AMERICAN FOREIGN POLICY COUNCIL

Gaming To Victory: Synthetic Training For Future Combat

November 14, 2017 **Jennifer McArdle** *War on the Rocks*

Related Categories: Cybersecurity and Cyberwarfare

It looked like a video game. From the comfort of a living room couch, with TV dinners in hand, families watched as precision-guided munitions rained down with seemingly perfect accuracy on Iraqi military and civilian targets. It was Jan. 17, 1991 - the start of Operation Desert Storm - and the combination of camera equipped high-tech weaponry and night vision equipment provided viewers an action-packed front-row view into the coalition's air war. What had seemed like science fiction was now a reality.

The Persian Gulf War is considered by some to be the first information war - the war that demonstrated the lethality of U.S. Department of Defense's information communication technology investments during the Cold War. The fusion of advanced microprocessors, new sensor based technology, and satellite communications, promised to improve battlespace awareness - potentially eliminating the fog of war. Likewise, precision-guided munitions would presage a more cost-effective future where a single munition could be deployed against a single target, or as one manufacturer noted "one target, one bomb."

However, despite this climate of intense optimism, the fog of war did not dissipate. As Gen. Walt Boomer, who led the marine assault on Kuwait, noted, "the intelligence stunk." He did not have the intelligence picture that he desired. Moreover, only about 80 percent of precision-guided munitions accurately hit their targets. Indeed, to more skeptically minded strategists, the Gulf War was only partially successful at translating technological concepts into battlefield victory. Friction remained.

Notwithstanding these limitations, Desert Storm did act as a formidable demonstrator for future war. Adversaries and aspiring peer competitors watched as the American-led coalition quickly dismantled the fourth-largest standing army in the world. At the same time, they took note of America's intense and growing dependence on information communication technology. The U.S. military's performance during the Gulf War was carefully scrutinized overseas, and acted as a catalyst for Chinese - and later Russian - efforts at military modernization and reform. Information communication technology came to be viewed both as a force multiplier and as a potential source of vulnerability for asymmetric exploitation.

While the U.S. military has experienced some networked - cyber, electronic, and information - attacks in battle, it has yet to fully face a near peer competitor, like Russia or China, in this domain. In the absence of a rich networked-infused battlefield experience, realistic training provides the best source of preparation prior to the crucible of high-end combat. The United States and its coalition partners should continue to modernize training, injecting greater realism into the military's training environment to best reflect current and future threats. This includes teaching all warfighters - not just cyber mission forces - to fight and win in a contested networked battlespace. Yet, as the military works to push the limits in training, live training will not suffice to provide the high-fidelity training option that the military requires. The synthetic training environment - computer-generated forces in a virtual environment - is essential to provide the requisite fidelity to mimic future networked combat.

Training for Networked Threats

The Army, Navy, Air Force, and Marine Corps are beginning to conceptualize how they can best plan to prevail within this brave new world. But the adaptive training process remains somewhat sluggish.

As one former senior U.S. Air Force officer told me, "the training in that realm is not fully integrated. It is a complementary element of some exercises, but it is not often the primary learning objective." Likewise, the Army's former Electronic Warfare Division chief Col. Jeffrey Church noted that the Army was "behind," before assuring that, "we are taking steps to get caught up." These views were echoed by members of the U.K. and Australian air forces when commenting on their own services, stating respectively that "it is a little immature" and "a shortfall we are working towards."

The still partial nature of this evolution in combat training is best demonstrated by the role of cyber operations in Red Flag - the U.S. Air Force's premier combat training exercise. While Red Flag does include a cyber component, it is often employed in parallel to the live flying training exercise. As two former senior Air Force leaders explained, the computer network defense exercise is often taking place in a separate facility and is thus, "not fully integrated across the fight."

Yet, the outcomes of the computer network defense exercise are often combined into the live flying - or a live fire - exercise at a later point. Networked, particularly cyber, injects are done via "white carding" - the literal use of a note card to inject friction. When a simulator or a live exercise can't emulate a scenario, an instructor is able to use a note card as an inject tool. The trainees are meant to respond as if the inject happened, and a debrief happens later. And while this does provide future warfighters with some insight into how their platforms may be impacted in the event of a networked attack, the lack of realism precludes them from experiencing and subsequently responding to that attack. This is somewhat problematic, as training should provide experiential learning - the type of learning that translates into quick reflexes, critical thinking, and system-based interactions on the battlefield.

The lack of networked integration into live exercises, however, is often for good reason. Indeed, as one former senior Air Force leader admitted, if the computer network defense operators failed, the Air Force does not want to risk crashing the entire Red Flag exercise. Similarly, such integration is largely not occurring because of safety risks. Live exercises occasionally take place near population centers. The use of electronic weapons may compromise civilian use of the electromagnetic spectrum, which can have knock-on effects for mobile phone or television use. Additionally, a cyber-attack on a military platform could have unintended consequences, potentially placing the warfighter and platform at risk. Finally, those same networked attacks on weapon platforms endanger exposing platform vulnerabilities to ever-curious adversaries.

The hesitation to inject networked effects into a live environment is understandable, but all the risks previously outlined could be circumvented by driving the military to rely more on high-fidelity synthetic training for networked operations. As one former Royal Air Force officer recently confided, "the cyber environment is going to become as important for realistic training in the synthetic world as an accurate representation of weather events."

Synthetic Training: From Information Assurance to Mission Assurance

It seems self-evident that any complex system with high interconnectivity - to include military platforms - will have cybersecurity vulnerabilities. Indeed, the same capabilities that provide the U.S. military with a technological edge over certain key competitors - for instance, electronic attack, communications, or sensor suites - also present unique cybersecurity risks. U.S. military systems can fall prey to adversary computer network operations against software, hardware, or firmware for the purposes of espionage, sabotage, or subversion. This threat, moreover, is amplified in the joint environment, as all joint functions are dependent on communications systems.

Information security professionals often refer to the "CIA triad" as the guiding construct for organizational information security. These practitioners work to ensure the (C) confidentiality, (I) integrity, and (A) availability of data within a system. While this model is typically used to guide information security policy, it also provides a useful starting point to extrapolate how networked effects could be introduced into the military's synthetic training environment.

Adversaries will work to undermine the confidentiality, integrity, and availability of military platforms and their communications backbone. In combat, the networked attacks that the military will likely face are availability threats - distributed denial of service or jamming. In a scenario reminiscent of Peter Singer and August Cole's *Ghost Fleet*, adversaries could manipulate the microelectronics supply chain or employ a computer network attack to sabotage communication networks or key weapon systems. The confidentiality of data on weapon system capabilities and vulnerabilities could be revealed via computer network exploitation. Additionally, by accessing command and control networks, adversaries could glean intelligence on operational planning and decision-making. Finally, the integrity of system information - via, for instance, optical, thermal-infrared, laser, or radar sensors - could be compromised via spoofing or the insertion of false information. Such an attack on the integrity of the information itself could undermine confidence in system information, thus causing a general loss of trust in battlespace awareness and command and control.

Such scenarios are entirely plausible. Indeed, both Russian and Chinese military strategies and operational concepts emphasize utilizing asymmetric networked attacks in both peace and war to gain a geostrategic edge. From the use of cyber and information operations in the 2008 Russo-Georgia War to the blending of electronic, information, and cyber operations in Ukraine - Russia is preparing to fight and win in a networked environment. The Russian military employs networked operations to "deceive, delay, and disrupt," often favoring methods that allow them to hold targets at risk - as evidenced by the presence of BlackEnergy malware in key European targets. The Kremlin, likewise, has adroitly employed low level networked operations - jamming, disinformation, and distributed denial of service attacks - to sow confusion and break down adversary decision-making and command and control networks. And while Russian capabilities may not be comparable, in the aggregate, to those of the United States, what really matters is the localized correlation of force in certain key regions. For instance, as the Russian military expert Michael Kofman told me, "in a fight on the Russian border, Russia could prove better than a peer." Similarly, China reportedly plans to fight and win "informationized local wars" in its near abroad, employing computer network attacks to target critical command and control and logistics nodes, electronic warfare to suppress and deceive adversary networked systems, and information operations for propaganda and disinformation purposes. Such measures fit squarely within Beijing's strategy of "winning without fighting."

While it is most likely impossible to entirely deny an adversary the ability to spoof or penetrate a system, our goal should be to sustain military operations in spite of these networked attacks. A 2015 RAND report highlights two factors that determine the impact of an attack on a system. The first, how gracefully a system degrades due to an attack, is largely a function of technical design. However, the second, the effectiveness of mitigation measures - either proactive or reactive - can be partially resolved through adequate training and education. This requires a paradigm shift away from information assurance to mission assurance. Mission assurance works to buttress mission success, even if some supporting elements fail. The emphasis is then placed on finding a new or creative route to victory, despite a denied, degraded, or spoofed environment.

Yet, creativity and experimentation often requires practice, which the synthetic environment is uniquely suited to provide. Much like the time-loop in *Edge of Tomorrow: Live. Die. Repeat* that transforms what was a suicide mission against a superior alien force into a more even confrontation - synthetic training provides a virtual Groundhog Day combat training environment. As Army Col. (ret.) Peter Newell noted, "gaming provides an ability to actually put yourself in the scenario, go through it and see it. Back up, change the scenario, go through it a different way... There are an infinite number of scenarios I can run soldiers through, because it's not about doing it per se, it's about having thought through it."

A Day Without Cyberspace? Overcoming Challenges to Adoption

In the early 2000s, the U.S. military began a campaign to better understand the effect of operations without space based assets. Dubbed "A Day Without Space" the awareness campaign was designed to educate commanders and warfighters - across the services - on the warfighting impact of the loss of satellite communications. As a result, a mandate emerged for degraded communications and GPS loss to be integrated into training exercises. Yet, after a while, as one former U.S. Air Force senior leader noted, commanders argued that while they understood the challenges, their first perceived priority was to train their warfighters for their more everyday missions.

While today it is relatively easy to simulate the loss of GPS, and more generally the loss of space based assets, simulating the loss of cyber enabling assets is far more challenging. Networked effects, as previously mentioned, can manifest in multiple ways and likewise, have the potential to have cascading effects throughout a system. Indeed, as another Air Force senior leader fretted: "How do you have a day without cyber once you are airborne? Depending on what your adversary does maybe it is just downing the plane and you must eject. Or, maybe, the airspace network goes out and then you go back to a non-networked 1970s air-fighter and your integration and effects are diminished."

Today, we are about where we were in the early 2000s when the military first grappled with a day without space. While the military acknowledges the systemic risks to military systems from adversary networked operations, the military has yet to develop a similar campaign around cyberspace. And like the challenges associated with "A Day Without Space," the current limitations to conceptualizing networked based injects are not necessarily technical - they are organizational and operational. The military still struggles to adjudicate training for many different mission types. This is partially a constraint of time - training scenarios and potential threats are far more numerous than a service's actual capacity for training. However, it is also a function of the military’s geographic focus over the past 15 years. The protracted wars in Iraq and Afghanistan have placed a combat training premium on counter-insurgency and counter-terrorism - two mission areas that do not necessarily prioritize networked operations. As a result, the United States has yet to face a peer competitor whose use of networked operations act as a driver for changes in acquisitions, doctrine, organization, leadership, personnel, or training and education. Indeed, as one former U.S. Air Force leader stated, "we haven't had our nose bloodied yet... We won't adapt until we are forced to adapt. Or we will adapt gradually."

Driving the military towards greater levels of synthetic training will prove challenging. Over the last two years, U.S., U.K., Australian, Canadian, and French warfighters tasked with synthetic training all lamented, during private conversations, that some service-level cultural change needed to occur in order for synthetic training to be equally weighted against live training. This bias towards live training is understandable - in the same way that Air Force cadets around the world retain a certain bias against unmanned systems. The virtual and constructive environment will never be able to fully replicate the sensations derived from the dirt, dust, and sweat of the physical world. Somewhat paradoxically, however, it may well turn out that when it comes to prepping for future high-end conflicts, the synthetic training environment proves more "realistic" in some regards.

Defense bureaucracies are slow moving beasts. Yet successful innovation in warfare hinges upon adaptation - the type of adaptation that anticipates and subsequently responds to meet the challenges of future wars. The key then, as one former Air Force leader stated, is to structure those networked effects so they resonate generally with the force - it can't be viewed simply as an add on. "It needs," he concluded, "to reshape the way we execute training."

Jennifer McArdle is an Assistant Professor of Cyber Defense at Salve Regina University, a Fellow in Defense Studies at the American Foreign Policy Council, and a PhD candidate in War Studies at King’s College London. She is a 2017 recipient of the RADM Fred Lewis I/ITSEC doctoral scholarship in modeling and simulation.