AOC ADVOCACY

AOC ISSUE BRIEF:
Non-Kinetic Warfare in the Modern Digital Battlespace

(Note: The following AOC Advocacy Issue Brief was prepared by Booz Allen Hamilton, a Premier Industry Solutions Partner for the AOC CEMAlite Virtual Summit.)

The world in which the U.S. can assume ownership of the best technology, knowing its high-tech approach to war confers a unique advantage, has ended. Competing nations now also have access to critical information and cutting-edge technology, often at low cost, and are moving fast to mature and connect digital assets. The U.S. must move faster—using new ways to integrate technologies and, in doing so, ensure that they are secure, open, agile, and smart.

The rise of the internet has revolutionized warfare through a “network of networks” architecture and the data links that support it have radically increased the ubiquity and velocity of data. The strategic edge inevitably began to move to speed: harnessing information and converting it to action faster than the adversary.

Regaining the Technological Edge

As adversaries grow closer to technological parity with the U.S., national policy is refocusing on the challenges posed by its most powerful geographical foes. In 2018, the U.S. National Defense Strategy stated that our military’s advantage is eroding. Declaring that inter-state strategic competition, not countering terrorism, is now our primary national security concern, DoD is setting a new priority: regaining the military’s technological edge.

As the U.S.’s fight against terrorism focused on conventional operations in which the U.S. could rely on its technology edge, near-peers have evolved their ability to wage an information-centric fight. The technology underlying these information advances is sophisticated and often commercially available—enhanced with private-sector innovations—allowing these competitors to easily and cheaply disrupt existing systems. Because of this, even small states and terrorist organizations can stage cyber attacks, conduct electronic warfare, and use low-cost solutions such as drones to inform their operations or deliver munitions.

The battle is now waged over establishing and maintaining superior information as the lifeblood of all other military operations. And the U.S. must find new ways to achieve and maintain this advantage.

Challenges to Information Superiority

In thinking about how to train, equip, and staff forces for this battle over information, DoD has evolved the concept of information warfare. DoD has set an imperative of maintaining information superiority, allowing the U.S. to "collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." (Source: **Joint Chiefs of Staff**)

However, the U.S. faces challenges to achieving information superiority—some technical, some organizational, including:

1. **The Fragile Information Chain**: Current military systems rely on data networks, including sensor inputs, communications, computing, and so on, creating absolute reliance on a chain of uninterrupted data availability and exchange. If the information chain is broken, or simply delayed by enough time, the systems don't work. These complex systems are vulnerable to disruption, sometimes with little effort.

2. **Lack of True Connectedness**: The ubiquitous data interchange needed in modern war is hampered by the inability of many separate systems to work together, seamlessly and in real time. While some networking of weapon systems has been achieved, it's only been with great difficulty and cost. "Intra" connectedness—within, say, one service or technical ecosystem—is not enough. The goal is to have "inter"-connectedness across all systems, devices, and nodes.

3. **Proprietary Designs**: The speed of conflict, added to the pace of change by the U.S.'s adversaries, demands the ability to rapidly adapt and evolve fielded systems. The closed design practices of many original equipment manufacturers and their resulting proprietary systems and application programming interfaces (API) make this a difficult and expensive proposition. This also makes the goal of interconnectedness more difficult to achieve.

4. **Hardware-Centered Acquisition**: Traditional buying practices are focused on discrete systems and hardware and often emphasize a low tolerance for risk. And innovation (within the U.S. and without) is outpacing DoD's procurement process.

5. **Data Overload**: The practical inability to handle the flood of information being produced by all the devices and sensors on the modern battlefield is well documented. In the future, this already intractable challenge will become insurmountable without revolutionary thinking now.

Incremental change is no longer enough to advance the mission. The U.S. must pursue a new approach for the future of national defense.

A New Approach to National Defense

Information warfare is essential for meeting the challenges of near-peer conflict and DoD needs to incorporate this concept into an all-encompassing vision to comprehensively prepare for the future of war. That vision must include an information-driven, fully integrated conflict space extending across all warfighting domains, which will transcend today's organizational and acquisition boundaries. It must assume that superiority depends on critical networks—communications; intelligence; positioning, navigation, and timing; and equipment—working together even in cyber-challenged, denied, or degraded environments. And it must recognize that information is all-pervasive and is, in fact, the central organizing feature for requirements creation, acquisition, and planning and operations across the force generation lifecycle—from how warfighters are equipped and trained to how they execute in battle.

This is in contrast to information warfare, which has led to strategic moves to align non-kinetic capabilities—cyber; intelligence, surveillance, and reconnaissance; electronic warfare—in coordinated commands but still results in a siloed organization. Information and physical operators remain separated in the absence of a larger vision that drives the entire DoD enterprise to organize itself around information superiority.

That larger vision would be best mastered with acquisitions designed around information challenges rather than hardware and software to be pieced together after fielding. It would require such advances as complete data interconnectedness based on open architectures designed to speed upgrades and adaptability, and ubiquitous use of artificial intelligence (AI) at the edge. These, in turn, require far more than consolidation of commands, as they have implications for the design and data requirements of nearly every system in the force. And once achieved, they create entirely new possibilities for tactical operations in every domain.

The drawbacks of proprietary designs can also be dealt with upfront when acquisition is directed toward optimizing the entire information ecosystem. This approach would allow warfighters, combat vehicles, ships, planes, and autonomous assets to access information securely and use it to make fast, informed decisions—functioning independently, yet in coordination—to advance the mission with increased lethality. In addition, it would also lead to highly resilient systems, unprecedented agility in evolving capabilities against new threats, and breakthrough technology applications. Ultimately, thinking from this more holistic vision will help the U.S. to prevail against near-peer challengers.

Recommendations

Large, complex systems requiring lengthy development and upgrade times need to be replaced with innovative, agile technologies and solutions. DoD needs systems designed to be open, smart, resilient, and secure, and capable of operating at the tactical edge. Moving forward, DoD should focus on implementing the following central attributes into warfighting capabilities:

1. **Open:** Proprietary architectures can't accommodate rapid upgrade cycles. DoD's data must be taken out of proprietary silos so information that flows between the wide array of devices in the battlespace—from sensors in drones to heads-up displays on warfighters to GPS receivers—can be fully connected and integrated. Private-sector technology provides ways to construct open frameworks so that:
   - Components and software modules can be switched in and out to fulfill rapidly changing requirements, missions, battlefield conditions, and tech advances.
   - Technologies are interoperable and plug-and-play.
   - Open architectures, data platforms, and APIs are understandable, usable, and accessible to facilitate data integration.

2. **Smart**: Information must be delivered as intelligence giving warfighters real-time context for the precise mission and situation. Yet data is pouring in faster than military and national security operations can analyze it, requiring new thinking to aggressively triage the data and quiet the noise. New computing paradigms need to be rapidly incorporated:
   - Machine learning (ML) and other forms of AI, trained and continuously refined, can accomplish routine tasks and substantially aid humans in resolving critical ones.
   - Developers must integrate data science expertise with in-depth mission and domain knowledge to achieve mission success.

3. **At the Edge:** Traditional communications channels and networks can be jammed or otherwise denied, which can impede command and control; processing, exploitation, and dissemination of intelligence; and situational awareness. Military systems need new capabilities to operate at the edge:
   - Networks and processing must be resilient against electronic warfare attack or other disruption.
   - Systems must operate without a cloud or network, empowering the user with increased situational awareness and real-time decision making.
   - To quickly develop systems that are agile and cost- effective, we must create ecosystems using smart devices already in the field.

4. **Resilient and Secure:** Open platforms, ML, AI, and edge processing and networks are being subjected to increasingly sophisticated cyber attacks and other electronic threats. Adversaries have invested heavily in emerging technologies and can disrupt these networks using cheap, commercially available equipment.
   - DoD must embed advanced cyber protection into solutions as they are developed, rather than bolted on later.
   - Cybersecurity must be continually refined and updated through agile processes.
   - Data scientists must work with machines, augmenting human expertise with advanced AI, to protect algorithmic models from spoofing and other attacks.

To learn more about this topic, visit **BoozAllen.com/DigitalBattlespace.**

Booz | Allen | Hamilton®