

## Playing Leapfrog - Getting Ahead in Future Warfare

“The art of war is simple enough. Find out where your enemy is. Get at him as soon as you can. Strike him as hard as you can, and keep moving on.” Warfare isn’t as linear now as Ulysses S. Grant had expressed in his time. In today’s battle, the enemy and the fight are both everywhere and nowhere. Yet the goal remains “to deter and defeat adversaries across multiple scales of conflict intensity.”<sup>1</sup> America’s technological, strategic, and operational edge has eroded as the result of nearly two decades of fighting at the lower end of the conflict spectrum. During that time adversaries have invested in competitive capabilities, acquired inexpensive, commercially-available technologies, or simply stolen them. Consequently, the U.S. must be ready to fight in a contested environment, where every potential battle and domain requires physical or virtual access. Addressing the narrowing capability gaps must be a priority. However, the priority should not be thought in terms of keeping up with the Joneses, but getting ahead of them. How? By going simpler, smarter, and smaller.

### Simpler

Modern warfare cannot be thought of solely as material advances, but also doctrinal and organizational changes. For example, modern warfare is often made even more complex by complicated authorities, rules of engagement, and capabilities. The ability to resource, train, plan and conduct maneuver through cyber and the electromagnetic spectrum, for example, would be bolstered by updating Title 10, 47 and 50 authorities. The artificial boundaries across these authorities hinder reconnaissance, targeting and maneuvering across the full range of military operations. As a result, constrained commanders and troops have had to use workarounds and less precise information at the risk of greater collateral damage. Likewise, industry partners have been hampered in developing multi-domain, multi-functional and multi-modal advanced technologies. Worse still, adversaries can and do exploit such limitations.

The need for simpler, especially in terms of being more user-friendly, is not lost across the armed forces. The Army has been exploring building greater simplicity into communications systems to enable soldiers to operate networks and communications systems themselves. “This complexity is not only a burden for the soldiers in the field operating them, but it is also a burden for sustainers and maintainers that have to work on them for the next forty years as the Army looks to keep programs of record around for several decades.”<sup>2</sup> Even standardizing the Army’s computer systems across 400 units, aimed at simplifying training, maintenance, and operations, in advance of the 2019 launch of the next generation Common Operating Environment, has been complicated by cost, scale and scope.

Simplification may also be applied to how national security organizations approach projects and problems. There have been a growing number of public-private partnerships and the federal government has made some progress in adopting commercial best practices when viable. Both

---

<sup>1</sup> Brad D. Williams, “DARPA’s ‘mosaic warfare’ concept turns complexity into asymmetric advantage,” *Fifth Domain*, August 14, 2017, <https://www.fifthdomain.com/dod/2017/08/14/darpas-mosaic-warfare-concept-turns-complexity-into-asymmetric-advantage/>.

<sup>2</sup> Mark Pomerleau, “Army seeking network simplicity,” *Army Times*, August 9, 2017, <http://www.armytimes.com/show-reporter/technet-augusta/2017/08/09/army-seeking-network-simplicity/>.

approaches leverage private sector research and development investments. However, the Department of Defense would also benefit from thinking more like the private sector. To get better, faster, cheaper, and simpler solutions, senior leaders down to project managers would need to address problems in a manner after Google or Amazon, across the organization's structure and with multiple perspectives, instead of how traditional programs currently do.

By simplifying authorities, processes, objectives and technologies, the U.S. would better position itself to enable leverage and reduce risk, operate with agility, invest in advanced technologies, and jump ahead of peer states who focus on longer-term strategic investment and centralized decision-making.

### Smarter

“In 21st century warfare, war is cognitive as much as it's kinetic.”<sup>3</sup> Cognitive technologies and autonomous systems have two significant advantages. They are simply able to do what humans cannot, and thereby compensate for an undermanned and underprepared force structure. By leveraging both the artificial and autonomous in conflict, the time associated with an OODA [observe-orient-decide-act] loop could be reduced to near-real time. Continuous learning technology can also perpetuate innovation, allowing integration into larger systems and hardware (think of Tesla cars that learn to avoid potholes and share that information). The future of warfare will require advanced human-machine interfaces to keep up with the combined speed and scale of threats, adversaries and technologies. “It is not sustainable to throw more widgets, platforms and sensors at problems. We have to look at human-machine teaming so that computers can access data, secure data and transport data. This will allow us to get back to the heart of what we do – analysis and decision making.”<sup>4</sup>

Making the force structure smarter is equally important. The Joint Force will still need to identify variables, analyze intelligence, provide context (historical, cultural, socio-economic, linguistic), and apply a moral compass to critical decisions and operations. Smarter technology might maximize agility and efficiency, but “Too little human control, too soon, and we risk compromising transparency and safety. Too much human control, and we'll suffer at the hands of tight enemy OODA loops.”<sup>5</sup> In either case, humans choose to initiate hostilities, act upon information, and make lethal decisions. “The technology enables what remains a contest between human brains.”<sup>6</sup> Simply put, there are certain things machine cannot – or should not – do.

Cognitive technologies and autonomous systems are certainly game-changing. The Third Offset strategy investments in artificial intelligence and autonomy are a start. However, “Our adversaries have invested heavily in technologies to deny us the superiority we have come to rely

---

<sup>3</sup> Mark Pomerleau, “‘Information’ is playing outside role in warfare,” *Defense News*, August 4, 2017, <https://www.defensenews.com/intel-geoint/2017/08/04/information-is-playing-more-outsized-role-in-warfare/>.

<sup>4</sup> Kris Osburn, “Air Force 3-star: ‘algorithmic warfare’ needed for future ISR, combat op,” *Defense Systems*, August 31, 2017, <https://defensesystems.com/articles/2017/08/31/air-force-it-drone.aspx>.

<sup>5</sup> Gen. John Allen, USMC (Ret.) and Amir Husain, “On Hyperwar,” *Proceedings*, July 2017, <https://www.usni.org/magazines/proceedings/2017-07/hyperwar>.

<sup>6</sup> Gideon Grudo, “Intel challenges and the holy grail,” *Air Force Magazine*, March 3, 2017, <http://www.airforcemag.com/Features/Pages/2017/March%202017/Intel-Challenges-and-the-Holy-Grail.aspx>.

upon.”<sup>7</sup> The trick then is not to duplicate capabilities, but to create new, distinct ones, and be smarter operators who know not just how to win the game, but change it.

### Smaller

Thinking big is an American mindset, but recent trends in technology have been to go “small.” What’s needed is achieving significant military advantages through “small” concepts that can mean less manpower intensive more deployable, modular, scalable, and even less expensive. Just look at smart phones that combined radios, computers, libraries, cameras, and more into a pocket-sized device. Drones are another prime example. In 2016 the Pentagon tested 103 Perdix drones each 30 centimeters in size. Released from three F/A-18 Super Hornets, the micro drones swarm demonstrated collective decision-making and adaptive formation flying. The test showed how “teams of small, inexpensive, autonomous systems...perform missions once achieved only by large, expensive ones.”<sup>8</sup> All of the services are actively scouting swarm and anti-swarm technologies to increase situational awareness, develop denial and deception tactics, and create persistent reconnaissance capabilities.

The same is true with satellites. NASA has been using CubeSats, which are cheaper, lighter, easier, and less risky to get into orbit. DARPA has also been working on low-earth-orbit micro-satellites to enhance ISR capabilities to be “persistent, survivable and available on-demand for tactical warfighting applications.” Technologies and sub-systems are under development for smaller and cheaper military satellites to provide secure and high-bandwidth RF, as well as optical inter-satellite communications links. Other space missions of the future could include spacecraft like the experimental X-37B, a smaller (29 feet long and 15 feet-wide wingspan) and cost-effective alternative to the Space Shuttle. The X-37B is believed to be testing “new military space satellite technologies including ion thrusters, and optical and radar-based sensors designed to spy on objects on the ground or other satellites.”<sup>9</sup>

Even the modernization of the U.S.’s nuclear arsenal is investigating smaller variable yield bombs that can target specific neighborhoods or larger areas. Vice Chairman of the Joint Chiefs of Staff, Gen. Paul Selva, noted that “the future of nuclear deterrence lies, at least in part, in smaller nuclear weapons that the United States might actually use.”<sup>10</sup> Russia possesses smaller, tactical nuclear weapons that it employs in exercises and had threatened to use them if NATO forces attacked pro-Russian forces in Eastern Ukraine.

Creating unique advantages may well come by redefining “shrinking” capabilities, but getting ahead of threats and adversaries will still require looking at the big picture.

---

<sup>7</sup> Gideon Grudo, “Widening the C2 Highway,” *Air Force Magazine*, July 2017, <http://www.airforcemag.com/MagazineArchive/Pages/2017/May%202017/Widening-the-C2-Highway.aspx>.

<sup>8</sup> Jasper Hamill, “Swarm-mongers; U.S. military unleashes swarm of tiny intelligent micro-drones,” *The Sun*, <https://www.thesun.co.uk/news/2578439/u-s-military-unleashes-swarm-of-tiny-intelligent-micro-drones/>.

<sup>9</sup> Kyle Mizokami, “Air Force's Secret Space Plane Set to Blast Off Again,” *Popular Mechanics*, September 5, 2017, <http://www.popularmechanics.com/military/research/a28068/air-force-x-37b-spacex/>

<sup>10</sup> Patrick Tucker, “US Military Eyes New Mini-Nukes for 21st-Century Deterrence,” *Defense One*, August 3, 2017, <http://www.defenseone.com/technology/2017/08/us-military-eyes-new-mini-nukes-21st-century-deterrence/139997/>.

While becoming simpler, smarter, and smaller can be done without reduced effectiveness or capabilities, there are prerequisites. A first consideration is rationalizing the budget process. Secretary of Defense Jim Mattis cautioned that the “Pentagon would be hamstrung in dealing with new advances in electronic, space and drone warfare if Congress passes another stop-gap budget measure this fall.”<sup>11</sup> He further warned that holding spending to current levels would leave the department unable to deal with emerging threats. Second, progress is needed in agile acquisitions to allow for faster, scalable, adaptable, and cheaper solutions and services, as well as flexibility as requirements change over the course of a project. Third, the government must get better at sharing. For example, electronic warfare interoperability has shared databases, but not sharing capabilities, across services. The same goes for partners. “Given that the U.S. rarely fights alone, its capabilities have to be compatible or at least shareable with allies in some way” to avoid being detected and denied as an adversary.<sup>12</sup>

Changes have to be made to better anticipate and shape the future, while avoiding the reactive mode of recent years. The national security community must think in time holistically; focusing on both the present and the future, on the whole as well as the component parts. Addressing immediate threats is necessary, but peers and adversaries didn’t develop by leaps and bounds by looking at the near-term. “In the future fight, we must evolve from a system defined by stovepipes and parochialism. Future commanders will have a profound breadth and depth of information and access to capabilities providing cross-domain effects, maneuver, and fires. Provided in a federated package of solutions, however, no matter how well executed, our joint capabilities will be vulnerable to a peer adversary with a more united solution. Now is the time to establish a shared visualization and understanding of what the future U.S. military will look like.”<sup>13</sup>

This all that means getting ahead...or risk falling behind.

---

<sup>11</sup> Travis Trittem, “Jim Mattis calls looming stop-gap budget ‘as unwise as can be’ for military,” August 15, 2017, <http://www.washingtonexaminer.com/jim-mattis-calls-looming-stop-gap-budget-as-unwise-as-can-be-for-military/article/2631569>.

<sup>12</sup> Mark Pomerlau, “How the Army and Marines are interoperating in electronic warfare,” *Defense News*, August 11, 2017, <http://www.defensenews.com/show-reporter/technet-augusta/2017/08/11/how-the-army-and-marines-are-interoperating-in-electronic-warfare/>.

<sup>13</sup> Gen. Robert B. Brown and Gen. David G. Perkins, “Multi-Domain Battle: Tonight, Tomorrow, and the Future Fight,” *War on the Rocks*, August 18, 2017, <https://warontherocks.com/2017/08/multi-domain-battle-tonight-tomorrow-and-the-future-fight/>.