The "Disruptive World" and the Integrated Force: Readiness through LVC

Jennifer McArdle

Good afternoon everyone. First, I'd like to thank the Royal Australian Air Force (RAAF) for hosting me to speak to this distinguished audience. I realize that I am standing between you and lunch, so I will do my best to hold your attention for the next thirty minutes.

On 17 November 2011, Gen. Martin Dempsey, then chairman of the US Joint Chiefs of Staff, asked a question, "What's after joint?" Six years later the US Army answered with their multi-domain battle concept, while today, the US Air Force (USAF) is finalizing their concept of multi-domain command and control. In summary, multi-domain battle seeks to move beyond services as organizing constructs for operations, to instead harness joint experience to produce integrated effects through multiple domains—air, land, sea, space, and cyber.

This past June, speaking at the Australia Strategic Policy Institute (ASPI), Vice Admiral Ray Griggs, the Vice Chief of the Defence Force, confessed that—to him, joint is now a limiting descriptor. And while multi-domain struck him as a bit of a faddish terminology, the key, he noted, to the future force is the integrated force— "integrated at an organizational level and integrated technically and culturally." Vice Admiral Ray Griggs advocated for a One Domain concept, that moves away from service and domain level silos.

Terminology aside, an overarching theme cuts across these different ideas—it is the aim to seamlessly work between services and domains by focusing on the desired effects that one wants to bring to bear on an adversary, rather than on a given service or domain. This should give warfighters and decision makers increased options, while multiplying adversaries' challenges. Additionally, there is a recognition that technology on its own will not be a panacea; that the way militaries choose to fight—seamlessly integrating kinetic and non-kinetic operations—will also influence the outcome on the battlefield. It is to be a truly integrated future force, across service, domain, and kinetic and non-kinetic operations.

In today's operating environment, such integration is necessary. Over the last decade, potential adversaries—China, Russia, Iran, and North Korea—have invested heavily in a range of military capabilities with the intention of depriving the U.S., allies, and coalition partners the capacity to project power into their near abroad. Labeled anti-access/ area-denial (A2/AD), these capabilities afford their owners a degree of strategic depth by raising the risk and cost of intervention. In tandem, these capabilities have provided cover for other more revisionist actions. Russia and China, in particular, have manifested an irredentist predilection for "gray zone" approaches—testing US and allied security commitments and platforms through "salami slicing" tactics that do not in and of themselves amount to a casus belli, but nevertheless threaten to change the status quo in the region. Moreover, potential adversaries have recognized that conflict is not solely defined by the exchange of fires—that shaping the information environment through "lawfare," economic statecraft, the crafting of historic or political narratives, and information operations can also yield strategic geopolitical ends. While these asymmetric strategies may differ in their capabilities or tactics, they all rely heavily on cyber, electronic, and information operations. Our militaries must be able to fight in—and through—an increasingly contested and complex environment. And likewise, they must be able to bring those same cyber, electronic, and information capabilities to bear as force multipliers for more lethal effect.

So, the question becomes, how should militaries fight as an integrated force in these contested environments? And how should they train for that?

Modeling and simulation—in particular, live, virtual, and constructive (LVC) training—provides the environment necessary for more integrated training, all while providing a high-fidelity rendition of the military's current and future operating environment. There are three types of techniques that militaries use for LVC:

1. Live: Real people operating in a real environment
2. Virtual: Real people operating in a simulated environment; and
3. Constructive: Simulated people or equipment operating in a simulated environment.

LVC entails linking live aircraft with manned simulators in the "virtual" world and computer-generated "constructive" forces. LVC is increasingly beneficial because today the live training environment is not conducive to many of the training needs of fifth generation platforms—like, for instance, the F-35 Joint Strike Fighter. However, and most importantly for this discussion, the live training environment fails to integrate with fidelity cyber, electronic, and information operations.

While nothing can obviously replace the sensations derived from the dirt, dust, and sweaty adrenaline of the live environment; in some cases, paradoxically, it may well turn out that when preparing for a future contested and complex battlespace, the synthetic training environment may prove more realistic. Indeed, to truly achieve an integrated force along the lines of multi-domain or one domain battle—or even Plan JERICHO for that matter— training will need to be increasingly pushed into the virtual and constructive environment.

I'll now try and spend the rest of my time more fully explaining why, and the remainder of my presentation will proceed in four parts:

1. I'll first discuss the need for military forces to train to fight in—and through—a contested environment saturated by adversary cyber and electronic operations. I'll also detail how the military and the defense industrial base can begin to conceptualize injecting cyber and electronic effects into the synthetic training environment.
2. I'll then discuss why it is necessary for the military to train for integrated offensive kinetic and non-kinetic operations, looking specifically at some of the challenges unique to integrating offensive cyber operations with more conventional operations. I'll detail some interesting initial work that integrates kinetic and non-kinetic synthetic environments.
3. I'm then going to switch over and look more broadly at today's information environment—in particular, how we are starting to see cyber and electronic operations converge with more traditional information operations—military information support operations (MISO), military deception (MILDEC), and psychological operations (PSYOP)— alongside social media, big data, and artificial intelligence to influence the information and cognitive dimensions of the battlespace. I'll talk a bit about why training for these types of operations must occur synthetically, and how the environment needs to evolve to provide the warfighter that experiential learning prior to combat.
4. Finally, I'll conclude by exploring how the synthetic training environment is uniquely suited for the military to experiment—to design new operating concepts and tactics, techniques, and procedures for this future battlespace.

Training to Fight Through a Contested Battlespace

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

USAF and RAAF with a technological edge over certain key competitors—for instance, electronic attack, communications, or sensor suites—also present unique cybersecurity risks. As the USAF Scientific Advisory Board noted last year, these vulnerabilities exist even in systems which lack Internet connections. 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 when operating as an integrated force, as all integrated 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 adversaries may seek to undermine military platforms and systems.

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. Likewise, adversaries could manipulate the microelectronics supply chain or employ computer network attack to sabotage communication networks or key weapon systems. These same methods could also be used to virtually illuminate assets, so that adversaries can identify where those same assets are hidden. 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. Synthetic training must evolve to include training for these types of cyber-attacks. But how?

Exactly how a system or platform would be disrupted by a cyber-attack depends on the details of that system. This requires a deep understanding of how the system works—for instance how a SA-400 surface to air missile works, but also how the system parameters are set and how the system fits into the broader network. And this understanding would need to evolve as the platform changes—with each software update, each patch, each new interconnection, etc. Moreover, cyber exploits are evolving—they aren't static—they reflect the tacit knowledge learned by the hacking community. What they choose to target and how they have structured an exploit will have different effects on a system. So, it may be impossible to model all the possible effects of a computer network attack on a system.

However, that doesn't mean that developing a suite of simulated cyber injects that may be slightly divorced from reality is not helpful. Indeed, given the number of ways that a computer network attack can impact a system, the goal should be to get the trainee to trouble shoot a diverse range of effects and creatively identify ways to maintain mission assurance despite the attack. How should a pilot react if their platform's GPS coordinates no longer seem to reflect reality? What should they do when the primary interface between their aircraft and their weapons are sabotaged? What if their fire control radar seems to be feeding in faulty information that doesn't correlate with previous information of the described mission? In some cases, the pilot may be able to trouble shoot and carry on with the mission, in other cases they may need to turn back. They should be trained to each of these ends. We need to start to think about how we can evolve our suite of synthetic training options to include these scenarios and others.

Training for Cyber and Electronic Operations as Force Multipliers

On 6 September 2007, Israeli F-15 Eagles and F-16 Falcons bombed a North Korean- designed nuclear facility in Syria. Even though these aircraft are far from stealthy, Syria's Russian-built air defense network showed nothing as they penetrated Syrian airspace. So, what happened? The images on Syrian radar screens weren't real—they depicted what the Israeli Air Force had injected there through cyber means. While there are various theories on how the Israeli's may have penetrated Syria's air defense network—for instance, transmitting malicious packets through the air defense system's radio-frequency (RF) signal via a stealthy unmanned aerial vehicle (UAV)—one thing is clear, the Israeli Air Force had effectively integrated kinetic and non-kinetic operations for maximum effect.

More recently, from late 2014 through 2016, Russian malware was covertly implanted in a legitimate Android application developed for the Ukrainian artillery. The original application, used by over nine thousand Ukrainian artillery personnel, enabled artillery forces to more rapidly process targeting data for Soviet-era D-30 Howitzers. The deployment of the malware likely facilitated Russian reconnaissance and superior targeting of Ukrainian artillery units. Indeed, a recent assessment by the International Institute for Strategic Studies (IISS) estimates that 15 to 20 percent of the Ukrainian D-30 inventory had been lost in combat operations.

It's obvious that cyber and electronic operations can be used as a force multiplier—or a support function—in conflict. Yet, effectively integrating non-kinetic and kinetic operations is no easy task. Current LVC training for cyber operators focuses entirely on the cyber aspect of operations and largely ignores the broader operational picture—placing it at odds with the realities of cyber support on the battlefield. Likewise, conventional warfighters tend to see cyber as a strategic capability, rather than something that can also be applied tactically as part of a range of mission effects. Few training opportunities—if any—exist for the conventional warfighter to build an understanding of how they may best leverage cyber capabilities at the tactical or operational level.

The USAF acknowledges that a multi-domain force requires them to produce airmen that understand how to combine air, space, and cyber together for more lethal effect. Yet, a gulf exists between those cyber warriors that are assigned to cyber protection teams and those assigned to support conventional forces as combat mission teams. The U.S. Army's Cyber Support to Corps and Below (CSCB) initiative and 2017's exercise RED FLAG's non-kinetic duty officer course show some promise towards combined cyber-kinetic arms training. However, much more needs to be done. New training and tools must be developed to support this type of training.

For instance, one could imagine a scenario where a cyber combat mission team has gained access to an adversary's command and control center—they are now able to monitor how the enemy chooses to deploy air power in a given theater of operations. If the cyber combat mission team's connection is via a fiber optic cable, it is in their interest to ensure that friendly forces do not damage that cable during operations. However, that same fiber optic cable could run across a bridge that friendly forces seek to deny to an adversary. Coordination—and integration across the force—needs to take place, as bombing that bridge could also deny the cyber combat mission team vital mission intelligence.

However, perhaps more importantly than just designing combined arms cyber-kinetic scenarios, warfighters must develop a deeper understanding of the strengths and weaknesses that cyber brings to the fight—an understanding that could be developed through integrated synthetic training. Cyber brings unique attributes that differ significantly from more conventional weapons.

For example, first, the timing and sequencing of non-kinetic and kinetic attacks is challenging. Targets cannot necessarily be hit at a moment's notice via computer network attack. Cyber

operators often take months or even years to work through the cyber kill chain: from reconnaissance to exploit development, delivery, vulnerability exploitation, malware installation, remote manipulation or command and control, to finally achieving their objectives. Likewise, the more critical a system is to a potential adversary, the more likely it is strongly protected, and thus the longer it will take to penetrate. However, once a system is penetrated and exploited, the effects of a cyber-attack can be near instantaneous, requiring rapid reaction on the part of more conventional warfighters for synchronization.

Secondly, warfighters and commanders need to know what a cyber-attack will do to a target. In the US, the Department of Defense has developed Joint Munitions Effectiveness Manuals, which indicates the characteristics and size of a kinetic weapon's detonation. The effect of a cyber-attack, however, unlike a kinetic weapon, isn't dependent on the weapon (or malware) itself. Its effects are based on the system that a piece of malware is targeting. Therefore, it is likely impossible, that one can precisely know the exact effects of a cyber-attack on a system. Instead, what is required is the ability to quickly conduct battle damage assessments—feeding that information back to the commander or warfighter for their subsequent decision or action.

Furthermore, combat in cyberspace can be a rapid measure-countermeasure game. The effect of a cyber-attack isn't necessarily permanent—target system's administrators can restore system functionality and integrity. Therefore, it is not enough to just integrate non-kinetic and kinetic effects—cyber and electronic operations must be synchronized and layered in time and space based on the mission.

So, what is needed is a sandbox—a place where warfighters and commanders can experiment. A place where they can start to imagine what these integrated operations could look like. We need to start to identify ways where we can integrate cyber simulators or ranges with kinetic simulators, allowing the effects in one environment to change the environment or the computer-generated forces in the other. This type of integration has already been demonstrated. Indeed, in 2016, at the Inter-Service/ Industry Training, Simulation, and Education Conference's (I/ITSEC) Blended Warrior, Carnegie Mellon University showcased a Cyber Kinetic Effects Integrator. They developed an application programming interface that bridged their cyber synthetic environment with a third-party kinetic mission training program. Their application programming interface would detect changes in their cyber environment, for instance, the triggering of an alarm, which would then be reflected in the kinetic mission training program. To create a high-fidelity training environment, Carnegie modeled all the systems involved with the mission, so that warfighters could creatively determine the best path to success. Moreover, the synthetic nature of the environment allows for the entire environment to be reset, so that teams can develop and test new operational concepts or tactics, techniques, and procedures.

And the time is ripe for Australia to start thinking about this, particularly with the recent inauguration of Defence Signals Intelligence (SIGINT) and Cyber Command. How can the Australian Defence Force (ADF) start to integrate their new Cyber Command with their conventional warfighters?

Training for Information Operations

The use of cyber and electronic operations extends beyond the subversion, sabotage, or espionage of platforms and systems. The information environment has changed, and adversaries have sought to asymmetrically challenge technical superiority through the adept use of information—targeting the information and cognitive dimensions of warfare. At its core, warfare is about the human mind—it is the ability to bend the adversary to your will. Information operations employ tools—any tool— to shape the information environment, whether that be undermining adversary decision making or creating conditions for various entities to make decisions that benefit friendly force missions.

States and non-state actors have demonstrated the potency of manipulating and controlling the information environment. 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 partially through shaping the information environment. Likewise, during Operation Valhalla in 2006, US Special Forces engaged a Jaish al-Mahdi death squad—killing sixteen, capturing seventeen, destroying a weapons cache, and rescuing a hostage. Shortly after US special forces had left Jaish al-Mahdi returned to the site and rearranged their fallen comrades on prayer mats—creating the impression they had been slaughtered while praying. They released press releases and photographs of the alleged atrocity in Arabic and English on social media. It took the US three days to respond with their story, and by that time the success of their mission had been undermined.

In some cases, training for information operations can be done in a live environment—for instance USAF's use of the EC-130J aircraft to broadcast their own signal over radio or television or to override broadcast stations on the ground. Likewise, in exercise VIKING, which simulates training for peace operations and crisis management, a media gaming cell injects different types of news into the scenario, forcing the participants to manage media response. However, in other instances, when cyber, electronic, artificial intelligence, bots, or social media may be involved, live training will fail to mimic with fidelity potential adversaries use of information operations. Likewise, the use of those capabilities in a live environment may risk revealing them to ever-curious adversaries.

While the integration of cyber and electronic effects into LVC training events is still in its infancy, information operations are routinely discounted or underutilized in training. This is surprising, as information operations have historically been a key component of integrated operations and will remain so in the future. Indeed, the need for a military force to shape the information space in conflict is not new. During WWII, Allies effectively shaped the information environment, causing German attention and resources to be diverted from the beaches of Normandy to Norway and the Pas-de-Calais. Similarly, in 1940, the Germans misled the Allies, causing them to concentrate their troops in Northern France on the Belgian border, rather than in the Ardennes prior to German's lightning thrusts through the forest. The Gulf War is largely considered to be the first information war—the war that demonstrated the lethal effect of information dominance on the battlefield. More recently, we have seen operations live tweeted in real time by unwitting civilian observers. In 2011, a Pakistani live tweeted the US raid on Osama Bin Laden's compound on Abbottabad. While, his tweets had no operational impact, one should wonder what the operational impact of that could have been today now that countries have more exquisite social media data mining capabilities? What would have happened if the ISI, the Pakistani military intelligence service, had caught wind of the ongoing operation?

US Marine Corps Lt. Colonel James McGrath has noted that much of the reason for information operation's exclusion and marginalization in LVC exercises can be attributed to the difficulty of simulating their effects over the exercises' time-period. Moreover, when one starts to include MILDEC, MISO, PYSOP, public affairs, EW, cyber, and other technical capabilities relevant to the information environment, the modeling and simulation (M&S) challenge grows significantly. How do you model the complexities of the physical, technical, and cognitive components of the information environment?

While, again, this is no easy task. It is imperative that militaries and the M&S and synthetic training communities start to work towards this future. We need to start to identify how our adversaries plan to use information operations in battle, so that we can accurately model those for the warfighter. How will adversaries—and likewise, how do we plan to use information operations—for psychological warfare, command and control warfare, denial and deception?

This could manifest in numerous ways—whether it is the use of tactical deception in a squadron-sized operation or it could be through the use of social media to influence a large population.

There are some interesting opportunities emerging for synthetic information operations training. Indeed, virtual training environments have started to emerge that emulate social media. These environments could be used to train intelligence officers, but they also could be used to train warfighters—like cyber or information warriors—to find and identify esoteric pieces of information that may actually have an impact on mission assurance. As Mark Amman, the CEO of the Nusra, a company that specializes in this type of training noted, "we've barely cracked the surface." The potential for these types of training environments are immense, as they could be used to experiment and train for psychological operations, intelligence gathering, and public affairs. Moreover, training goal dependent, integrating these types of environments with other more traditional platform-based synthetic training environments could provide multiple trainees a deeper understanding of how the information environment may impact mission assurance or, likewise, how they can leverage information tools for more lethal effect. Developing application programming interfaces that bridge these different environments, propagating effects across environments, would provide warfighters a test-bed for information operations prior to the crucible of combat.

Synthetic Training and Experimentation: Readiness Through LVC

According to the Department of Defense's military dictionary, readiness is the "ability of military forces to fight and meet the demands of assigned missions." Moving beyond this somewhat broad definition, readiness at its core depends on the articulation of a coherent strategy: The military must describe what it must be ready for, when it must be ready, and what components of a force structure should be maintained in a state of readiness. If that is not challenging enough, defense planners must then decide what inputs to readiness—personnel, equipment, sustainment, and training—should be allocated to achieve those ends.

Readiness requires not just a trained force, but a trained force that can meet the strategic and operational requirements of future wars. LVC is not simply a training platform, but a tool for innovation and experimentation. New operational concepts, doctrines, technologies, and integrated force structures can be tested in virtual worlds—virtual worlds that can evolve autonomously to better reflect changing requirements. In a conversation about a month ago with a RAAF senior leader, he mentioned to me over a discussion about the integration of cyber, electronic, and information operations, that "first we need to work out how we will fight, and then we will train to that." LVC provides the environment to experiment, potentially fail, regroup, and adopt innovations before the first shot is fired or the first sortie is deployed.

Achieving a truly integrated force that breaks down service and domain level silos should not be considered an objective, but a never-ending pursuit as warfare evolves and forces us to innovate. An integrated force should be intrinsically tied to readiness—we need to experiment, and then develop synergy across the force through realistic and repetitive training. As the ADF begins to conceptualize how they can best integrate cyber, electronic, and information effects—particularly with the recent inauguration of the new Defence SIGINT and Cyber Command—LVC should provide a path forward.