PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

Rethinking Cyber Training for the Non-Cyber Warrior

Conference Summary and Conclusions

Jennifer McArdle

January 2019

Cover photo: U.S. Air Force (USAF) enlisted personnel in the Adaptive Flight Trainer. Photo credits: USAF Maj. Travis H. Sheets and USAF Maj. Matthew P. Elmore.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

January 2019

Rethinking Cyber Training for the non-Cyber Warrior: Conference Summary and Conclusions

Jennifer McArdle

On September 6 – 7, 2018, Salve Regina University's Pell Center for International Relations and Public Policy convened an interdisciplinary group of experts from the United States, Australia, France, and Canada to discuss how best to train the non-cyber warfighter to fight in—and through—an increasingly contested and complex battlespace saturated by adversary cyber operations. Participants hailed from academia, the military services, the cyber and defense industries, government, and the defense policy community. The conference was held under Chatham House Rule[1] to encourage frank discussions among participants. It sought to address three pressing questions:

1. How should the military train to fight through a contested battlespace?
2. What unique challenges exist when trying to integrate cyber operations with traditional kinetic operations?
3. How can the military and the defense industry best bridge the gap between today's training technologies and future service needs? [2]

This conference summary highlights the group's deliberations.

Train as You Fight

At present, cyber training for non-cyber warriors is limited across the military services and combatant commands. Few opportunities exist for warfighters to develop an understanding of how a cyber attack may impact their military platform, systems, or broader mission. To the extent cyber is included in a service or combatant command exercise, it often takes place in a separate facility and is not fully integrated across the fight. Non-cyber warfighters rarely get to experience "cyber play" while it is ongoing. This lack of cyber training is problematic, because, as some participants noted, military services must "train as you fight." Moreover, as dictated by the *Joint Training Manual for the Armed Forces of the United States*, "the [Department of Defense] DoD will incorporate realistic cyber conditions into all wargames and exercises…to develop a trained and ready joint force capable of mitigating the effects of denied, manipulated, or contested battlespace conditions."[3]

While participants felt that cyber awareness was increasing across the services, agreement existed that more must be done. Indeed, a lack of cyber awareness was highlighted as a key challenge by some participants when developing cyber training for the non-cyber warrior. One former military leader noted that senior leadership must be

Jennifer McArdle is an Assistant Professor of Cyber Defense at Salve Regina University and a Faculty Fellow at the Pell Center for International Relations and Public Policy. *She would like to thank her students, Alexandra Brodeur, Ryan Ciocco, Cassidy Lynch, and Alexis Smith for their assistance with this conference summary.*

convinced that the cyber threat warrants a change to training regimes. The participant stated that this can be challenging, as some senior leaders lack knowledge on "cyber threats, cyber capabilities, or more generally, the technology." Others felt that a fear of "cyber's potential cascade effects" by some exercise planners and commanders prevented its inclusion in some exercises. Exercise planners and commanders must train their warfighters to multiple training objectives, making the risk of a live cyber effect inadvertently sabotaging an exercise or creating safety risks to warfighters untenable.

As a result, many participants felt that the only way to include high-fidelity cyber effects in training was through a live, virtual, and constructive (LVC) training environment. In brief, LVC can be defined as follows:

- Live: Real people operating in a real environment,
- Virtual: Real people operating in a synthetic environment, and
- Constructive: Synthetic people or forces operating in a synthetic environment.[4]

The Best Approach for Developing Tactical Cyber Injects?

An animated discussion on the best mechanism to design simulated tactical-level cyber effects for training took place over the course of the conference. Many tactical training simulators in use by the military today are unclassified, but cyber training often occurs at the classified level. This creates challenges when attempting to develop high-fidelity tactical effects, as the requisite knowledge may be inaccessible to exercise designers or planners. How then do you create tactical level cyber injects for non-cyber warfighters? Two schools of thought emerged among participants:

- Systems Engineering Approach: Some participants felt that the best way to design simulated cyber effects was to employ a systems engineering approach. Through this approach, an analyst is first meant to identify the cyber attack vector (social engineering, malware, tampered microelectronics, etc.). From there, the analyst then identifies the target of that attack vector. This could include the human organization, mission, networks, systems, or devices and datalinks. Finally, the effect of the cyber attack at that layer is identified. For instance, as one participant noted, an attack vector could include the employment of malware, which targets a platform's operating system or a military network. The follow-on effects could include information

Figure One: Depiction of Live, Virtual, and Constructive Training Applications. Image credit: Veronica Beretta.

Simulating cyber effects in a virtual or constructive environment would alleviate many of the risks associated with integrating cyber into a live environment, such as safety risks to warfighters and local civilians, the danger of inadvertently disrupting the entirety of an exercise, or the potential to expose military platform vulnerabilities to ever-curious adversaries.

inaccuracies, induced system failures, denial of service, or data exfiltration. Each of these effects would then be simulated for the warfighter.

- Information Assurance Approach: Other participants felt that an information assurance paradigm called the "CIA triad" was a more useful framework to identify cyber effects. The "CIA" triad seeks to ensure the (C) confidentiality, (I) integrity, and (A) availability of data within a system. By applying the CIA triad to key platform capabilities, one can then extrapolate how the loss of a given capability's confidentiality, integrity, or availability can impact the broader platform.

More broadly, disagreement persisted on the need for tactical level cyber effects to be simulated for warfighters. Some argued that these effects are already simulated in other capacities for non-cyber warfighters, and are thus, already a "normal function expected of those in tactical mission command roles." For example, a cyber attack that sabotages key platform functionality would have similar simulated effects to an equipment malfunction that occurred through, for instance, mechanical or electrical failure. Therefore, no new simulated effects need to be developed. Others argued that cyber does produce some unique tactical level effects and should be included in tactical training scenarios. The manipulation of the integrity of system or platform information was highlighted as a particularly insidious threat that can produce unique cyber effects.

The Need for an Integrated Training Environment

Developing training for non-cyber warriors to fight in—and through—an increasingly contested and complex battlespace does not just involve simulating an adversary's cyber attacks against U.S. and allied platforms and systems. U.S. and allied warfighters must also understand some of the unique attributes that their cyber counterparts bring to the fight when conducting multi-domain operations.[5]

As one participant noted, the predictability of offensive cyber operations differs significantly from traditional kinetic operations. The U.S. DoD employs Joint Munitions Effectiveness Manuals (JMEMs) when modeling and simulating U.S. offensive operations for training. JMEMs indicate the characteristic and size of a kinetic weapon's detonation, providing some predictability to U.S. warfighters on the outcome of planned operations.[6] However, the effect of a cyber-attack, 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.[7] Therefore, it is likely impossible to precisely predict the exact effect of a cyber-attack on a system.[8] Instead, warfighters need the ability to quickly conduct battle damage assessments—feeding that information back to friendly forces for their subsequent decision or action. Such a capability would naturally benefit from integrated training.

Participants agreed that integrated training across functional areas must occur to build greater awareness, understanding, and linkages between non-cyber warfighters and cyber warriors. However, there are immense challenges to achieving that vision. As one participant stated, at present, "there is a doctrinal disconnect" in the military services.[9] Air, land, sea, space, and cyber doctrine are all very different, which creates stove-piped operations. The participant went on to explain that a "structural disconnect also exists in the military." Despite the importance the DoD attaches to operating as an integrated joint force, the participant felt that "the services lack a culture of combined arms." Operating as a joint force, let alone a multi-domain force, remains a challenge. Such views were echoed by an instructor at the Air University's Air Command and Staff college,

> We basically get trained in stove pipes as symmetrical thinkers. Army guys first think about what tanks can do against tanks. It may not be their instinct to think about what airpower or cyber can do against a tank. Likewise, airmen think about what the F-35 can do to a SU-27, but they

> don't think about what Army special operations forces with a bunch of quadcopters or a space based cyber inject can do. We need a new methodology for training to get us as people to be disciplined and true about asking the question through planning, execution, and acquisition about how we can provide value in adjacent domains.[10]

Additionally, while synthetic training environments do exist for cyber warriors and conventional warfighters, these environments are often siloed. Synthetic environments are frequently limited to their specific task (i.e. training cyber warriors) and are not necessarily linked with other simulations for integrated training across the force. For instance, synthetic training for cyber warriors tends to focus entirely on the cyber portion of an operation, often ignoring the larger battlefield picture. Likewise, kinetic mission training programs rarely demonstrate what a cyber warrior can bring to the fight. Training isn't necessarily geared towards integration across services—let alone across domains.

Yet, despite present challenges, there are ongoing efforts within the scientific community to demonstrate the plausibility of an integrated synthetic environment. As one participant noted, Carnegie Mellon University's Software Engineering Institute developed a Cyber Kinetic Effects Integrator (CKEI) that linked a cyber simulator with a kinetic mission training program called *Virtual Battlespace* 3 (VBS3). CKEI allowed effects (like the triggering of an alarm) to propagate across the two synthetic environments, allowing cyber warriors and warfighters to develop a better understanding of what their counterparts could bring to the fight.[11] Participants felt that these initial scientific demonstrations were useful steps in the right direction and should form a baseline of future technical inquiry and development.

LVC and Future War: The Training End Goal Must be Considered Up Front

Participants were asked to provide their perspectives on how the U.S. and allied military services are imagining future war. The discussion sought to identify how the armed forces and defense industry can best bridge the gap between today's training technologies and those required to provide a high-fidelity depiction of tomorrow's battlefield.

Participants began by cautioning that humility may be the greatest of virtues when predicting future war—it is impossible to delineate with absolute certainty how the future battlespace may unfold. As a result, the United States must be prepared to fight in a range of complex contingencies spanning the spectrum of conflict, from counterinsurgency and counter terrorism operations to high-tempo, informationized operations against near-peer or peer competitors.[12]

Participants felt LVC directly addressed this challenge. U.S. services are being asked to train for a range of mission sets without the requisite time or resources. Synthetic training provides opportunities for warfighters to train for an assortment of contingencies in a cost-effective and efficient manner. Participants felt that training focus should be on "reps and sets" in simulators—building needed tactical and operational skills, critical thinking, and creativity. This complements current DoD efforts. Indeed, former Secretary of Defense, James Mattis recently stated that warfighters should experience twenty-five bloodless battles in simulators before the first fight.[13]

When employing synthetic training technologies, participants highlighted the necessity of ensuring that the training platform benefits the end-user. If a simulator or a synthetic training application is too complex, it will not be useful. One service member emphasized the importance of user studies, to facilitate end-user feedback and ensure that training platforms meet end-user needs.[14] Moreover, participants noted that the training system should be tailored to its intended audience. As one attendee stated, "cadet training is fundamentally different than training for someone with more experience."

Perhaps, most importantly, all participants stressed the need for the training end-goal to be considered up front. Synthetic training environments and training scenarios should directly support the skill-sets and relevant

lessons that an exercise seeks to develop. In some cases, this may require a high-fidelity immersive training environment. In other cases, it may not. Training technologies and environments should be tailored to the desired training outcomes.

LVC and Experimentation

Conference attendees highlighted that LVC is not simply a training platform, it's also 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.[15] LVC provides the environment to experiment, potentially fail, regroup, and adopt innovations before the first shot is fired or the first sortie is deployed. However, as one participant cautioned, when employing synthetic environments for experimentation, "it can't be done aimlessly—there must be a question that we seek to answer, some fact that we wish to establish or disprove." LVC cannot be employed to experiment towards serendipity.

Indeed, a similar methodology should be applied to experiments in synthetic environments as employed when experimenting in live environments. A military experiment must include the following:

- an *event* that can have multiple outcomes;
- a *question* that can have multiple answers; and
- a *matching*—almost always pre-stated—between the outcomes of the event and the answers to the question.[16]

When conceptualizing how best to fight as an integrated force in a future contested and complex battlespace, LVC—if employed properly—provides the requisite fidelity to experiment and innovate. Achieving a truly integrated force that breaks down service and domain level silos should not be considered a finite objective, but an ongoing pursuit—a moving target—as warfare evolves and forces us to innovate.

Concluding Thoughts

In conclusion, participants felt that an intimate interdisciplinary forum like the one provided at Salve Regina University's Pell Center for International Relations and Public Policy provided a unique opportunity to address some of the more challenging questions tied to military training, future war, and readiness. The size of the conference—limited to 50 people—allowed for a diversity of opinions, while ensuring that everyone's voice was heard by the other participants. Participants were provided ample opportunity to network with the hope that connections developed at the conference would develop into deeper relationships and future work and/or research on synthetic training and future warfare. Indeed, the goal of the conference was to move the debate forward on these pressing issues, as training must evolve to support future combat.

To quote the Defense Science Board, "if you wish to increase military proficiency now, the best place for your marginal dollar is training."[17] If the United States wishes to continue to field the world's finest fighting force, its military and defense industrial base will need to move toward more fully supporting and investing in synthetic training.

Endnotes

1. Participants are free to use conference information, but neither the identity nor the affiliation of the speaker can be identified.

2. For an in-depth study that addresses some of these questions, amongst others, see: Jennifer McArdle, "Victory Over and Across Domains: Training for Tomorrow's Battlespace," Center for Strategic and Budgetary Assessments (January 2019).

3. Joint Staff, Joint Training Manual for the Armed Forces of the United States CJCSM 3500.03E (20 April 2015): G-F-1.

4. Roger D. Smith, *Military Simulation and Serious Games* (Orlando, FL: Modelbenders LLC, 2009): 15.

5. For the purpose of this conference report, multi-domain operations are defined as operations that move beyond services as organizing constructs, and instead harness joint experience to produce integrated effects through multiple domains—air, land, sea, space, and cyber. The goal of multi-domain operations should be to focus on the desired effects that one wants to bring to bear on an adversary, rather than on a given service or domain. See, for instance: US Air Force LeMay Center for Doctrine Development and Education, The Doolittle Wargame 2018: Multi-Domain Command and Control (Maxwell Air Force Base, 5-8 November 2018) and US Army Training and Doctrine Command, "Multi Domain Operations," US Army, 4 October 2018, https://www.army.mil/standto/2018-10-04.

6. Colin Michael Anderson, "Generalized Weapon Effectiveness Modeling," Naval Postgraduate School (June 2004).

7. Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016): 130.

8. Despite this difficulty, DOT&E is currently working with the Joint Technical Coordinating Group for Munitions Effectiveness (the producer of JMEMs) to identify data that will assist in developing predictive tools for anticipating cyber effects. See: Director, Operations Test & Evaluation, FY 2017 Annual Report, (January 2018): 317.

9. For more on the role of doctrine in joint operations, see: Miranda Priebe et. al., *Promoting Joint Warfighter Proficiency: The Role of Doctrine in Preparing Airmen for Joint Operations* (Santa Monica, CA: RAND, 2018).

10. Author interview with US Air Force Lt. Col. Peter Garretson, Maxwell Air Force Base, Montgomery, AL, 23 January 2018.

11. Rotem Guttmann, "Combined Arms Cyber-Kinetic Operator Training," Carnegie Mellon University Software Engineering Institute SEI Blog, 20 March 2017, https://insights.sei.cmu.edu/sei_blog/2017/03/combined-arms-cyber-kinetic-operator-training.html.

12. For an overview of the diversity of potential threats, see: Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence (13 February 2018).

13. Secretary Mattis' comments were directed towards the infantry, however, his statement has far larger applications. Jen Judson, "25 bloodless battles: Synthetic training will help prepare for current and future operations," *Defense News*, 5 September 2018, https://www.defensenews.com/smr/defense-news-conference/2018/09/05/25-bloodless-battles-synthetic-training-will-help-prepare-for-current-and-future-operations/.

14. Lionel Beehner and John Spencer, "Even Realistic Videogames Like Call of Duty Won't Help Us Win Wars," *Wired*, 5 January 2018, https://www.wired.com/story/even-realistic-videogames-like-call-of-duty-wont-help-us-win-wars/.

15 See, for instance, CAE's Dynamic Synthetic Environment: CAE, "Dynamic Synthetic Environment," https://www.cae.com/media/media-center/documents/datasheet.CAE.Dynamic.Synthetic.Environment.pdf.

16 Brian McCue, "The Art of Military Experimentation," Center for Naval Analysis (June 2004): 7.

17 Ralph Chatham and Joe Braddock, "Defense Science Board Task Force on Training for Future Conflicts," Defense Science Board (June 2003): 7.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

About the Pell Center

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Claiborne Pell's legacy, the Pell Center promotes American engagement in the world, effective government at home, and civic participation by all Americans.

www.pellcenter.org