

Dead Dinosaur Command and Control (C2)

Thursday, November 26, 2020

Authors



CDR (USN) Matthew Cegelske

Matt Cegelske is a 19 year Naval Officer and an aspiring leader in the Information Warfare Community and qualified Submariner. He has commanded Cyber Defense Activity SIXTY FOUR, Cyber National Mission Force's Task Force FOUR, and a Navy Network Operations Center. He's had the opportunity to serve aboard a Carrier Strike Group, Expeditionary Strike Group, and began his naval service in the Submarine force. He currently serves on The Joint Staff focusing on national security, cyber operations, and supporting the further development and readiness of the Cyber Mission Force. He served as a Cyber Fellow at Carnegie Mellon University and is a graduate of Maine Maritime Academy and the University of Maryland. He's humbled and thankful for the mentorship of the other two authors and the opportunity to work with them on this piece.



VADM (USN Retired) Timothy White

TJ White is a 30-plus year national security practitioner, strategist, and cyber operations expert leading joint military formations and combined intelligence community organizations. His most recent assignments were as the Commander, US Fleet Cyber Command / United States TENTH Fleet and previously as the Commander, US Cyber National Mission Force. He is a former Director of Intelligence for US Indo-Pacific Command and has served globally in various combat zones and conflict areas supporting competition dynamics. A former CINCPACFLT Shiphandler-of-the-Year, he misses his days driving a Battleship. His focus of effort remains risk assessment and consequence management with respect to cybersecurity, critical infrastructure, supply chain, technology policy, and trust relationships. A 1987 graduate of the US Naval Academy, he holds diplomas from the Naval Postgraduate School, Naval War College, National Defense University and other professional educational institutions.



RDML (USN Retired) Danelle Barret

Danelle Barrett served as Director of Current Operations at U.S. Cyber Command, and as the Navy's Cyber Security Division Director and Deputy CIO. She led the Navy's strategic development and execution of digital and cyber security efforts, enterprise IT improvements and cloud policy and governance for 700K personnel across a global network. She implemented visionary digital transformation to modernize with unprecedented speed, significantly improving Navy Information Warfare capabilities. Her other assignments include Commanding Officer, Naval Computer and Telecommunications Area Master Station Atlantic, and tours at Multi-National Forces Iraq, U.S. NAVCENT and 2nd Fleet, Carrier Strike Group 2 and Carrier Strike Group 12 which included deployments in support of Operations Enduring Freedom in Afghanistan and Unified Response in Haiti. She currently executes a portfolio of work that includes Independent Director on several boards, consulting, public speaking, and writing. Her book, "Rock the Boat: Embrace Change, Encourage Innovation and be a Successful Leader" will be out in June 2021.

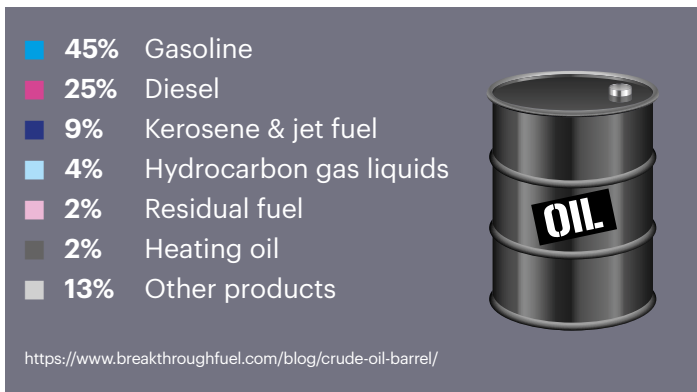
Like Oil, You Can't C2 Data...

Your Goal Should Be to Produce, Assure, and Consume

Data is the “new oil.” Dead dinosaur is a euphemism for oil industry product created through millions of years of molecular transformation (time, heat, and pressure). Oil remains relevant for a number of strategic geographic and political economy reasons. How oil gets commoditized as part of the energy sector and delivered to market is **less** command and control (C2) and **more** consumer driven. It is also a high confidence, resilient, assured, and standardized product.

Like the ubiquity of the global energy sector and its oil market, the Navy risks being a dinosaur in a world where data driving operations and warfighting is evolving at a staggering pace. The Navy's view of data must transform or it will fail critical Distributed Maritime Operations (DMO) objectives and will be on an extinction path. To prevail in Great Power Competition (GPC), we must avoid The Flintstones and embrace The Jetsons by making deliberate choices to invest in our data-driven digital domain.

What's in a barrel (bbl) of oil?



Data generation and consumption is a perfect match of want and need. You can't C2 it but you can disrupt, shape, and expand it. The dead dinosaur market is bigger than any one producer or consumer, and is both resilient and elastic.

There is a future which assesses uncertainty and past performance; fully commodified, literally, cash on the barrelhead. Everybody wants some, and the appetite for more increases by the minute.

Military commanders want C2 as a means to reduce uncertainty, manage risk, and better organize for combat outcomes. Are they learning the lessons of the oil commodity markets that C2 of dead dinosaurs is a fool's errand, as is C2 of data? The real task for operational commanders is threefold:

- (i) pressurize expectations,
- (ii) accurately identify requirements, and
- (iii) leverage quality, actionable, timely, secure and authoritative data.

Data must come from all sources, employ operations analysis and machine learning (ML), and optimize change detection while augmenting human performance. This is how we win at the lethality boundary of DMO.

Battlespace, environment, and terrain data combine to maintain tactical situational awareness, inform targeting, facilitate combat assessment, generate decision-making insight, and fuel the kill chain. Once we started shooting over the horizon (OTH), data became the commodity of kinetic and non-kinetic operational fires. When we began arming unmanned and autonomous systems, the lethality boundary became governed by trusted data. As 'over the horizon' and 'lethal' (accuracy, precision, rate, distributed) fires evolve, the more vital trusted data becomes. In traditional military planning and thinking, conventional wisdom misinterprets this to be Operational Control (OPCON) or C2, and has been misapplied to data.

The intelligence community (IC) enterprise (engineering, design, manufacturing, operations, and network) necessary to generate precise OTH fires-associated data desired by modern military commanders is exquisite. Little appreciated is the exceptional contribution of modeling and simulation to optimize resource tasking and sensor production to that data end-state. Much like oil, there is upstream exploration (sensors), and downstream processing (cybersecurity, algorithms, compute and transport). End-stream oil consumers rarely know the skill in discovery, commitment of capital, extraordinary efforts undertaken to buy-down risk, and the fact that oil from any well is assimilated into the global spot market with efficient pricing mechanisms and effective production and distribution. The same is true of Navy data consumers.


Over the past two decades, we dropped anchor in shallow water, safe harbor, uncontested domains, and underinvested cyberspace and its supporting infrastructure. Continuing the market analog, whilst primarily engaged in the Global War on Terror, we have incurred technical and operational debt that will be stressed by great power competitors going forward. Consider the stark contributing realities from our shift in focus:

- **Imagine our surprise that space is hard, high, fast, and expensive.**
- **Maritime operations were a simple matter of time/distance and a harder problem reconciling force employment (Fe) culture and force generation (Fg) capacity.**
- **Air power remains unchallenged.**
- **A lack of digital value– economy, society, democracy, and sensors – because many remain convinced data isn’t warfighting. Whoever “they” are think C2 of the end-to-end kill chain is a precondition to fight tonight. They don’t understand that data warriors are everywhere fighting today and preparing the groundwork for future wins.**

As in the oil industry, digital governance and standards are necessary for the Navy to effectively leverage data for strategic and operational advantages. The Department of Defense’s recently published data strategy, initiatives like Joint All Domain Command and Control (JADC2) connecting distributed sensors, shooters and data from all domains to all joint forces, and United States Cyber Command’s Project IKE using artificial intelligence (AI)-enabled tools alongside the Unified Platform to integrate cyber capabilities, systems, infrastructure, and data analytics supporting full spectrum cyber operations, are steps in the right direction. However, detailed alignment of resources, processes, technology, and policy is required if the Navy is to gain the desired information advantage the Nation requires.

What’s in a barrel (bbl) of Data?

■ ELINT	◆ Insight
■ COMINT	◆ Warning
■ EO	◆ Threat
■ IR	◆ Tracks
■ SAR	◆ Geolocation



The data north star needs two points:

- 1) **An afloat digital ecosystem which leverages the entire naval enterprise and aligns with the joint force. This ecosystem must encompass the naval information enterprise from the tactical edge (weapons, sensor, combat and control systems).**
- 2) **An entire ashore enterprise (business, force readiness (Fr), and national intelligence systems) increasingly hosted in the commercial cloud.**

This complicated system-of-systems must account for the global transport of data (quick, efficient, and secure) across the tactical edge and anywhere throughout the shore enterprise. Navy capability architects too often assume Ao=1 in the efficient discovery, processing, and data movement needed for the fight between the shore and the tactical edge, all while not ensuring that information infrastructure is in place.

Why invest in data?

More better data, less antiquated C2

Peter Drucker's "Culture Eats Strategy for Breakfast" sentiment summarizes the magnitude of the Navy's challenge. We either barely recognize the value of the data surrounding us or default to "admiring the problem." Our culture drives a C2 ownership paradigm limiting us from harnessing pervasive data streams to deliver our information advantage. This is because we lack data governance, policy, and holistic understanding of the current and future data landscape. While you can't C2 data, it still must be organized and standardized to enable discovery, interoperability, and lethality. It isn't.

Much like the oil industry which has long-standing and perhaps misplaced confidence in the survivability and future utility of their product in the face of growing competition from alternative energy sources, why are we confident in DoD's data-stream? Decision-making dinosaurs, expecting to conduct Joint All Domain Operations, must understand the Nation has already made strategic decisions about data which the Navy must embrace. It expects a:

- 1) Data Strategy – its sovereignty to be defended like any other strategic asset, manifest the same within the National Security Strategy and leverage Cyber Solarium Commission recommendations.**
- 2) Data Culture – to act upon data at speed and scale for operational advantage.**
- 3) Data Source – deliver authoritative data from its vast sensor front.**
- 4) Data Transport – Across robust, capable networks to the tactical edge and flowing into a data lake in the Cloud ashore for analysis, enabling warfighting advantages. This must occur in a "Zero Trust" cybersecurity framework, protecting data with permissions at the individual level for role-based access.**

The decision-space remaining for Combatant Commands (CCMDs) and the Navy is to make all data visible, accessible, understandable, linked, trustworthy, interoperable, and secure (aka, VAULTIS) to every other DoD entity. The operational imperative for the Navy is clear: extract warfighting advantage from every BTU in the producible data bbl.

What can our data deliver?

A better reality and a faster decision

Data across the digital domain delivers a force multiplier to all warfighting domains. Consider a plausible maritime operational scenario enabled by VAULTIS data. For that new track – beyond basic track data – picked up via Cooperative Engagement Capability (CEC), the system proactively provides a guide on recent contact movement. As more data sources enrich the track, AI/ML capabilities generate the complete history of the contact (e.g., home airfield, range, operating locations, refueling behavior, behavioral changes based on aircraft loading (e.g., wings dirty or clean)), weapon ranges, and capability of weapons against specific naval or joint platforms. In parallel, the ships' native AI/ML Combat Systems identify effective, least-cost weapons engagement to mission-kill the contact should it become hostile. After deeper analysis, this contact is placed in the prioritized threat stack for the operating area. The data-driven digital systems aggregate at every level across the tactical and operational chain-of-command about each units' specific operating picture. This achieves an "every commander" key operational advantage – data confidence and time to decide.

The importance of time-advantaged, better-informed kill-chain decision-making cannot be overstated. Our peer competitors are already leveraging enormous data volume and accelerating technical capabilities for influence or lethal effects. The advantage of time afforded by exceptional data, leveraged by the Navy's digital domain will allow for:

- **Recognizing a wings-dirty hypersonic weapon shooter earlier.**
- **Operationalizing Combat System AI/ML capabilities to reprioritize the hypersonic shooter to the top of the threat list and tailoring the weapon selected to neutralize it, biasing for speed vice cost.**
- **Identifying adversary behavioral changes in the Information Environment as they pass beyond historical tripwires.**
- **Proactive defensive posture in crew, weapons, sensors, spectrum, and assigned warfare areas.**
- **Redirecting friendly units across the naval tactical grid for intercept or supplemental targeting.**

In these scenarios, the team leveraged afloat and ashore data enterprises and gained 1.5 minutes of extra tactical decision space ; enough time to determine hostility and make successful engagement decisions.

What needs to change in our heading?

Commodity markets compete; Navies engage in lethal combat

To avoid becoming an “oil dinosaur,” the Navy must fix the end-to-end foundation of our operational data architecture and platforms. The future will be an ecosystem where technical capability is quickly added, data are secure and real-time, information is resilient, and warfighting excellence is reliable. The Navy’s digital decision environment must revolutionize now; evolving is too slow. Pockets of excellence – the N1 and N4 digital transformation initiatives, NAVWAR’s Compile to Combat in 24 Hours modernizing Agile Core Services of development, security and operations (DEVSECOPS) environments for the afloat enclave, and NAVSEA’s digital twin – exist. Tough decisions prioritizing resources, policy, and structures rewarding a culture that embraces rapid modernization of our data ecosystem is required. Absent a technical understanding of our data and transport ecosystem requirements, primacy in the digital domain will not be achieved. Simply adding more aircraft, submarines, and ships to a disadvantaged decision environment won’t win. Ten key changes are required today:

Overcome parochial barriers built around resourcing and acquiring last century’s technology and dinosaur C2 constructs to transform existing Flintstones capability to Jetsons for speed, improved cybersecurity, and emerging ML/AI with a sense of urgency.

Align with industry best practices facilitating transport and IC common standards (specifically for sensor data) for end-user consumption.

Recognize and accept we don’t have a complete digital Ao picture. Program managers assume capacity to move their unique data via satellites that is below the mission requirement, or there is insufficient tactical edge storage capacity or processing power to execute advertised information capabilities.

Implement Navy enterprise transport architecture which includes all program requirements for autonomous vehicle and Internet of Things (IoT) devices balanced against the transport bandwidth required to support them.

Assign sole responsibility for producing / maintaining Navy’s enterprise transport architecture (Operational, Systems and Technical Views). The basis for these requirements is being codified in Fleet Cyber Command’s Fleet Design for DoDIN-Navy Operations. Commanders must continually assess and update their data exchange and decision-making information requirements.

Aggressively inject converging transport capacity and data security technologies. Relentless examination of data transport technologies, like laser communications and YouTube’s ability to drive advancement in codec technologies to reduce bandwidth. Transport requirements will change with new missions, when existing missions adjust, or as new technology becomes available.

Significantly increase bandwidth connecting ships in port, at shore teleport sites, and to key facilities that exchange data across ashore cloud providers.

Adherence to open data standards and changing how we develop and deliver content across the enterprise is an absolute. The architecture must support the information and decision environment in the most austere conditions, resilient across the enterprise.

Operators must think critically about information needs and define data requirements in terms of the art of the possible. Articulate “new reality” data and information needs for quick, accurate, and reliable decision-making. For example, a ship’s Navigator may need to combine course and speed data with weather data (from unmanned vehicles, higher-level weather model analytics from the cloud ashore), along with chart data, recent updates to navigational hazards, and intelligence on recent adversary activity in the vicinity. This data synthesis, using AI agents that understand the Navigator’s role and responsibilities, can suggest courses of action in real-time or alert the navigation team of possible hazards to vessel or mission.

People define their roles so that technology and processes can “understand” required context and push data needed to support them. Machines do the repetitive manual data lifting and sifting. Computers search, discover, and aggregate data in new and unconventional ways. Sailors do the mental shifting. AI/ML augments how each person or role processes the information needed.

Excelling in Future Fight where Data is the New Oil...

The Navy can choose this path, it’s in the mission profile. Aggressively addressing resourcing, process, policy, and technology underpinning data – the “new oil” – is necessary for the Navy to attain supremacy in the digital domain and to propel advantage in all other warfighting domains. GPC was here before.

We slowly recognized it, but solutions are possible now to get in front of the threat. Transforming culture is key. Stop wasting time demanding data C2 and start driving a culture that out consumes better data than the adversary as the key to winning lethal combat and avoid becoming a dead dinosaur.

Footnotes

- i** We define digital ecosystem as the technology that underpins data generation, transport, and analysis. Generally, the combination of hardware, firmware, software and operational engineering to sustain the network.
- ii** We define information environment as where and how human decision-making happens.
- iii** DoD Data Strategy (2020)
- iv** Assumptions: Identifying at 200 miles with AI/ML capabilities; twice as far as your previous deployment at 100 miles (before digital modernization of AI/ML capabilities). Assuming the hypersonic weapon carried has an average of Mach 5, your unit has recognized and adjusted posture at 200 miles, which is about 3.1 minutes of flight time for the weapon. Significantly better than what would have been at the 100- mile point which would only provide 1.5 minutes of tactical commander decision space.
- v** Codecs are compression technologies and have two components, an encoder to compress the files, and a decoder to decompress.