150's mission is to "innovatively meet operational requirements with relevant capabilities, enabling the warfighter to maintain C2 superiority" (Colpo, 2016).

On the other hand, U.S. ships' maritime operations, particularly in the littorals, will continue to be contested and dangerous; therefore, it is imperative to develop DMO and EABO towards a unifying operational vision. DMO aims to support national and strategic objectives in contested environments. The DMO concept considers not only offensive strikes as the primary

tactic for winning in battle, but also identifies the ability to deceive and confuse the enemy as a critical task to achieve success in a contested environment. The current efforts are focused on integration of existing platforms, systems, and capabilities with the DMO specific tactics to achieve maritime strategic and operational objectives. DMO is defined as the "warfighting capabilities necessary to gain and maintain sea-control through the employment of combat power that may be distributed over vast distances, multiple domains, and a wide array of platforms" (Navy Warfare Development Command [NWDC], 2017).

The development of DMO as a concept for the operations of Navy and Marine assets stems from the Distributed Lethality (DL) model (Popa et al., 2018). The concept of DMO adopts an extended viewpoint of DL, comprised of three pillars: the ability to increase the offensive power of individual warships through networked firing capability, distribution of the offensive capability over a wide geographic area, and the allocation of sufficient resources to the surface platforms in order to enable the enhanced combat capability (Rowden, 2017). DMO also stresses the need for more resilient and sustainable surface platforms in all domains, including air, subsurface, and cyber warfare. The futuristic view of DMO is to be a fleet-centric fighting power, enabled by integration, distribution, and maneuverability that allows simultaneous and synchronized execution of multiple capabilities and tactics across multiple domains (contested-air, land, sea, space, and cyberspace; DoD, 2018) in order to fight and win in complex contested environments (Canfield, 2017). Therefore, DMO not only includes traditional warfare capabilities of sensors, platforms, networks, and weapons, but also extends to other tactics that evolve with new technologies. The DMO concepts use advanced detection and deception involving ISR, machine learning (ML), and artificial intelligence (AI), with the use of unmanned systems particularly for enhanced capabilities in offensive tactical operations; therefore, by potentially leveraging different combinations of platforms, sensors, weapons, networks, and tactics, the combat power of a diverse yet unified force can be amplified across all maritime domains.

The DMO concepts include detailed capabilities such as tactics for counter-measures, counter-targeting, and counter-engagements. Counter-measures are defensive capabilities which aim to divert threats. Counter-targeting may be offensive capabilities, deceptive tactics, and operational maneuvers that divert a threat. Deceptive tactics include swarms of unmanned assets, mechanical and physical counter-measures, electronic jamming, and the limiting of electromagnetic radiation, or emissions control (EMCON). Counter-engaging is to neutralize a threat.

Traditionally, a baseline force structure consists of a fixed set of friendly force ships and aircraft arranged into action groups including a Carrier Strike Group (CSG), Expeditionary Strike Group (ESG), Surface Action Group (SAG), and various independent deployable units such as expeditionary Marine units for EABO.

The DMO operational requirements include capabilities, manpower, maintenance, and supply, among other resources, to be carefully analyzed, planned, and executed, which require the right data strategy, distributed infrastructure, and deep analytics. The technical concept of Threat and Capability Coevolutionary Matrix (TCCM) addresses the requirements of DMO and EABO operations. A threat is a problem that a capability tries to deal with, including the complexity and urgency. A capability is the solution to the problem that represents the threat. Coevolutionary algorithms from the ML/AI community explore domains in which the quality of a capability or combination of capabilities are determined by their ability to successfully defeat a threat or combination of threats. Coevolutionary algorithms used in a wargame simulation are similar to the Monte Carlo simulation widely used in defense applications, except they engage ML/AI like forecast and prediction, optimization, and game (minmax) algorithms. The DMO and

EABO concepts require flexibility and evolution of the capability and resource networks that handle ever changing and evolving threats.

Methodology Review

A TCCM contains three aspects, as follows:

Data strategy

One data strategy for a big organization such as the U.S. Navy is to build a centralized big data store for all the suborganizations. For this strategy, one needs to gather data from across the organizations and enterprises and put them in a centralized location. Building centralized data repositories can be very expensive, in addition to creating security and trust issues. An alternative strategy is distributed data strategy, where a complex enterprise usually includes highly interacting, interrelated, and interdependent sub-systems. For example, data for a complex enterprise might be collected using distributed locations. This data strategy provides convenience, safety, and privacy for the data; however, it presents difficulty and challenges for data fusion and deep analytics. Traditional data sciences, even ML/AI algorithms used in small- or moderate-sized analysis, typically require tight coupling of the computations, where such an algorithm often executes in a single machine or job and reads all the data at once. Making a generic case of parallel and distributed computing across distributed data source proves a difficult task. One requires novel infrastructure such as Collaborative Learning Agents (CLA; Zhao & Zhou, 2014) or federated learning, where data from system of systems can be quickly examined locally, while analytic models from multiple agents can be also fused properly.

Distributed Infrastructure and Collaborative Learning Agents

The data strategy we focus on here is not only relevant to information warfare, but also to physical infrastructure such as force distribution, as well. Distributed force distribution allows avoidance of detection and flexibility of C2 among other innovations; for example, dynamic emergence and self-organization of new global structures can confuse the threats and adversaries. CLAs include distributed, networked, and peer-to-peer agent architecture and analytics. A single agent represents a single system capable of ingesting data, indexing, cataloging information, and performing knowledge and pattern discovery, machine learning from data, and separating patterns and anomalies from data. Multiple agents can work collaboratively in a network in Figure 1. In more detail, a CLA first applies unsupervised machine learning and data mining algorithms, indexes, catalogs, and data-mines structured and unstructured data sources and discovers knowledge patterns, then fuses models from its peer lists and makes them available for search and pattern match used for prediction. A network of CLAs' collaboration is achieved through a peer list defined within each agent initially, through which each agent passes shared information to its peers, and then re-organizes or emerges based on a coevolution wargame with the threats. A CLA network and collaboration mechanism is fault-tolerant, self-organizing, adaptive, and resilient. A CLA is fault-tolerant because if one CLA goes down, it can be locally excluded and does not affect the whole network; it is self-organizing because each CLA can have trusted peers (e.g., friends) based on its own real-time situation awareness and change dynamically. A CLA is adaptive because the top-level search, pattern match, and prediction depend on the real-time self-organized network structure. A CLA is resilient since it can apply the coevolutionary analytics in a wide space and simulate novel threat and capability for new and unknown situations.

CLAs have been used in Navy applications such as building swarm intelligence to health monitoring of systems of systems such as ships, Internet of Things (IoTs; Zhao & Zhou, 2019), and edge computing. CLA also participated in a Naval Trident Warrior exercise (Zhou et al., 2009).

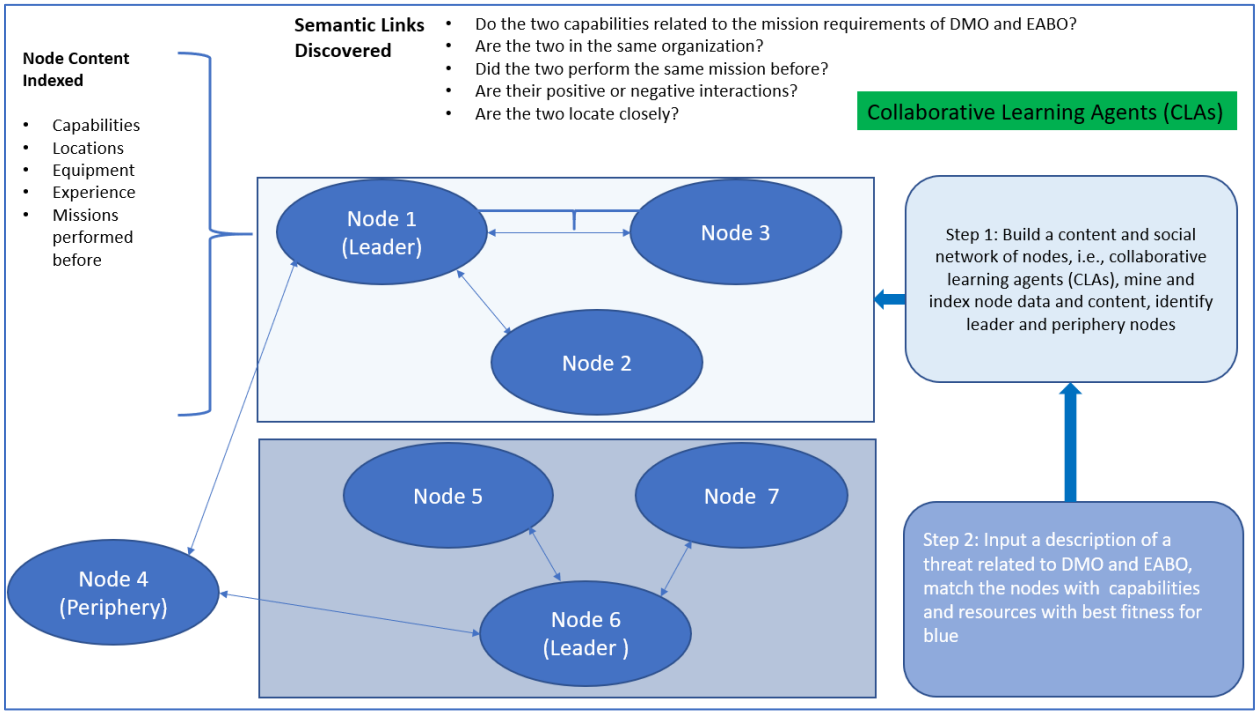

Figure 1. A CLA is Used in Each Node

Note: Each node's content and data may include capabilities; capability needs to be indexed, cataloged, and data-mined first.

Analytics

The core analytics for TCCM is a wargame simulation with two asymmetrical players. The self-player (blue) is the capability holder. The opponent (red) of the self-player is a threat generator. The opponent generates new threats that may challenge the self-player's capability. The self-player tries to predict and optimize capabilities to counter the opponent's threat. The whole process iterates. The self-player uses a wargame simulation to constantly perform what-if analyses in both threat and capability perspectives to defend a complex enterprise and its operations in a distributed and contested environment. Such a wargame simulation allows one to search, simulate, and detect vulnerability of the complex enterprise and evolve countermeasures, solutions, and resilience in a dynamic and flexible fashion.

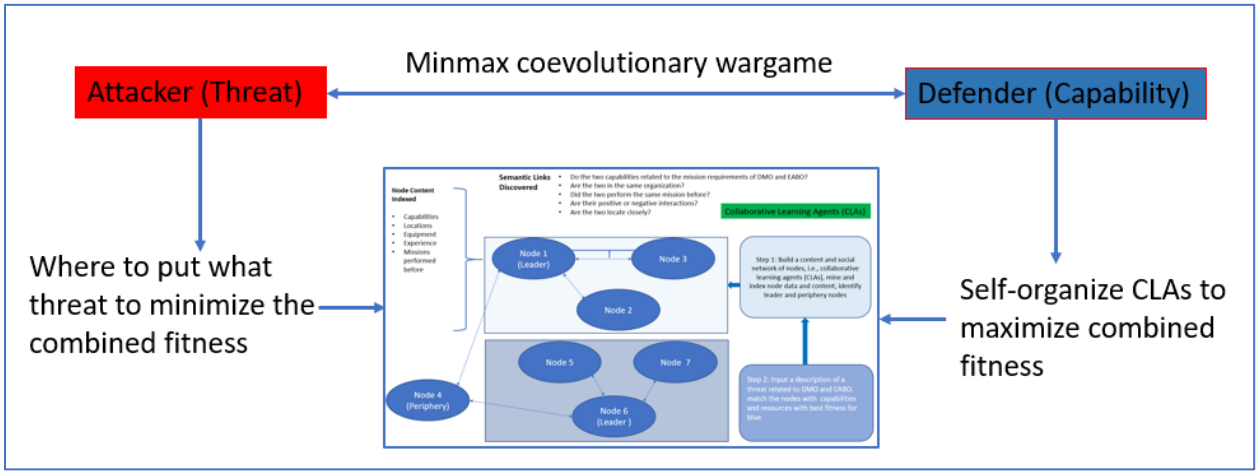

Figure 2. The Concept of TCCM and Wargame Simulation

Coevolutionary algorithms (Goldberg, 1989; O'Reilly & Hemberg, 2018; Popovici et al., 2012) provide search and optimization mechanisms based on evolutionary and genetic principles such as selection, mutation, and crossover. Coevolutionary algorithms explore domains in which the quality of a candidate solution (i.e., capability) is determined by its ability to successfully pass some set of tests (i.e., threats). Reciprocally, a threat's quality is determined by its ability to force errors and inefficiencies from a capability. Such a competitive coevolution is similar to game theory (Brown & Sandholm, 2017); however, it does not require computation of gradient as in ML algorithms and requires less data compared to other ML/AI algorithms. The search can lead to an arms race between threats and capabilities, with both evolving while pursuing opposite objectives. Coevolutionary algorithms are similar to those encountered by generative adversarial networks (GANs; Arora et al., 2017; Goodfellow et al., 2014).

The mutation and crossover evolutionary principles are unsupervised with known trends to produce better solutions. In TCCM, a selection is accomplished by evaluating a fitness function for the capability holder to see how likely it can successfully defeat a threat. A fitness function is typically modeled using supervised or reinforcement machine learning algorithms when a payoff (reward or penalty) can be clearly observed. By using a CLA to represent a self-player as a capability holder, the fitness function in this paper refers to a nearest neighbor lookup for an input threat (see the Use Case Scenario).

Use Case Scenario

The goal of this use case scenario is to help a program executive office (PEO) to wargame capabilities and threats in DMO focused areas. We will use this scenario to show a proof-of-concept of the TCCM.

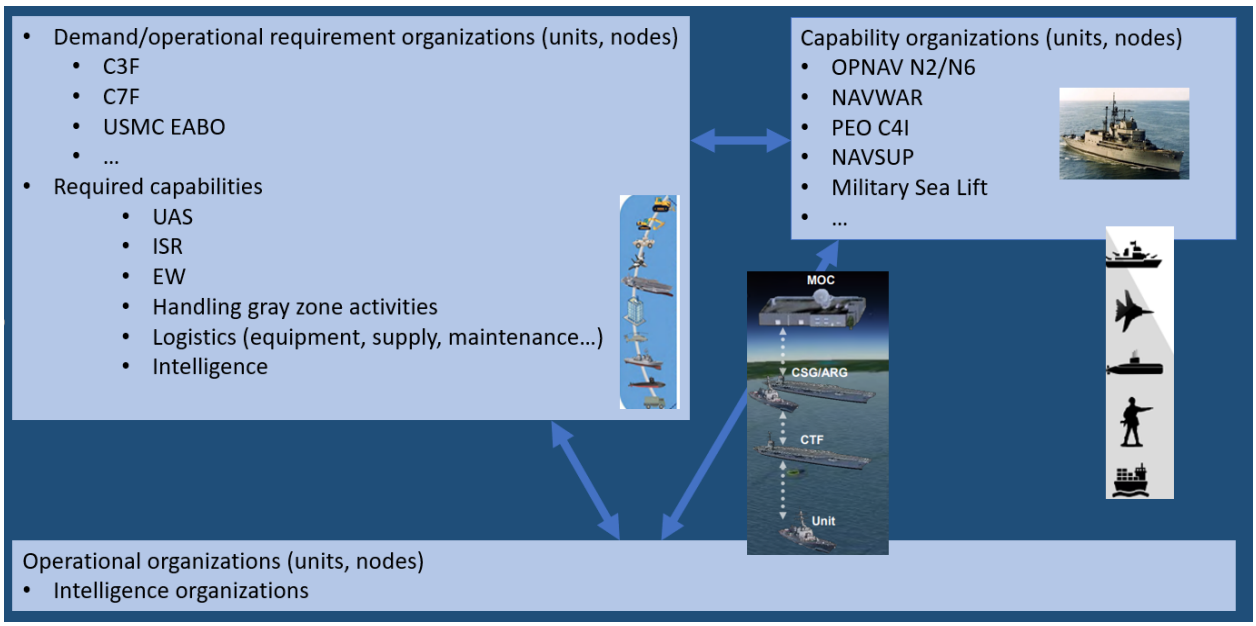

Figure 3. TCCM Use Case Scenario

As shown in Figure 3, the Navy's warfare resource, capability, and assets may reside in different traditional warfare domains such as sensors, platforms, networks, and weapons, as well as the new tactics related to the DMO concept. The goal is to achieve the creation and continuous use of a distributed tactical common operational picture, weapon system network, and the integration of unmanned assets and existing platforms to enhance defensive and offensive capabilities.

An order of battle (OOB) incorporates maritime platforms of surface ships, aircraft, weapons systems and sensors for both friendly and enemy forces. The high-level information of each platform, and asset for this paper, is compiled from open source databases, where a kill chain typically contains three steps: "find, target, and engage" (Joint Chiefs of Staff [JCS], 2013).

Operational domains can also include different areas such as air, surface, subsurface, land, and cyber, as well as detailed tactics that are associated with each domain. In a DMO environment, flexible combinations of these capabilities and tactics can provide powerful swarms of new capabilities that are unpredictable to new threats. A demand or operational node, such as U.S. Fleet Forces C3F or C7F as a node, may encounter a threat that may require capabilities of UAS, ISR, EW, new capabilities of handling gray zone (e.g., South China Sea) activities, logistics, or intelligence. The requirements go to capability organizations (units, nodes). In current C2 structure, a Maritime Operations Center (MOC) may communicate with a carrier strike group (CSG) or an amphibious ready group (ARG), then a carrier task force (CTF), and other units. Can the structure be more flexible, re-organized in a more dynamic fashion, and handle a vast amount and wide range of capabilities, resources, and requests? Future DMO enables a force that is capable of winning a fleet-on-fleet engagement through the integration of manned and unmanned systems, execution of deceptive tactics, and enabling units to conduct offensive strikes (Popa et al., 2018).

A wargame between a threat and capability can be set up as follows using the concept of coevolutionary process:

Self-player (blue, capability): Evolve a solution based on a current threat's characteristics (e.g., location). The solution may mean to find another CLA based on the input of required capability to increase the fitness functions representing measures of effectiveness (MOEs; global and overall measures) and measures of performance (MOPs; metrics for subtasks); for example, the selected CLA that represents an asset needs to contain required capability, and the asset has the highest probability of detection (POD) or probability of kill (POK) as MOP and MOE.

Opponent (red, threat): Evolve the location and other characteristics to reduce the fitness of the self-player.

A detailed simulation is set up based on a matrix of association and fitness values shown in Table 1. A synthetic data of such a table can be formed using the reference (Popa et al., 2018); for example, sensor capabilities and platforms associations for the blue force can be shown as in Table 2.

Table 1. Threat and Capability Association Matrix

	Capability's Sensor *Cs*	Capability's Platform *Cp*	Capability's Network *Cn*	Capability's Weapon *Cw*	Capability's Tactics *Ct*	Threat's Sensor *Ts*	Threat's Platform *Tp*	Threat's Network *Tn*	Threat's Weapon *Tp*	Threat's Tactics *Tt*
Capability's Sensor *Cs*		x	x	x	x	x				
Capability's Platform *Cp*	x		x	x	x					
Capability's Network *Cn*	x	x		x		x				
Capability's Weapon *Cw*		x		x	x	x	x	x	x	x
Capability's Tactics *Ct*	x	x	x	x	x	x	x	x	x	x
Threat's Sensor *Ts*	x	x	x							
Threat's Platform *Tp*	x	x								
Threat's Network *Tn*	x		x	x	x					
Threat's Weapon *Tp*	x	x	x	x	x		x		x	x
Threat's Tactics *Tt*	x	x	x	x	x	x	x	x	x	x

Table 2. Sensors and Platforms for the Blue Force (Popa et al., 2018)

Sensor Capabilities	Platforms
Visual	All Surface, All Air, All Unmanned
Infrared	CVN, LHD/LHA, CG, DDG-51, DDG-1000, LCS, LPD, F-35, F/A-18, EA-18, E-2, P-8, MH-60, AH-1, MQ-8 Fire Scout, MQ-4 Triton, TERN
Electronic Support Measures (ESM)	CVN, LHD/LHA, CG, DDG-51, DDG-1000, LCS, LPD, F-35, F/A-18, EA-18, E-2, P-8, MH-60, AH-1, MQ-8 Fire Scout, MQ-4 Triton
Air Search Radar	CVN, LHA/LHD, CG, DDG-51, DDG-1000, LCS, LPD, MH-60, AH-1, TERN
Surface Search Radar	All Surface Platforms, MH-60, AH-1, TERN
Fire Control Radar	CVN, LHD/LHA, CG, DDG-51, DDG-1000, LCS, LPD, MH-60, AH-1, MQ-8 Fire Scout
Navigation Radar	All Surface Platforms
Phased Array Radar	CVN, CG, DDG-51, DDG-1000
AESA (Active Electronic Scanned Array Radar)	F-35, F/A-18, EA-18, E-2, P-8, MQ-4 Triton
Airborne Early Warning Radar	E-2, P-8
Synthetic Aperture Radar—Maritime	MH-60, MQ-8 Fire Scout, MQ-4 Triton

Weapon capabilities and platforms associations for the blue force are sampled in Table 3.

Table 3. Weapon Capabilities and Platforms Associations for the Blue Force (Popa et al., 2018)

Missile	Designator	Type	Launching Platform(s)
Standard Missile-2	RIM-66	Medium Range Surface to Air	CG, DDG-51, DDG-1000
Standard Missile-3	RIM-161	Ballistic Missile Defense	CG, DDG-51, DDG-1000
Standard Missile-6	RIM-174	Extended Range Surface to Air, Anti-Ship Cruise Missile (ASCM)	CG, DDG-51, DDG-1000
LRASM	AGM-158C	Long Range Anti-Ship Missile	CG, DDG-51, DDG-1000, F-35, F/A-18
Maritime Strike Tomahawk	MST	Long Range Anti-Ship Cruise Missile	CG, DDG-51, DDG-1000
Harpoon	AGM/RGM-84	Over the Horizon Anti-Ship Missile	CG, DDG-51, LCS, F-35, F/A-18
ESSM	RIM-162	Evolved Sea Sparrow - Medium Range Surface to Air Missile	CVN, LHA/D, LPD, CG, DDG-51, DDG-1000, LCS
Sidewinder	AIM-9	Short Range Air to Air	F-35, F/A-18, EA-18, AH-1
Hellfire	AGM-114	Short Range Air to Surface	F-35, F/A-18, MH-60, AH-1, MQ-8, TERN
AMRAAM	AIM-120	Advanced Medium Range Air	F-35, F/A-18
HARM	AGM-88	High Speed Anti-Radiation	F-35, F/A-18

The current operations for efficient ships are enabled by multiple systems and multiple weapons systems on a single platform. However, with DMO, “rather than heavily invest in expensive and exquisite capabilities that regional aggressors have optimized their forces to target, naval forces will persist forward with many smaller, low signature, affordable platforms” (Blivas, 2020), for example, integrating the Marine’s EABO systems. These smaller platforms will be greatly advantaged by employment from EABOs situated on partner territory in proximity to close and confined seas (Corbett, 2018). Also, even with the current capabilities, weapons and sensors do not have to be in the same platform to collaborate for a kill chain; for example, an Aegis ashore can launch a missile when another DDG detects a threat.

Table 3 lists examples of DMO tactics and counter-measures. As stated by Chung (2015), with the “increasing availability and proliferation of unmanned system technologies, such as unmanned aerial vehicles (UAVs) in civilian and military applications, both opportunities and challenges arise in addressing large numbers of robots capable of collective interactions.” Swarm, described as a cooperative system comprised of numerous UAVs that function with limited operator involvement (Lachow, 2017) or as a tactic for deception, including saturation of radar and detection systems by deploying a large number of remotely piloted vehicles, as well as the ability to emulate a larger vessel such as a surface combatant or manned aircraft by radiating active emissions from the unmanned systems.

IR Smoke can be used as a decoy for heat-seeking sensors and weapons. Electronic jamming is a function within the EW subcomponent of electronic attack and serves to overwhelm or deceive a sensor through the controlled and directed propagation of electromagnetic signals. Electronic jamming can also exploit a specific vulnerability such as the reliance on a single frequency. An EMCON employs measures to reduce the electromagnetic, acoustic, heat, and radar cross section signatures from the platform. For example, a ship or aircraft can limit nearly all navigation, communications, propulsion, and weapons systems to the minimum in order to reduce the probability of being detected.

Another example is developing detection capabilities of signature deception for DMO and EABO since emerging ISR capabilities mean the applicability of DMO, and EABO is dependent on a competition of detection. The deliberate use of signature emission to deceive a self-player and use of detection methods to detect deception have the potential.

Table 4. Examples of Blue Force DMO's Tactics (Popa et al., 2018)

Variable	Minimum	Maximum	Type
Swarm	0	1	Discrete
Chaff	0	200	Continuous
Flares	0	50	Continuous
Visual Smoke	0	50	Continuous
IR Smoke	0	50	Continuous
Active Decoys	0	25	Continuous
Passive Decoys	0	300	Continuous
Spot Jamming	0	1	Discrete
Barrage Jamming	0	1	Discrete
Sweep Jamming	0	1	Discrete
DRFM Jamming	0	1	Discrete
GPS Jamming	0	1	Discrete
CG EMCON	0	1	Discrete
DDG-51 EMCON	0	1	Discrete
DDG-1000 EMCON	0	1	Discrete

Application of Threat and Capability Coevolutionary Matrix

One CLA can associate with an asset, a platform, a unit, or a node, and the matrix in Table 1 can translate into the following representation in a CLA's association for a node:

- Capability_Platform_ddg-51 Capability_Sensor_visual 1
- Capability_Platform_ddg-51 Capability_Sensor_infrared 1
- Capability_Platform_ddg-51 Capability_Sensor_ESM 1
- Capability_Platform_ddg-51 Capability_Sensor_fire_control radar 1
- Capability_Platform_ddg-51 Capability_Sensor_phased_array_radar 1

Given a knowledge that the sensor of infrared is able to detect a threat platform x, an association between the threat's characteristics (e.g., platform x) and a capability's feature dimension can be stored in a node (e.g., Sensor 1 in Figure 4) as follows:

- Capability_Sensor_infared Threat_Platform_x 1
- Capability_Weapon_y Threat_Platform_x 1

The primary focus for collaborative assets with respect to DMO is to employ various traditional capabilities as well as DMO specific tactics and counter-measures that enable the disruption of the threat's kill chain to either prevent or lower the probability of the success of the threat. As shown in Figure 4, if a Threat Platform x shows up in a battlefield, the initial phase of a kill chain consists of a sequence of activities of sensor capability to detect and locate the threat. A Platform z equipped with CLA 0 in Figure 4 may send requests as inputs to its peer list of Sensor 1 (CLA 1) and Sensor 2 (CLA 2), which both have the infrared capability. Either of the sensors can potentially detect Threat Platform x and become the solution for Platform y's (CLA

0) request. The following other factors can be integrated into the TCCM's CLA's fitness computation:

- The probability of find or detection (POD), an important dimension for Platform z to make the decision of which solution to select from the sensors, may be different because of distance and range parameters.
- Even for the same sensor, POD can vary due to environmental factors such as weather, clutter, threat employed counter-measures, counter-engagements, and counter-targeting tactics. The environment in the vicinity of contested areas has the potential to impact the ability to perform DMO, specifically with respect to weather conditions and sea states, for example, the heavy presence of neutral commercial air and sea traffic (clutters) that cause significant congestion in sea lanes and air passages. For example, one-third of all global shipping passes through the South China Sea, as it is the one of the most used sea transit lanes in the world (Hoffmann et al., 2016). This may cause significant variation for POD, while an optical or infrared sensor can distinguish the threat as a legitimate target or neutral traffic; however, the fact can be also leveraged as an advantage for deception and decoy operations.
- A factor could be association constraints, for example, a U.S. aircraft carrier is a high value unit that is typically the highest targeting priority for the threat; therefore, the adversary's combat capable platforms will have a non-zero probability of being assigned the CVN for targeting and engagement.
- Another challenge is that adversaries may use maritime militia fishing fleets that serve as non-militarized ISR platforms, and the blue forces include general lack of geographical familiarity with the region as well as considerations for the attempted control and management of the electromagnetic spectrum.

Considering all the factors into the fitness best solution to Platform z via CLA 1 is the highest fitness from both sensors, for example, Sensor 1 (CLA 1) is selected. Since the peer list of the Sensor 1 (CLA 1) only includes Weapon 2 (CLA 4), Weapon 2 (CLA 4) is used for engaging with the Threat in the next step of the kill chain. Should Weapon 2 (CLA 2) be selected, which is a peer for Weapon 1 (CLA 3), Weapon 1 (CLA 3) would be used in the engaging step.

If the threat is successfully engaged and killed, the adversaries may try to learn from the experience (data) and may try to avoid the detection by moving away from the last location of detection and engagement. For example, the Threat Platform x may try to move to a different location that is away from the combination Sensor 1 (CLA 1) and Weapon 2 (CLA 4); because of the distributed and different peer lists and combinations of the self-player's assets, the self-player (blue) may be not predictable from the experience for the Threat, since the Threat can be caught up with Sensor 2 (CLA 2) and Weapon 1 (CLA 3) should the Threat move to a different location.

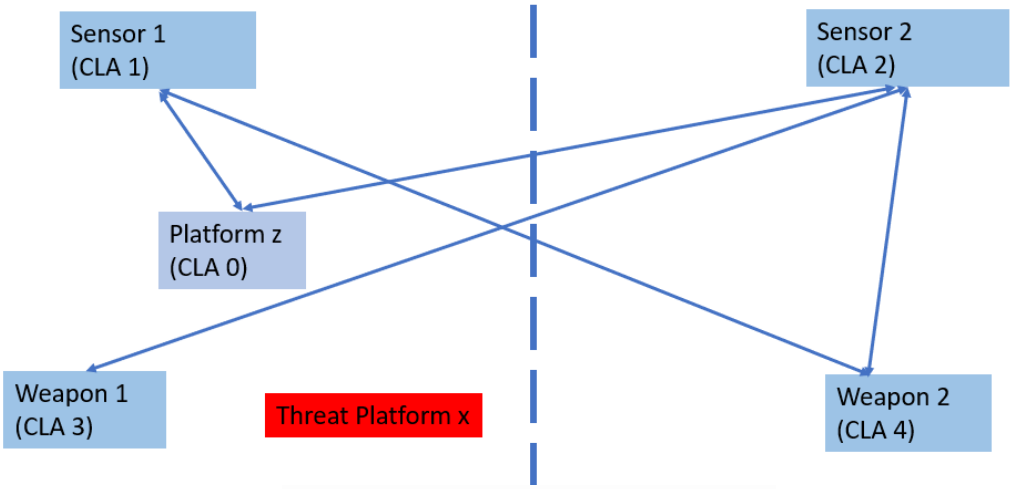

Figure 4. A TCCM Example for Illustration

Therefore, the following list shows the advantages of TCCM:

- TCCM uses the peer lists to combine capabilities at the various stages of a kill chain to disrupt and degrade the threat progress to its target of blue and confuse its learning. Even the self-player (blue force) can become less predictable or unpredictable if the peer lists are purposely altered randomly and periodically.
- TCCM represents pooled resources, and the model represents DMO as a united network of offensive lethality and firepower, and, therefore, all missiles are shared for cooperation and collaboration for all the assets and CLAs.
- Because of the potential dimensions, features, and characteristics of threats and capabilities, and their combinations, peer lists can be extremely large. For example, with the current systems, there are many different types of procedures or action chains used to conduct a detect-to-engage (DTE) series of events where sub-tasks must occur for a weapons system to effectively engage a threat's platform or location. Combinations of detecting or finding the target, establishing a track on the target's location and movement, communication of targeting data between the sensor and weapon system, conducting the engagement with either kinetic or non-kinetic weapons, and evaluating the engagement to determine follow-on actions, can be extremely large. It is necessary to apply a systematic engine like TCCM to manage the large-scale tactical and distributed decisions.
- TCCM is fault tolerant since the network is peer-to-peer. The network can be resilient like swarm intelligence, and CLAs can be re-organized to form emerging patterns which can be effective out of the box, given a wide range of contexts, and adapted to many others through reconfiguration and/or replacement (Goerger et al., 2014).

Conclusions

We show a TCCM and map it to a scenario that can help simulate threats and develop adaptations of capabilities for the benefits of the AAF, DMO, and EABO.

TCCM has the potential to systematically optimize, recommend, and evolve solutions to warfighters' requirements, which are more effective, suitable, survivable, sustainable, and affordable as a network of distributed and shared assets. A CLA network and collaboration

mechanism in TCCM makes it fault-tolerant, self-organizing, adaptive, and resilient. TCCM contains a system of data strategy, distributed infrastructure, and deep analytics that can greatly assist reconstructing defense acquisition, improving process effectiveness, and implementing the AAF, DMO, and EABO.

Compared to the current method with less DMO and without CLA, the probabilities of detection and kill or fitness functions for a kill chain are modeled adaptively and are therefore much less predictable by the opponent, threat, or adversaries' point of view, potentially adding to the concept and desired outcome of DMO for offense and defense. Should the opponent also adapt such a strategy, because of the asymmetry of assets and capabilities, the self-player is potentially still more advantageous over the opponent. Future work will include quantitative simulation to implement TCCM.

References

Arora, S., Ge, R., Liang, Y., Ma, T., & Zhang, Y. (2017). Generalization and equilibrium in generative adversarial nets (GANs). *Proceedings of the 34th International Conference on Machine Learning*, *70*, 224–232. http://proceedings.mlr.press/v70/arora17a.html

Blivas, A. (2020). 6 platforms for Marine expeditionary advanced base operations logistics. *The Diplomat*. https://thediplomat.com/2020/11/6-platforms-for-marine-expeditionary-advanced-base-operations-logistics/

Brown, N., & Sandholm, T. (2017). Safe and nested endgame solving for imperfect-information games. *Proceedings of the AAAI Workshop on Computer Poker and Imperfect Information Games*. https://arxiv.org/pdf/1705.02955.pdf

Canfield, J. (2017). *Fleet design* [Presentation]. NPS CRUSER Warfare Innovation Continuum Workshop, Naval Postgraduate School, Monterey, CA.

Chung, T. H. (2015). Advancing autonomous swarm capabilities: From simulation to experimentation. *Proceedings of the 2015 Winter Simulation Conference*. https://www.informs-sim.org/wsc15papers/236.pdf

Colpo, D. (2016, October 26). *NDIA C41 industry day* [PowerPoint slides]. Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C41). https://www.ndia-sd.org/wp-content/uploads/2017/02/2.PMW%20150_NDIA%20Fall%20Forum%202016%20Brief_OCT16.pdf

Corbett, A. (2018). *Expeditionary advanced base operations (EABO) handbook: Considerations for force development and employment*. Marine Corps Warfighting Lab, Concepts & Plans Division. https://mca-marines.org/wp-content/uploads/Expeditionary-Advanced-Base-Operations-EABO-handbook-1.1.pdf

DoD. (2018). *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American military's competitive edge*. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Goerger, S. R., Madni, A. M., & Eslinger, O. J. (2014). Engineered resilient systems: A DoD perspective. *Procedia Computer Science*, *28*, 865–872.

Goldberg, G. (1989). *Genetic algorithms in search, optimization, and machine learning*. Addison Wesley.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 2672–2680. https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf

Hoffmann, J., et al. (2016). *Review of maritime transport 2016*. United Nations Conference on Trade and Development. http://unctad.org/en/PublicationsLibrary/rmt2016_en.pdf

Joint Chiefs of Staff. (2013). Simplification of F2T2EA kill chain to FTE process. In *Joint Targeting* (Joint Publication 3-60). https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf

Lachow, I. (2017). The upside and downside of swarming drones. *Bulletin of Atomic Scientists, 73,* 96–101. https://www.tandfonline.com/doi/full/10.1080/00963402.2017.1290879

Navy Warfare Development Command. (2017). *CNO visits Navy Warfare Development Command*. https://www.nwdc.usff.navy.mil/Press-Room/News-Stories/Article/2406186/cno-visits-navy-warfare-development-command/

O'Reilly, U., & Hemberg, E. (2018). An artificial coevolutionary framework for adversarial AI. *Proceedings of AAAI Fall Symposium: Adversary-Aware Learning Techniques and Trends in Cybersecurity (ALEC)*. http://ceur-ws.org/Vol-2269/FSS-18_paper_37.pdf

Popa, C., et al. (2018). *Distributed maritime operations and unmanned systems tactical development* (NPS capstone project report). https://calhoun.nps.edu/handle/10945/59587

Popovici, E., Bucci, A., Wiegand, R. P., & De Jong, E. D. (2012). *Coevolutionary principles.* In G. Rozenberg, T. Back, and J. N. Kok (Eds.), *Handbook of natural computing* (pp. 987–1033). Springer.

Rowden, T. S. (2017). The U.S. Navy's surface force strategy: Return to sea control. *CHIPS*. https://www.doncio.navy.mil/Chips/ArticleDetails.aspx?ID=8574

Office of the Under Secretary of Defense for Acquisition and Sustainment. (n.d.). https://www.acq.osd.mil

Office of the Under Secretary of Defense for Acquisition and Sustainment. (2020). *Operation of the adaptive acquisition framework* (DoD Instruction 5000.02). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2019-05-01-151755-110

Zhao, Y., & Zhou, C. (2014). *System and method for knowledge pattern search from networked agents* (U.S. Patent No. 8,903,756). U.S. Patent and Trademark Office. https://www.google.com/patents/US8903756

Zhao, Y., & Zhou, C. (June, 2019). Collaborative learning agents (CLA) for swarm intelligence and applications to health monitoring of system of systems. In J. Rodrigues et al. (Eds.), *Computational Science – ICCS 2019* (pp. 706–718), *Lecture Notes in Computer Science* (Vol. 11538). Springer. https://link.springer.com/chapter/10.1007/978-3-030-22744-9_55

Zhou, C., Zhao, Y., & Kotak, C. (2009). The collaborative learning agent (CLA) in Trident Warrior 08 exercise. *Proceedings of the International Conference on Knowledge Discovery and Information Retrieval (KDIR)* (Vol. 1, pp. 323–328). https://doi.org/10.5220/0002332903230328

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net