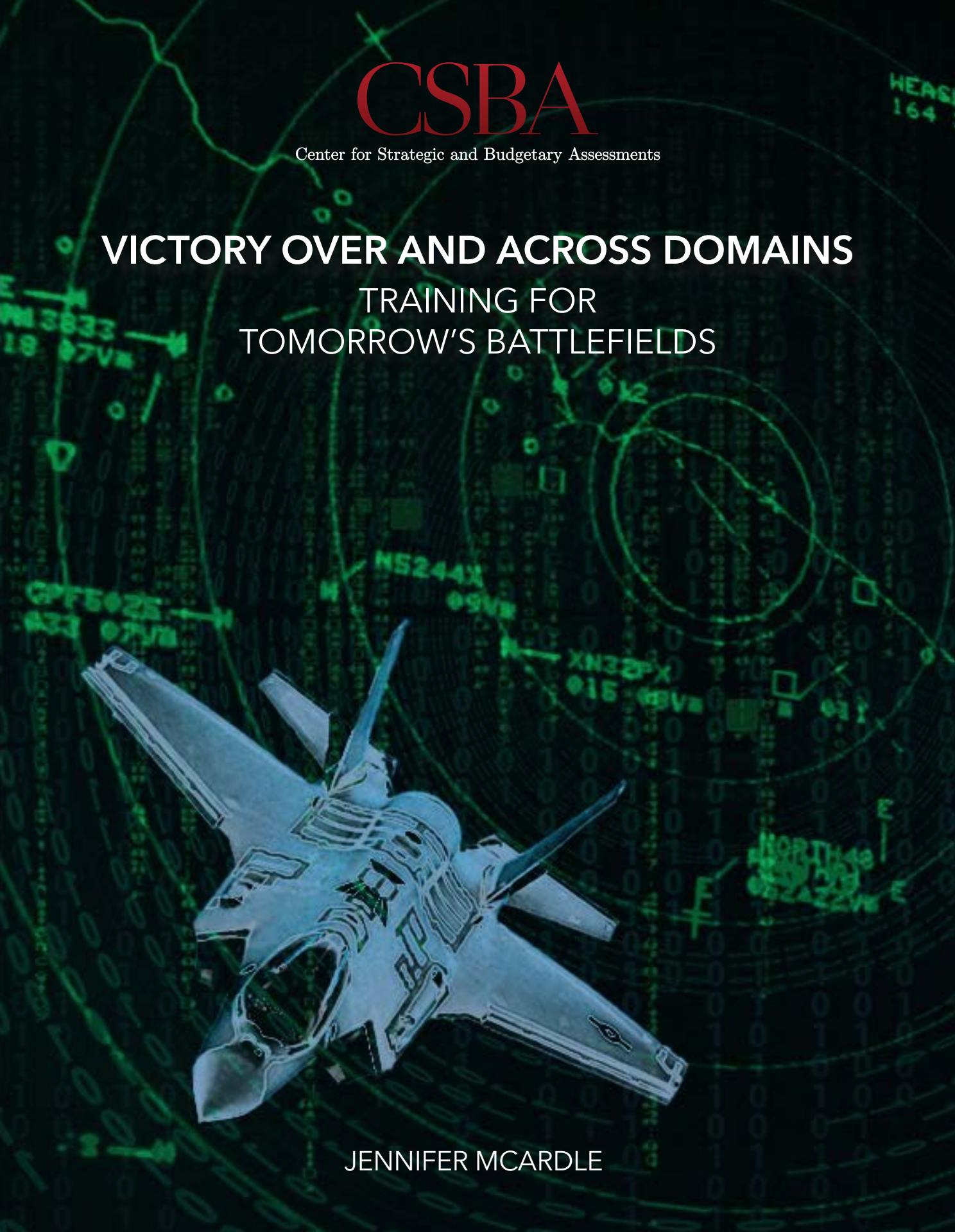
CSBA

Center for Strategic and Budgetary Assessments

VICTORY OVER AND ACROSS DOMAINS

TRAINING FOR TOMORROW'S BATTLEFIELDS



JENNIFER MCARDLE

VICTORY OVER AND ACROSS DOMAINS

TRAINING FOR TOMMORROW'S BATTLEFIELDS

JENNIFER MCARDLE

CSBA
Center for Strategic and Budgetary Assessments

2019

ABOUT THE CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS (CSBA)

The Center for Strategic and Budgetary Assessments is an independent, nonpartisan policy research institute established to promote innovative thinking and debate about national security strategy and investment options. CSBA's analysis focuses on key questions related to existing and emerging threats to U.S. national security, and its goal is to enable policymakers to make informed decisions on matters of strategy, security policy, and resource allocation.

ABOUT THE AUTHOR

Jennifer McArdle is a Non-Resident Fellow at the Center for Strategic and Budgetary Assessments and is an Assistant Professor of Cyber Defense at Salve Regina University. Her research interests include cyber operations, military synthetic training, and military innovation. Her work has been featured in Real Clear World, The Cyber Defense Review, National Defense Magazine, and War on the Rocks, among others. She currently serves on Congressman James Langevin's Cyber Rhode Island Advisory Committee. Jennifer previously worked at the Potomac Institute for Policy Studies, where she served as a contractor for the Department of Defense, Defense Microelectronics Activity on cyber hardware and supply chain security. She has also held positions at the American Association for the Advancement of Science and the U.S. National Defense University, in addition to working in New Delhi, India at two defense research institutions. She is currently a PhD candidate in War Studies at King's College London and a recipient of the RADM Fred Lewis (I/ITSEC) doctoral scholarship in modeling and simulation.

ACKNOWLEDGMENTS

The author would like to thank the CSBA staff for their assistance with this report. Special thanks go to Dr. Evan Montgomery and Dr. Thomas G. Mahnken for their thoughtful suggestions and to Kamilla Gunzinger and Maureen Fitzgerald for managing the publication of the report. The author would also like to thank Richard Bejtlich; Lt. General (ret.), Yvan Blondin; Air Marshal (ret.), Geoffrey Brown; JD McCreary; and Dr. Iskander Rehman for their helpful comments on previous versions of the report. Additionally, the author thanks her Salve Regina University students for providing valuable research assistance over the course of the project: Alexandra Brodeur, Ryan Ciocco, Eli Dias, Jacob Leahey, Cassidy Lynch, Allyssa Medeiros, Alexis Smith, and Nicholas Palumbo. The graphics were designed by Salve graphic design student, Veronica Beretta. The analysis and findings presented here are solely the responsibility of the author.

CSBA receives funding from a broad and diverse group of contributors, including private foundations, government agencies, and corporations. A complete list of these organizations can be found on our website at www.csbaonline.org/about/contributors.

Cover: Design by Veronica Beretta and Kamilla Gunzinger. The image of the F-35 is adapted from a photo of an F-35A Lightning II aircraft during a flight from England to the United States on July 13, 2015. Air Force photo by Staff Sgt. Madelyn Brown.

Contents

FIGURES

TABLES

Executive Summary

Today's U.S. military is an information-dependent force, one that is wholly reliant on information communication technology (ICT) for current and future military operations. The adaptation and integration of ICTs into weapons platforms, military systems, and in concepts of operation has put the battle for information control at the heart of great power competition. While the use of ICTs exponentially increases the U.S. military's lethality, the dependence on these technologies, in many ways, is also a vulnerability. U.S. competitors and adversaries—most notably Russia, China, Iran, and North Korea—recognize this reality. Each state plans to employ a range of cyber and informationized capabilities to undermine the confidentiality, integrity, and availability of U.S. and allied information in competition and combat.[1]

It is impossible to deny an adversary entirely of the ability to shape aspects of the information environment, to include spoofing and sabotaging ICT-based warfighting systems. As a result, the U.S. military's goal should be to sustain military operations *in spite of* a denied, disrupted, or subverted information environment. This requires a paradigm shift away from *information assurance* to *mission assurance*. U.S. warfighters should be trained to fight as an integrated whole in and through an increasingly contested and complex battlespace saturated by adversary cyber and information operations. The battle for information control should drive training adaptation to provide warfighters the experiential learning that translates into quick reflexes, critical thinking, and cross-domain synergies on the battlefield.

This report engages in a detailed analysis of current and future cyber and informationized training for the non-cyber warfighter. In so doing, it seeks to address two main questions:

1. How should U.S. armed forces train its warfighters tactically and operationally for a battlespace saturated by adversary cyber and informationized attacks on U.S. platforms and systems?

1 A recent Government Accountability Office (GAO) report highlights the mission critical cyber vulnerabilities present in many U.S. weapon systems and platforms. GAO, *Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities* (Washington, DC: GAO, October 2018).

2. How should U.S. armed forces train its warfighters to exploit the advantages of the cyber domain for multi-domain operations?

In exploring these questions, the report introduces initial recommendations on how training simulations and scenarios can be updated to better reflect the future operating environment.

Current Cyber and Informationized Training for the Non-Cyber Warfighter

U.S. armed Services are beginning to conceptualize how they can train non-cyber warriors for an information-saturated, hyper-connected battlespace. At this juncture, however, a high-fidelity training environment that realistically simulates the effects of cyber or informationized attacks on military platforms and systems remains somewhat aspirational. Tactical cyber and informationized training across the Services is nascent and not fully integrated across the force. To the extent cyber is included in training events, the focus is primarily on networks and mission command systems.

During large-scale Service or combatant command exercises, cyber training is often employed in parallel with traditional kinetic training programs and is not fully integrated. Non-cyber warfighters do not necessarily experience the effects of "cyber play" while it is ongoing. When cyber and informationized effects are integrated into live training events, they are often "white carded," which involves the literal use of a rudimentary note card to inject friction. Although this does provide warfighters some insight into how their systems or platforms may be affected in the event of a cyberattack, the lack of realism precludes them from experiencing and subsequently troubleshooting that attack.

The lack of cyber and informationized effects in live training is often for good reason. The integration of these effects into a live training environment could sabotage the entirety of an exercise, present safety risks to warfighters and local civilians, or reveal platform vulnerabilities to inquisitive adversaries. Yet, these live training challenges should not preclude the Department of Defense (DoD) from training for a future contested and complex battlespace. These live training risks could be circumvented through high-fidelity synthetic training. Synthetic training can take four forms:

1. Virtual Simulations: real people operating synthetic systems;
2. Constructive Simulations: synthetic people operating synthetic systems;
3. Gaming: video games with real or synthetic operators; and
4. Augmented Reality: adding synthetic overlays onto the real world.

Modeling and simulating realistic cyber and informationized effects within a training simulator or in a broader synthetic training exercise should provide warfighters some insight into how a cyber or informationized attack will affect their system or mission. Yet, to date,

simulating cyber and informationized effects in a synthetic environment for the non-cyber warfighter have been rare experiments.[2] Simulated tactical- and operational-level cyber and informationized injects must be developed and integrated into training exercises across the force.

Current Training for Multi-Domain Operations

Integrating cyber and informationized operations into non-cyber warrior training does not just require simulating the effect of an adversary's cyber or information operations in a synthetic training environment. Warfighters must also understand the unique attributes that cyber warriors bring to the fight when pursuing multi-domain operations, to include timing, authorities, and classification, among others. Multi-domain operations require warfighters to more seamlessly work between domains to support, augment, or assure their mission. An integrated synthetic training environment must support this end.

Synthetic environments exist for cyber and informationized training, but these environments are often siloed. They are incompatible with the conventional simulations employed to train non-cyber warfighters and battle staff. Synthetic training environments for cyber and information operations 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.[3]

Notwithstanding these limitations, the scientific community has demonstrated the plausibility of developing an integrated synthetic training environment. Cyber simulators have been integrated with kinetic mission training programs, allowing effects (like the triggering of an alarm) to propagate across environments.[4] Likewise, initial models of the information environment have been developed with the goal of integrating information effects into constructive simulations. These ongoing scientific programs and models are certainly steps in the right direction. They act as initial testbeds to evaluate the plausibility of a multi-domain training environment.

2 To date, experiments such as the Cyber Operational Architecture Training System (COATS) and the Cyber Operations Battlefield Web Services (COBWebS) have replicated the effect of a cyberattack on traditional command-level training simulations. For more information, see David Wells and Derek Bryan, "Cyber Operational Architecture Training System—Cyber for All," *Journal of Cyber Security and Information Systems* 6, no. 2, July 2018; and Henry Marshall et al., *Cyber Operations Battlefield Web Services (COBWebS)—Concept for a Tactical Cyber Warfare Effect Training Prototype* (Orlando, FL: Simulation Interoperability Standards Organization, 2015).

3 For instance, the United States has developed realistic, closed-network cyber ranges such as the DoD Cybersecurity Range, the Joint Information Operations Range (JIOR), and the National Cyber Range to train cyber warriors in a range of tactics, techniques, and procedures for offensive and defensive computer network operations. Likewise, synthetic environments that emulate some of the technical and cognitive dimensions of the information environment also exist: like those in Aptima's Cultural Awareness for Marines Operation (CAMO) program or DARPA's Compass program, for example.

4 Carnegie's Cyber Kinetic Effects Integration (CKEI) program and the Cyber Operational Architecture Training System (COATS) are strong examples. See Rotem Guttmann, "Combined Arms Cyber-Kinetic Operator Training," *Carnegie Mellon University Software Engineering Institute (SEI) Blog*, March 20, 2017, available at https://insights.sei.cmu.edu/sei_blog/2017/03/combined-arms-cyber-kinetic-operator-training.html; and Wells and Bryan, "Cyber Operational Architecture Training System."

These different integrated architectures must be evaluated for performance and the deployment of multi-domain training. This naturally requires scenario development.

Recommendation: Develop Unique Tactical-Level Cyber and Informationized Effects for Simulators

Simulating tactical-level cyber and informationized effects in synthetic trainers should be a function of platform capabilities and their potential vulnerabilities. Exactly how a system or platform could be disrupted by a cyberattack depends on the details of that system. This calls for deep knowledge of how the system works, its specifications, and how the system fits into its broader battle network. This information is often highly classified, especially with regard to the military's most technologically advanced platforms. Meanwhile, many training simulators in use by the military are often unclassified. As a result, such expertise may not be readily available to inform the modeling and simulation of cyber or information effects. Developing a suite of simulated cyber and informationized injects can still be helpful, however, even if those injects are slightly divorced from reality. Given the number of ways that a cyberattack can affect a system, the goal should be to get the trainee to troubleshoot a diverse range of effects and creatively identify ways to maintain mission assurance despite the attack.

Information assurance professionals often refer to the "CIA triad" as the guiding construct for organizational information security.[5] These practitioners work to ensure the (C) confidentiality, (I) integrity, and (A) availability of data within a system. Although this model is typically used to guide information security policy, it also provides a simple conceptual point of departure to extrapolate the effects of adversaries' cyber or informationized operations on military platforms and systems. By assessing key platform capabilities against each component of the triad, one can begin to design effects that simulate with a measure of fidelity the impact of adversary cyber or informationized operations on the broader platform. The focus should be on identifying what effects are unique to cyber when developing tactical-level training for the non-cyber warrior. These effects could then be used as the basis for modeling and simulating master scenario event list (MSEL) events/injects.

Recommendation: Depict Adversary Cyber and Informationized Operations with a Measure of Fidelity

It is likely impossible to predict with absolute certainty how an adversary may choose to employ offensive cyber and informationized operations against U.S. forces. Cyber capabilities, by their very nature, must remain secretive. Once a cyberattack is employed, U.S. system administrators can respond, patching the vulnerabilities to render the same exploit unusable. Given the secretive nature of cyber operations, incentives also exist for adversaries to

5 Security Ninja, "CIA Triad," *InfoSec Institute*, February 7, 2018, available at http://resources.infosecinstitute.com/cia-triad/#gref.

deliberately misrepresent their cyber capabilities, to include personnel, zero-day stockpiles, or other potential indicators of strength. Likewise, the most compelling information the United States has on potential adversaries' cyber capabilities is classified, as they are likely the result of hidden and possibly ongoing intrusions into adversaries' networks and systems. This can prove problematic for training scenario development, as some exercises, simulations, and simulators operate at the unclassified level.

Despite these challenges, most competitors and potential adversaries—China, Russia, North Korea, and Iran—have issued strategic or doctrinal documents that provide some indication of how they may use cyber and informationized capabilities in a conflict. Combining these documents with material on potential adversaries' past cyberattacks and intrusions can provide a baseline for simulating realistic red (opposing) forces in training scenarios. This report identifies four key insights on the aims of adversary cyber operations:

1. *Targeting key nodes:* U.S. adversaries prioritize the targeting of key nodes prior to, or at the onset, of hostilities. Key nodes include military communications systems, command facilities, combat support functions, logistics systems, satellites, and ground stations, among other assets that are integral to the communication and prosecution of military operations. Training-level-dependent, simulated events could emulate the loss of the command and coordination systems necessary for combined arms or joint functions, among other cascade effects.

2. *Emphasizing informationized or psychological to cause a loss of trust in systems or networks:* U.S. competitors emphasize informationized or psychological operations in their strategic, operational, and tactical warfighting strategies. Information operations at the strategic level of warfare can be reflected in background scenario information, helping to provide a broader geopolitical context for the exercise. At the operational level of warfare, scenarios should include training goals that provide warfighters experiential learning on adversary deception and information operations. These training goals should force warfighters to critically assess information, questioning its validity, while correlating that information against multiple sources. At the tactical level, simulated injects could include the spoofing or manipulation of data in key military platforms or systems, causing a loss of trust in battle networks and platforms.

3. *Employing cyber as force multipliers in anti-access/area-denial (A2/AD) bubbles:* U.S. rivals have developed A2/AD strategies with varying levels of sophistication that employ a range of conventional capabilities that will be augmented by cyber operations. When developing scenarios for joint mission essential task lists (JMETLs), emphasis should be placed on mimicking adversary A2/AD capabilities and their operational impact on U.S. forces. This should include the attrition of physical and virtual U.S. forward sanctuaries, to include space, cyberspace, and the electromagnetic spectrum (EMS).

4. *Conducting cyber operations that will likely follow the logic of conventional capabilities:* States will likely employ cyber capabilities to enhance and ensure the success of their traditional kinetic weapons systems. MESLs that simulate cyber operations should also draw on current intelligence on adversary kinetic weapon capabilities. These capabilities should help to inform assessments of the *blended* strategies, combining kinetic and non-kinetic attacks, that adversaries may adopt in the event of conflict.

Recommendation: Develop Multi-Domain Training Scenarios for the Test and Evaluation of Integrated Synthetic Training Architectures

While an integrated synthetic training environment does not yet exist, that should not preclude commanders and exercise planners from designing multi-domain scenarios and story lines for the test and evaluation of future integrated training architectures. Designing a solid story line is important, as it allows for more dynamic play and less scripted events, all while meeting the exercise's objectives. Scenarios should shape the exercise's narrative, providing the conceptual scaffolding for each of the training events.

This report develops three initial scenarios that could be used as an initial point of departure for the test and evaluation of future integrated synthetic training architectures while also contributing to JMETL and MSEL development. Each of the scenarios seek to highlight a unique attribute of cyberspace and the information environment for multi-domain training.

Looking Ahead

A common mantra within the U.S. military has been to "train as you fight." Yet, live training fails to replicate with fidelity the type of cyber and informationized operations that warfighters will experience in a contested and complex battlespace. The synthetic training environment can inject a much-needed degree of realism, replicating an information-saturated combat environment for non-cyber warfighter training. However, synthetic training systems, scenarios, and models must evolve to support this future. The report is designed as an initial point of departure to support cyber and informationized training for the non-cyber warfighter.

Introduction

> *And for pleasure, there was the simulator, the most perfect video game that he had ever played. Teachers and students trained him, step by step, in its use. . . . It was exhilarating at last to have such control over the battle, to be able to see every point of it.*
>
> Orson Scott Card, *Ender's Game*[6]

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 (PGM) rained down with seemingly perfect accuracy on Iraqi military and civilian targets.[7] It was January 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 Gulf War is considered by some to be the first information war, one that demonstrated the full lethality of DoD's information communication technology-based investments during the Cold War.[8] The fusion of advanced microprocessors, new sensor-based technology, and satellite communications promised to improve battlespace awareness and potentially burn through the fog of war. PGMs 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."[9]

Despite the climate of intense optimism, the fog of war did not entirely dissipate. As General Walt Boomer, who led the Marine assault on Kuwait, later noted, "The intelligence stunk."[10]

6 Orson Scott Card, *Ender's Game* (London: Orbit, 1985), pp. 260–261.

7 Donald Humphreys, "War on Television," *Museum of Broadcast Communications,* available at http://www.museum.tv/eotv/warontelevi.htm.

8 Norman C. Davis, "An Information Based Revolution in Military Affairs," in John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Washington, DC: RAND Corporation, 1997), p. 80.

9 United States General Accounting Office (GAO), *Operation Desert Storm: Evaluation of the Air Campaign* (Washington, DC: GAO, June 1997), p. 25.

10 "Oral History: Walt Boomer," *FRONTLINE,* available at https://www.pbs.org/wgbh/pages/frontline/gulf/oral/boomer/1.html.

He did not have the intelligence picture or the complete battlespace awareness that he desired. Moreover, only about 80 percent of PGMs launched succeeded in accurately hitting their targets.[11] Indeed, to more skeptically minded strategists, the Gulf War was only partially successful at translating technological concepts into actual battlefield victory.[12] Friction remained.

Yet, even with these limitations in mind, Operation DESERT STORM did act as a formidable demonstration of the changing character of war.[13] 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 ICTs. The U.S. military's performance during the Gulf War was carefully scrutinized overseas and served as a catalyst for Chinese and Russian efforts at military modernization and reform.[14] Today, those lessons learned have globally metastasized, as indicated by an ever-burgeoning number of states developing and acquiring ICT-based military capabilities.[15] ICTs have come to be viewed as a force multiplier in combat, but they are also a potential source of U.S. vulnerability for asymmetric exploitation. Indeed, ICTs are uniquely vulnerable to cyber-attacks for the purposes of espionage, sabotage, or subversion.

Although the United States has experienced some cyberattacks in battle, it has yet to fully face a near-peer competitor. In Iraq and Afghanistan, the use of cyber operations by insurgents have reportedly been primarily limited to geo-locating military assets or intercepting unencrypted unmanned aerial vehicle (UAV) feeds, among other fairly rudimentary operations.[16] Accordingly, integrated offensive cyber and conventional operations by U.S. forces in the

11 GAO, *Operation Desert Storm*, p. 119.

12 Barry Watts, *Clausewitzian Friction and Future War*, McNair Paper 52 (Washington, DC: National Defense University Press, October 1996), pp. 37–58.

13 For more on the changing character of war, see Hew Strachman and Sibylle Scheipers, *The Changing Character of War* (Oxford, UK: Oxford University Press, 2011); and Benjamin Jensen, "Emergence: The Changing Character of Competition and Conflict," *War on the Rocks*, February 6, 2017, available at https://warontherocks.com/2017/02/emergence-the-changing-character-of-competition-and-conflict/.

14 See, for instance, Stephen Cimbala, "Chinese Military Modernization: Implications for Strategic Arms Control," *Strategic Studies Quarterly*, Summer 2015; and Benjamin Lambeth, *Desert Storm and its Meaning: A View from Moscow* (Santa Monica, CA: RAND Project Air Force, 1992).

15 A dated estimate from 2011 places the number of states with developed military cyber capabilities at approximately 33. This estimate also includes Iran and North Korea, two states that have an adversarial relationship with the United States. See James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington, DC: Center for Strategic and International Studies, 2011).

16 See, for instance, John Reed, "Insurgents Used Cell Phone to Geotag and Destroy AH-64s in Iraq," *Defense Tech*, March 15, 2012, available at https://www.military.com/defensetech/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq; and Noah Shachtman, "Insurgents Intercept Drone Video in King Size Security Breach," *Wired*, December 17, 2009, available at https://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/.

region have focused on relatively low-end adversaries.[17] When confronted with the absence, thus far, of a richly ICT-infused battlefield experience, realistic training provides the best source of preparation prior to the crucible of future high-intensity informationized combat.

This report engages in a detailed analysis of current and future cyber and informationized training for the non-cyber warfighter. It addresses two main questions:

1. How should U.S. armed forces train its warfighters tactically and operationally for a battlespace saturated by adversary cyber and informationized attacks on US platforms and systems?

2. How should U.S. armed forces train its warfighters to exploit the advantages of the cyber domain for multi-domain operations?[18]

To answer these two questions, this report proceeds in three substantive parts. The first chapter explores the changing character of warfare by examining the cyber and informationized threats to military platforms and systems. It argues that while the United States may attempt to better secure their platforms and systems against adversaries' cyber or informationized attacks, no system can be entirely cyber-secure. As a result, a paradigm shift from *information assurance* to *mission assurance* must take place within the military. Emphasis should be placed on finding a new or creative route to victory, despite a denied, degraded, or spoofed environment. Training is integral to support this end.

The second chapter assesses current U.S. cyber and informationized training for the non-cyber warfighter. It first explores how the military presently trains its warfighters at the tactical and operational level to withstand and fight through adversary cyber and informationized attacks on U.S. platforms and systems. It then considers current opportunities for the non-cyber warfighter to train alongside cyber warriors for the prosecution of multi-domain operations. Throughout, attention is drawn to the limitations associated with current training techniques, to include the dangers of live cyber fire training and the difficulty and sensitivity of simulating cyber effects in synthetic training environments. It concludes that, at present, U.S. armed forces have inadequately prepared non-cyber warriors for the cyber vulnerabilities they will encounter on the battlefield. Likewise, the armed forces have failed to train non-cyber warriors

17 The battle against the Islamic State has furnished the United States with a testbed for the close integration of cyber and more traditional military operations. However, the Islamic state—an adversary that uses ICTs primarily for recruitment and the distribution of propaganda—is not a highly sophisticated cyber adversary. Dam Lamothe, "How the Pentagon's Cyber Offensive Against ISIS Could Shape the Future Elite US forces," *The Washington Post*, December 16, 2017, available at https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/?utm_term=.42b838427f81.

18 For the purposes of this report, multi-domain operations are defined as operations that move beyond the 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, Amy McCullough, "USAF Looks to Create New Command and Control Structure," *Air Force Magazine*, June 6, 2018; and "Multi Domain Operations," U.S. Army Training and Doctrine Command (TRADOC), October 4, 2018, available at https://www.army.mil/standto/2018-10-04.

for the potential opportunities of employing the cyber domain alongside their conventional operations to assure mission success.

The third and final chapter reiterates that the synthetic training environment is essential to mimic cyber and informationized operations with the requisite fidelity to prepare the non-cyber warfighter for future combat. However, training systems, scenarios, models, and simulations must evolve to support this future. The recommendations provided in the final chapter are designed as an initial point of departure to achieve this vision.

CHAPTER 1

The Battle for Information Control

During the Cold War, forces prepared to operate in an environment where access to communications could be interrupted by the adversary's advanced capabilities. . . Through years of practice and exercise, a culture of resilience took root in the military and units were ready and prepared to operate in contested environments. . . . In the face of an escalating cyber threat, the lessons of the previous generations must now be passed down. The Defense Department must be able to carry out its missions to defend the country. Organizations must exercise and learn to operate without the tools that have become such a vital part of their daily lives and operations.

Department of Defense Cyber Strategy 2015[19]

The U.S. military has evolved from an *information-enabled* force in the Persian Gulf War to an *information-dependent* force, one that is wholly reliant on ICTs for current and future military operations. As the 2012 *Defense Strategic Guidance* noted, "modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space."[20] This dependence is set to increase. From the increased employment of robotics on the battlefield, to the use of unmanned system swarm optimization and artificial intelligence augmenting human commander decision-making, ICTs will continue to act as the backbone for modern military operations.[21] While the use of ICTs increases the U.S. military's lethality, the dependence on these technologies also

19 DoD, *The Department of Defense Cyber Strategy* (Washington, DC: DoD, 2015), p. 4.

20 DoD, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: DoD, January 2012), p. 5.

21 Mick Ryan, *Human-Machine Teaming for Future Ground Forces* (Washington, DC: Center for Strategic and Budgetary Assessments, April 2018).

increases, in many ways, the U.S. military's fragility.[22] Information is both a force multiplier and a target in conflict.

Information and the Changing Character of War

The impact of information superiority in war is not new—far from it. Xenophon, writing in the 4th and early 3rd century BC, understood and highlighted the importance of information in Greek competition and conflict.[23] In the 13th century, the Mongols' use of battlefield information dominance laid the foundation for their conquest of Eurasia and the establishment of the Mongol Empire.[24] Although the nature of war remains the same, what has changed is the means. ICTs have become integral to the collection, processing, and dissemination of information on the battlefield. The adaptation and integration of ICTs into weapons platforms, military systems, and in concepts of operation has changed the character of competition and conflict in a way that adds to the salience of information gathering, targeting, and instrumentalization. As a result, some defense analysts argue that ICT-enabled information has become the "most consequential trend" in warfare and that it "may well become the dominant factor in deciding the outcomes of battles, operations, or even wars."[25]

In response to these trends, DoD has sought to ensure that the Joint Force gains and maintains information superiority in battle.[26] As the recent unclassified summary of the 2018 *National Defense Strategy* highlights, ongoing defense investments emphasize capabilities that allow U.S. warfighters to gain and exploit information across multiple domains, all while denying those same advantages to adversaries.[27] However, it is not just information superiority that the DoD seeks to achieve in battle, but decision superiority.[28] These ICT-connected technologies are designed to augment and ideally compress warfighter and commander decision-making time, allowing them to prioritize tactical and operational missions while quickly

22 For an excellent overview of the cyber capability vulnerability paradox, see Jacquelyn Schneider, *Digitally Enabled Warfare: The Capability Vulnerability Paradox* (Washington, DC: Center for a New American Security, August 2016).

23 For more information on intelligence in Classical Greece, see Frank S. Russel, *Information Gathering in Classical Greece* (Ann Arbor, MI: University of Michigan Press, 1999), pp. 5–7.

24 John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2, Spring 1993.

25 Barry Watts, *Countering Enemy "Informationized Operations" in Peace and War* (Washington, DC: Center for Strategic and Budgetary Assessments, 2013), pp. 6–7. See also Zalmay Khalilzad and John White, *Strategic Appraisal: The Changing Role of Information in Warfare* (Santa Monica, CA: RAND Corporation, 1999).

26 See, for instance, Office of the Secretary of Defense (OSD), *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: DoD, 2018), P. 6. The DoD Joint Publication on information operations defines information superiority as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Chairman of the Joint Chiefs of Staff (CJCS), *Information Operations*, Joint Publication 3-13 (Washington, DC: CJCS, November 20, 2014), p. GL-3.

27 Ibid.

28 DoD, *International Science and Technology Strategy for the United States Department of Defense* (Washington, DC: DoD, April 2005), p. 5.

assessing the effects of previous actions. The goal is to out-think and out-decide the enemy through the exquisite and tailored use of information.

ICT-based capabilities have not only improved and condensed decision-making cycles, they have also deepened and expanded areas of competition, blurring the lines between war and peace.[29] ICTs have facilitated more covert and efficient mechanisms of espionage.[30] Cyber tools provide new means to disrupt and corrupt adversary military and civilian systems and networks. Digital propaganda has become a tool to spread true or false information quickly, "priming" a populace to exploit, obstruct, or delegitimize an adversary's military operations.[31] The fusion of big data, behavioral science, predictive analytics, and machine learning has engendered new opportunities for targeted deception and psychological operations.[32] These ICTs present new opportunities to affect an adversaries' tactical, operational, or strategic decisions, providing advantages to those who leverage these technologies and integrate them into their broader mission planning.[33]

The Paradox of ICT-Based Capabilities

ICTs present the United States with a paradox: the same capabilities that provide a warfighting edge also create unique vulnerabilities that adversaries can exploit to their advantage.[34] As a 2018 report from the Office of the Secretary of Defense (OSD) noted, "DoD missions and systems remain at risk from adversarial cyber operations . . . cyber defenses are improving, but not enough to stop adversarial teams from penetrating defenses, operating undetected and degrading missions."[35] U.S. military systems, whether new or legacy, can fall prey to adversary cyber operations against software, hardware, or firmware for the purposes of espionage, sabotage, or subversion (see Table 1).[36]

29 Michael Mazarr, *Mastering the Gray Zone: Understanding the Changing Era of Conflict* (Carlisle, PA: United States Army War College Press, 2015).

30 U.S. China Economic and Security Review Commission (USCC), "China's Intelligence Services and Espionage Threats to the United States," in *2016 Annual Report to Congress* (Washington, DC: USCC, November 16, 2016), Chapter 2, Section 3; and National Counterintelligence and Security Center (NCSC), *Foreign Economic Espionage in Cyberspace* (Washington, DC: Office of the Director of National Intelligence, 2018), available at https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

31 DoD, *Strategy for Operations in the Information Environment* (Washington, DC: DoD, June 2016), p. 2.

32 See, for instance, Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing, 2014), p. 140; and Steve Hosmer, "The Information Revolution and Psychological Effects," in Khalilzad and White, *Strategic Appraisal*, pp. 428–494.

33 Russia's use of information operations during the 2008 Russo-Georgia War and in Ukraine would be an example. See George T. Donovan, *Russian Operational Art in the Russo-Georgian War of 2008* (Carlisle, PA: US Army War College, 2009); and Kenneth Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO Cooperative Cyber Defence Center of Excellence, 2015).

34 Schneider, *Digitally Enabled Warfare*.

35 OSD, Director, Operational Test & Evaluation (DOT&E), *FY 2017 Annual Report* (Washington, DC: DoD, January 2018), p. 315.

36 GAO, *Weapon Systems Cybersecurity*.

TABLE 1: ILLUSTRATIVE CYBER THREATS TO SOFTWARE, HARDWARE, AND FIRMWARE

	Example Vulnerability/Threat	Hypothetical Effect of Vulnerability on Weapon Platform
Software	A malicious actor can exploit vulnerabilities in software that underlie key weapon system capabilities for espionage, sabotage, or subversion.	Vulnerabilities in software associated with an aircraft's distributed aperture system are exploited by a malicious adversary. The integrity of the information is manipulated, providing false information to the pilot on incoming aircraft and missile threats.
Hardware	A malicious actor could attempt to compromise the integrity of the microelectronics supply chain, installing "backdoors" in microelectronics for potential espionage or sabotage.	Compromised microelectronics in a GPS-guided artillery shell are sabotaged by a malicious actor and detonate over friendly forces.
Firmware	A malicious actor could attempt to "brick" (make unusable or unbootable) a machine's firmware for sabotage. Attacks on firmware are particularly insidious, as they can give the attacker persistent access through software updates.	Firmware underlying the electro-optical and infrared (EO/IR) multispectral sensor turrets in an intelligence collection aircraft are sabotaged, resulting in reduced situational awareness.

For more information on vulnerabilities associated with software, hardware, or firmware, see Robert Behler, "Cyber Vulnerabilities in Aviation Today," webinar, Carnegie Mellon University, Software Engineering Institute, November 2015; Marina Malenic, "DoD Chief Tester Warns on F-35 Cyber, Software Issues," *IHS Jane's*, January 26, 2016, available at http://www. janes.com/article/57454/dod-chief-tester-warns-on-f-35- cyber-software-issues; John Villasenor, *Compromised by Design? Securing the Defense Electronics Supply Chain* (Washington, DC: Brookings Institution, November 2013); Roger A. Grimes, "What You Need to Know About Firmware Attacks," *CSO*, August 7, 2012, available at https://www.csoonline.com/article/2618113/security/what-you-need-to-know-about-firmware-attacks.html; and Larry Wyche and Greg Pieratt, "Securing the Army's Weapon Systems and Supply Chain Against Cyber Attack," *ILW Spotlight* 17, no.3, November 2017.

Platform and system vulnerabilities will continue to proliferate. Future combat systems are increasingly complex; many contain embedded processes that correlate data from a diversity of sources, providing the warfighter with an easily digestible assessment of their operating environment for their subsequent decision or action. System complexity increases an adversary's potential attack surface. Each application, function, and interconnection can act as a potential threat vector for exploitation.[37]

Whereas cyberattacks exploit system vulnerabilities, the ultimate goal for an adversary is to undermine the confidentiality, integrity, or availability of information. In combat, the attacks that the military will likely face are availability threats that deny warfighter access to information via electronic or cyber means, such as jamming or distributed denial of service (DDoS) attacks.[38] The confidentiality of information associated with weapon system capabilities and vulnerabilities could be revealed via computer network exploitation. Additionally,

37 System complexity also increases the time it takes for vulnerability discovery and makes those same flaws difficult to ameliorate. For more information, see Dan Ward, *Cybersecurity, Simplicity and Complexity: The Graphic Guide to Making Systems More Secure Without Making Them Worse* (Washington, DC: New America Foundation, March 2016), pp. 7–8.

38 Electronic warfare (EW) is outside the scope of the report. For an in-depth study of EW, to include jamming, see Bryan Clark and Mark Gunzinger, *Winning the Airwaves: Regaining America's Dominance in the Electromagnetic Spectrum* (Washington, DC: Center for Strategic and Budgetary Assessments, 2015); and Bryan Clark, Mark Gunzinger, and Jesse Sloman, *Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance* (Washington, DC: Center for Strategic and Budgetary Assessments, October 2017).

by accessing command and control (C2) networks, adversaries could glean intelligence on operational planning and decision-making. Finally, the integrity of system information via optical, thermal-infrared, laser, or radar sensors, for instance, could be compromised through the insertion of false information. A cyberattack on the integrity of the information itself could undermine confidence in system information, thus causing a general loss of trust in battlespace awareness and C2.

Such scenarios are entirely plausible. U.S. competitors and adversaries—most notably Russia, China, Iran, and North Korea—continuously seek to optimize their targeting of U.S. platforms and battle networks and undermine U.S. operational concepts. As part of Russia and China's informationized strategies, Moscow and Beijing aim to achieve information dominance by focusing their operations on U.S. centers of information gravity, negating the U.S. ability to exploit accurate information for strategic, operational, or tactical ends.[39] Although information dominance can be accomplished via conventional or electronic means, cyber has emerged as a key pillar of their informationized strategies.[40] Indeed, from the employment of cyber and information operations in the 2008 Russo-Georgian War to the blending of electronic, information, and cyber operations in Ukraine, it is clear that Moscow plans to fight and win partially through cyber means.[41] The Kremlin employs cyber operations to "delay, deceive, 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.[42] Likewise, China plans to fight and win "informationized local wars" in its near abroad, employing cyberattacks as part of a broader A2/AD strategy to target C2, air defense systems, missile launch positions, and logistics centers.[43] Meanwhile, Iran is considering the battlefield use of cyber to sabotage C2,

39 See, for instance, Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts," *The Journal of Slavic Military Studies* 27, no. 1, 2014; and Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017).

40 See, for instance, Amy Chang, *Warring State: China's Cybersecurity Strategy* (Washington, DC: Center for New American Security, December 2014); Timothy L. Thomas, *Decoding the Virtual Dragon* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007); Roland Hickerö, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Stockholm, Sweden: FOI: Swedish Defence Research Agency, 2010), p. 13; and "Military Doctrine of the Russian Federation," press release, Office of the President of the Russian Federation, December 25, 2014, available at https://rusemb.org.uk/press/2029.

41 Donovan, *Russian Operational Art in the Russo-Georgian War of 2008*, and Geers, *Cyber War in Perspective*.

42 Keir Giles, *Handbook of Russian Information Warfare* (Rome, Italy: NATO Defense College, December 2016), available at http://www.ndc.nato.int/news/news.php?icode=995; and Ben Buchanan and Michael Sulmeyer, *Russia and Cyber Operations: Challenges and Opportunities for the Next U.S. Administration* (Washington, DC: Carnegie Endowment for International Peace, December 2016), available at http://carnegieendowment.org/2016/12/13/russia-and-cyber-operations-challenges-and-opportunities-for-next-u.s.-administration-pub-66433.

43 Thomas, *Decoding the Virtual Dragon*, pp. 31–32; Roger Cliff et al., *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States* (Santa Monica, CA: RAND Corporation, 2007); Evan Braden Montgomery, "Contested Primacy in the Western Pacific: China's Rise and the Future of U.S. Power Projection," *International Security* 38, no. 4, Spring 2014; and James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrines, Organizations, and Capability," in Roy Kamphausen et al., *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle, PA: Strategic Studies Institute, US Army War College, 2009), p. 263.

aerial and naval unmanned systems, logistics, and missile defense networks.[44] Similarly, North Korea plans to target U.S. and South Korean command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) in the early phases of conflict via cyber means as part of its "quick war, quick end" strategy.[45]

Apart from exploiting vulnerabilities in key weapon platforms or systems, adversaries are identifying other ICTs by which they can target U.S. access to credible information and disrupt decision-making. Indeed, Russia, China, Iran, and North Korea's strategies all emphasize the importance of shaping their region's information environment to the detriment of U.S. military and allied forces.[46] The use of propaganda, disinformation, strategic leaks, and deception all support these strategies by propagating false and insidious narratives that may undermine friendly force missions, undercut local support, or muddy the cognitive waters of military decision makers.

A Paradigm Shift from Information Assurance to Mission Assurance

Efforts are ongoing in the United States to address these ICT-based risks. The FY 2016 National Defense Authorization Act (NDAA) tasked the Secretary of Defense with evaluating all major weapon systems for cyber vulnerabilities by December 31, 2019.[47] Meanwhile, the OSD Director, Operational Test and Evaluation (DOT&E) is also pressing for all ICT-based systems to undergo cybersecurity testing.[48] Although these efforts are to be commended, they still fall short of U.S. needs. Merely identifying vulnerabilities in platforms and systems and subsequently patching them is not enough. Information assurance is not an end goal, but a moving target. U.S. military systems and networks will never be entirely secure. Each new system, interconnection, or software update will create new vulnerabilities. Information assurance efforts should be geared toward mitigating the cyber threat while working toward the more critical goal of mission assurance.[49]

44 Michael Eisenstadt, "Iran's Lengthening Cyber Shadow," *Research Notes*, The Washington Institute for Near East Policy, July 2016; and Michael Eisenstadt, "Cyber: Iran's Weapon of Choice," *The Cipher Brief*, January 29, 2017, available at https://www.thecipherbrief.com/cyber-irans-weapon-of-choice-2.

45 Jenny Jun et al., *North Korea's Cyber Operations: Strategy and Responses* (Washington, DC: Center for Strategic and International Studies, December 2015).

46 See, for instance, Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2001); Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, DC: Potomac Books, Inc., 2009), pp. 10–11; Ladan Yazdian, "The Strategies and Methods of Iranian Irregular War," in Ilan Berman, ed., *The Logic of Irregular War: Asymmetry and America's Adversaries* (Lanham, MD: Rowman & Littlefield, 2017); and Jun et al., *North Korea's Cyber Operations*, p. 2.

47 National Defense Authorization Act (NDAA) FY 2016, Section 1647.

48 OSD, DOT&E, *FY 2017 Annual Report*, p. 317.

49 For more on adopting a posture of mission assurance, see William J. Bender, "The Cyber Edge: Posturing the US Air Force for the Information Age," *The Mitchell Forum*, no. 15, August 2017; Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016), p. 161; and Don Snyder, George E. Hart, Kristin F. Lynch, and John G. Drew, *Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems: Guidance for Where to Focus Mitigation Efforts* (Santa Monica, CA: RAND Corporation, 2015).

Mission assurance seeks to ensure the continued performance of capabilities and assets in support of DoD mission-essential functions and overarching strategic objectives.[50] As the DoD reorients toward multi-domain operations, tactical and operational leaders should work more seamlessly between domains to support, augment, or assure their mission's success in any future operating environment.[51] Indeed, it is impossible to entirely deny an adversary the ability to shape aspects of the information environment. As a result, the U.S. military's goal should be to sustain military operations *in spite of* a denied, disrupted, or subverted information environment.

Two overarching factors determine the impact of a cyber or informationized attack on a military system.[52] The first, how gracefully a system degrades due to an attack, is largely a function of technical design. 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*. U.S. warfighters should be trained to fight as an integrated whole in and through an increasingly contested and complex battlespace saturated by adversary cyber and information operations. As General Robert Brown, then-commanding general of the Army Combined Arms Center, noted, what the United States needs is "individuals who improve and thrive in conditions of uncertainty and chaos." What is required, therefore, is greater "institutional agility," that provides for "realistic training that replicates the complexity of the world," and furnishes the "ability to out think the adversary and figure a way out of complex situations."[53]

The battle for information control should drive training adaptation to provide warfighters the experiential learning that translates into quick reflexes, critical thinking, and cross-domain synergies on the battlefield.[54] Ideally, training emphasis should be placed on finding a new or creative route to victory despite a denied, degraded, or spoofed environment. As we shall see in the following chapter, however, current training has yet to fully and successfully adapt to these fundamental changes in the character of military competition.

50 For more information on mission assurance, see "Mission Assurance," DoD Directive 3020.40, November 29, 2016; and "Mission Assurance Construct," DoD Instruction 3020.45, August 14, 2018.

51 Albert Harris III, "Preparing for Multidomain Warfare: Lessons from Space and Cyber Operations," *Air and Space Power Journal* 32, no. 3, Fall 2018.

52 Snyder, Hart, Lynch, and Drew, *Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems*.

53 Lisa Ferdinando, "Carson: Changes Needed in Army's 'Archaic' Retention, Promotion System," *US Army*, October 17, 2014, available at https://www.army.mil/article/136395.

54 For more on the need for training to reflect future conflict, see Defense Science Board Task Force, *Training for Future Conflict* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, June 2003), p. 10; and Donald E. Vandergriff, *Today's Training and Education (Development) Revolution: The Future is Now!* (Arlington, VA: The Institute of Land Warfare, April 2010), p. 2.

CHAPTER 2

Current U.S. Training for a Contested and Complex Battlespace

Since more than a century ago, when the rifle bullet began its reign over the battlefield and soldiers slowly became aware that the day of close-order formations in combat was forever gone, all military thinkers have pondered the need of a new discipline. It has been generally realized that fashioning the machine to man's use in battle was but half of the problem. The other half was conditioning man to the machine. The mechanisms of the new warfare do not set their own efficiency rate in battle. They are ever at the mercy of training methods which will stimulate the soldier to express his intelligence and spirit.

S. L. A. Marshall[55]

This was the first time I'd ever held a real gun. Even so, the weapon felt familiar in my hands, because I'd fired thousands of virtual firearms in the OASIS.

Wade Watts[56]

This chapter assesses current U.S. cyber and informationized training for the non-cyber warfighter. It begins by assessing how the U.S. armed forces presently train warfighters at the tactical and operational level to withstand and fight through adversary cyber and informationized attacks. It then highlights the limitations associated with current training techniques, particularly live training, for simulating adversary cyber and informationized operations. Although it contends that live training risks can be averted through the employment

55 S. L. A. Marshall, *Men Against Fire: The Problem of Battle Command* (Norman, OK: University of Oklahoma Press, 1947), p. 22.

56 Quote by character Wade Watts in Ernest Cline, *Ready Player One* (New York: Broadway Books, 2011), pp. 300–301.

of synthetic training, it highlights the current difficulties and sensitivities associated with modeling and simulating cyber effects in a synthetic environment.

The chapter then reflects on current opportunities for the non-cyber warfighter to train alongside cyber warriors for multi-domain operations. It argues that current techniques fail to train non-cyber warriors to exploit the potential opportunities of working alongside the cyber domain to assure mission success. However, ongoing research within the scientific community may provide a future synthetic training environment that supports integrated training across Services and domains.

Current Training to Fight through a Contested and Complex Battlespace

The U.S. military Services are beginning to conceptualize how to train non-cyber warriors to maintain mission assurance in an information-saturated, hyper-connected battlespace. At present, however, a high-fidelity training environment that realistically simulates the effects of cyber or informationized attacks remains somewhat aspirational. Cyber training for the non-cyber warrior is not yet fully developed across the Services and combatant commands (COCOMs). In a series of interviews in 2016 with U.S. Air Force (USAF) instructor pilots and squadron commanders, Lt. Col. Jason Settle noted a general lack of awareness of the threats a cyberattack could pose to their respective weapon systems. Although aircrews receive an assortment of threat information during initial weapons training, the impact of cyberattacks on weapons platforms have not yet been fully integrated into aircrew training.[57] The still partial nature of this evolution in combat training is best demonstrated by the role of cyber operations in Red Flag—the Air Force's premier combat training exercise.[58] Red Flag does include a cyber component, which provides airmen some insight into the detrimental effects of a cyberattack on their tactical mission, but the integration of cyber effects into Red Flag is largely viewed as a novelty by those airmen that participate in the exercise.[59] Cyber effects are not yet incorporated into training at an airman's home station, which can lead to skills decay, or worse, a false sense of confidence about the scope and significance of the cyber threat.[60] Concerns over cyber threats, such as the potential loss of GPS, have also driven changes in Navy training. In 2011, the Navy reinstated celestial navigation training for quartermasters and junior officers, which was subsequently expanded in 2016 for midshipmen.[61] Yet, despite

57 Jason R. Settle, *Cyber Threat Awareness for the Warfighter* (Maxwell AFB, AL: Air War College, Air University, February 16, 2016), p. 4.

58 For more on the USAF Red Flag exercise, see "Nellis Air Force Base Flying Operations," Nellis Air Force Base Official United States Air Force Website, available at http://www.nellis.af.mil/Home/Flying-Operations/.

59 For more information, see Brick Eisel, "Space and Cyber at Red Flag," *Air Force Magazine,* September 2017, available at http://www.airforcemag.com/MagazineArchive/Pages/2017/September%202017/Space--Cyber-at-Red-Flag.aspx.

60 Settle, *Cyber Threat Awareness for the Warfighter*, pp. 4–6.

61 Kyle Cregge, "Automated Celestial Navigation for the Navy," *The Maritime Executive* blog, December 13, 2017, available at https://www.maritime-executive.com/blog/automated-celestial-navigation-for-the-navy.

these initial efforts, a gap currently exists at the tactical level for the integration of cyber effects into traditional tactical kinetic training programs.[62]

To the extent cyber is integrated into training events, the focus has primarily been on networks and mission command systems. Indeed, since 2011, the Army's opposing force (OPFOR) has simulated state-level cyberattacks against Army Battle Command Systems at Combat Training Centers (CTCs) for corps, division, and brigade-level exercises. This training has provided crucial insight for system administrators and commanders on the need to protect mission command systems during battle. However, this training is not fully integrated across the Army, to include tactical-level training and operational decision-making above the brigade level.[63]

Per a 2018 OSD report, "Although directed by the Chairman of the Joint Chiefs of Staff in 2011, and endorsed by two subsequent Secretaries of Defense, DOT&E has not observed many demonstrations that Commands can 'fight through' a major cyberattack and sustain their critical missions."[64] Furthermore, when cyber operations are included in large-scale Service or COCOM exercises, they are often employed in parallel to live training.[65] As a former USAF senior leader explained when commenting on past Red Flag exercises, the computer network defense exercise often takes place in a separate facility, and is thus, "not fully integrated across the fight."[66] This observation was echoed by former warfighters when commenting on COCOM exercises.[67] Non-cyber warfighters do not necessarily experience the effects of "cyber play" while it is ongoing.

The Limitations of Integrating Cyber Effects into Live Training

When computer network defense exercises are included in non-cyber warrior training, they are often combined into live exercises at a later point.[68] Cyber injects are often done via white carding, which is the literal use of a note card intended to represent cyber friction. When a

62 Jonathan Butts and Michael Glover, *Developing a Tactical Environment Cyber Operators Training Program* (Virginia Beach, VA: McKellar Corporation, January 31, 2015), p. 2.

63 Marshall et al., *Cyber Operations Battlefield Web Services (COBWebS)*, p. 4.

64 OSD, DOT&E, *FY 2017 Annual Report*, p. 319.

65 Live simulation involves real people training on physical ranges with actual assets. Like Maverick in the 1986 drama *Top Gun*, live training allows people and their platforms to train in the real environment, allowing them to experience the dirt, dust, and sweat of combat on their equipment. See National Training and Simulation Association (NTSA), *A Primer on Modeling and Simulation* (Arlington, VA: NTSA, December 2011), pp. 11–12.

66 Author interview with U.S. Air Force Brig. Gen. (ret.) Bruce McClintock, October 11, 2017.

67 Jennifer McArdle, "Rethinking Cyber Training for the Non-Cyber Warrior: Conference Findings," Pell Center for International Relations and Public Policy, forthcoming in 2019.

68 For more on the use of white carding during a live fire exercise, see Jen Judson, "US Army Moves to Improve Electronic Warfare Tactics," *Defense News,* July 15, 2016, available at https://www.defensenews.com/land/2016/07/15/us-army-moves-to-improve-electronic-warfare-tactics/; and Wells and Bryan, "Cyber Operational Architecture Training System," p. 2.

simulation or exercise can't emulate a scenario, an instructor is able to use a note card as a rudimentary inject tool. The trainees are meant to respond as if the event happened, and a debrief happens later. Although this provides warfighters some insight into how their systems or platforms could be affected in the event of a cyberattack, the lack of realism precludes them from experiencing and subsequently troubleshooting that attack.

Avoiding the introduction of genuine cyber effects in live exercises occurs for the same reason live fire isn't necessarily used against U.S. troops in training. The use of live fire against a military platform could have unintended consequences and potentially put trainees and the platform at risk. Given the importance of military directives aimed at ensuring safety, unit commanders are often hesitant to inject variables into training that could unintentionally have adverse consequences. Safety concerns are a considerable factor in delaying or preventing more seamless cyber incorporation in exercises.

Yet, perhaps more unique to cyber, the Services and COCOMs are often hesitant to integrate realistic cyber effects into major exercises because of its potential for cascading failure.69 As Brig. Gen. (ret.) Bruce McClintock explained, "Exercises sometimes have to limit the potential effects of a devastating cyberattack in order to ensure other exercise objectives are met."[70] Warfighters need to be trained to all mission essential tasks outlined for an exercise, not just the cyber related training goals. When one considers the sheer organizational and personnel costs associated with holding Red Flag or a comparable-in-size joint exercise, the risks of inadvertently sabotaging the exercise via a live cyberattack exponentially increases. Finally, conducting cyberattacks in a live environment on weapon platforms risks exposing platform vulnerabilities to inquisitive adversaries. Put simply, the live training environment is not conducive to simulating a contested and complex battlespace saturated by adversary cyber operations.

The Drive for Synthetic Training

This hesitation to inject cyber effects into a live environment should not preclude the DoD from training for a future contested and complex battlespace. As the *Joint Training Manual for the Armed Forces of the United States* notes, "The 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."[71] Indeed, a failure to integrate cyber or informationized effects into training will lead to inadequate preparation for the changing character of conflict and competition. The

69 For more on the potential for cascading effects and cascading failure in interdependent networks, see Dong-Hoon Shin, Dajun Qian, and Junshan Zhang, "Cascading Effects in Interdependent Networks," *IEEE Network*, July/August 2014.

70 Author interview with U.S. Air Force Brig. Gen. (ret.) Bruce McClintock. See also Angus Batey, "Military Cyber Training Still Tough Problem to Solve," *ShowNews,* July 17, 2018, available at http://m.aviationweek.com/farnborough-airshow-2018/military-cyber-training-still-tough-problem-solve.

71 CJCS, *Joint Training Manual for the Armed Forces of the United States*, CJCSM 3500.03E (Washington, DC: CJCS, April 20, 2015), p. G-F-1.

live training risks previously identified could be circumvented through high-fidelity synthetic training.

Synthetic training broadly falls into four different categories: virtual simulations, constructive simulations, gaming, and augmented reality.

1. *Virtual Simulations: Real People Operating Synthetic Systems*
   Popularized in society's collective imagination by Orson Scott Card in his novel *Ender's Game,* virtual simulation allows warfighters to perfect their skills in a virtual world prior to the crucible of combat. Virtual simulation can run the gamut of devices from a simple virtual reality headset to a multi-million dollar full-motion simulator that replicates with a high level of fidelity the interior of a fighter jet, submarine, or other military platform. Simulators will mimic the performance characteristics of military platforms, their instrumentation, communication links, battle networks, and the environment within which a conflict may occur.[72]

2. *Constructive Simulations: Synthetic People Operating Synthetic Systems*
   A constructive simulation is a computer program. The people, platforms, and the environment are simulated. Simulated people and platforms, often called computer generated forces (CGF), model the behavior of military entities, to include military forces, civilians, and other individuals necessary for the simulation. Constructive simulations can take multiple forms, both semi-automated and fully automated. Semi-automated constructive simulations involve some human input prior to the CGFs carrying out their assigned function. Fully automated CGFs, on the other hand, employ artificial intelligence as a replacement to human intervention.[73] Constructive simulations can be used for training, defense planning, operations, and acquisitions.[74]

3. *Gaming: Video Games as Training Tools*
   The U.S. military has experimented with modifying popular commercial video games to meet their training needs since the 1980s, when Atari unveiled its pioneering *Battlezone* arcade game. Following *Battlezone*'s success, the U.S. Army's Training and Doctrine Command (TRADOC) solicited Atari's assistance in generating a unique Army version of *Battlezone* that could train soldiers to operate the Bradley infantry vehicle. *Army*

72 Roger D. Smith, *Military Simulation and Serious Games* (Orlando, FL: Modelbenders LLC, 2009), p. 15. An emerging technology in this area is the dynamic synthetic environment, a virtual world that evolves during training or mission rehearsal. For more information, see "CAE Dynamic Synthetic Environment," Canadian Aviation Electronics datasheet, available at https://www.cae.com/media/media-center/documents/datasheet.CAE.Dynamic.Synthetic.Environment.pdf.

73 Fully automated CGFs exist, but their intelligence is not strong enough to make high-fidelity decisions for training. When realism is required, semi-automated CGF are employed, but this could change in the future.

74 Uwe Dompke, "Computer Generated Forces: Background, Definition and Basic Technologies," in Research and Technology Organisation (RTO)/NATO, *Simulation of and for Military Decision Making*, RTO lecture series 222 (Neuilly-sur-Seine, France: RTO/NATO, June 2003), pp. 7-1–7-14, available at https://pdfs.semanticscholar.org/1af7/7641059c2996d0f24d0c9e7cf95cb874ea71.pdf; and Nacer Abdellaoui, Adrian Taylor, and Glen Parkinson, *Comparative Analysis of Computer Generated Forces' Artificial Intelligence* (Ottawa, Canada: DRDC Ottawa and xplorenet, October 2009), available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a567877.pdf.

Battlezone, also known as the *Bradley Trainer*, while produced, was never used.[75] However, since that time, a slew of military video games has built on the burgeoning popularity of the commercial video game industry. From first-person shooter games, like *Marine Doom* to *UrbanSim,* which teaches warfighters the complexity of counterinsurgency operations, the military has sought to blend work and play, harnessing the gaming proclivities of younger generations of recruits for training purposes. Educational video games, at times referred to as "serious games," have now been utilized by the armed forces for training, recruitment, and the psychological well-being of troops, to include sexual harassment training and post-traumatic stress disorder.[76]

4. *Augmented Reality: Combining the Physical World with a Virtual Overlay*
   Augmented reality combines elements of both the physical and virtual environments in one setting. Typically, augmented reality applications overlay virtual images on the physical world, much like Google Glass or Pokémon GO. Military leaders are utilizing augmented reality technologies on training sites, such as the Marine Corps Base at Camp Pendleton in California. Camp Pendleton includes an indoor and outdoor training facility, which incorporates mock villages. Throughout training scenarios, the Services will employ actors to act as adversaries. However, under law, child actors cannot be employed, and children are important to training scenarios. As an example, should a soldier be on patrol and find children missing from a village, that should raise the alarm; it is often a sign of an impending attack. Augmented reality allows for virtual children to be superimposed onto the physical environment, providing a higher level of realism in training.[77]

Although these synthetic training environments can be used in a compartmentalized fashion, militaries argue that the future of training lies in their fusion into one single synthetic environment that seamlessly links to the live training environment. Referred to as LVC (live, virtual, and constructive), this training integrates the virtual and constructive training environments with the live environment through a network such as the distributed mission operations

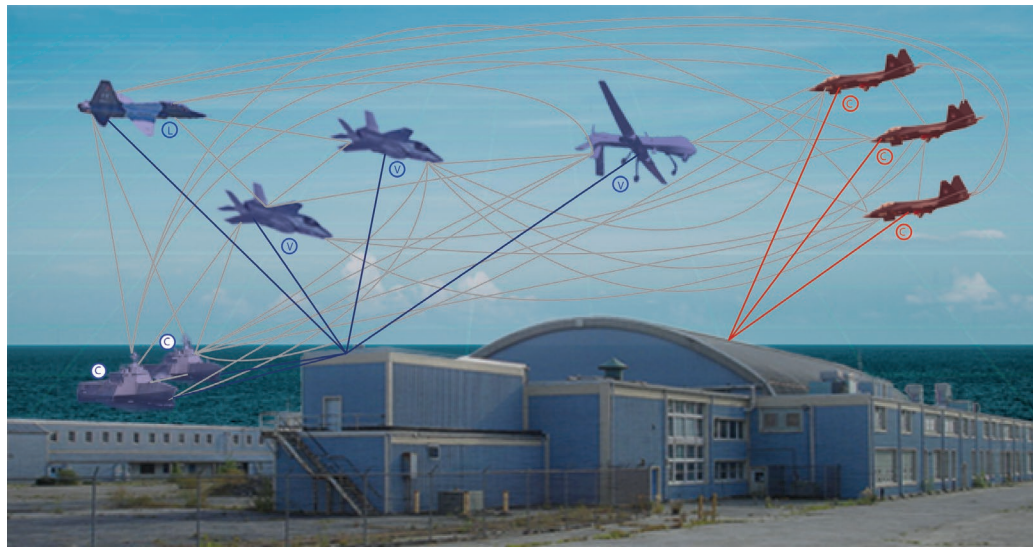
75 Corey Mead, *War Play: Video Games and the Future of Armed Conflict* (New York: Houghton Mifflin Harcourt Publishing Co., 2013), p. 18.

76 Ibid.

77 Vivienne Machi, "The Future of Training and Simulation: Preparing Warfighters for Tomorrow's Battlefields," *National Defense* Magazine, December 2017, p. 29.

network (DMON).[78] For instance, LVC training links live aircraft with manned simulators in the virtual world and computer-generated constructive forces.

FIGURE 1: DEPICTION OF LIVE, VIRTUAL, AND CONSTRUCTIVE (LVC) ASSETS INTEGRATED FOR MISSION REHEARSAL



An LVC environment can mimic adversary cyber operations with higher fidelity. In his prepared statement for the House and Senate Armed Services Committees on the USAF's Appropriations for FY 2015, then-USAF Deputy Assistant Secretary David Walker noted that "the training need for LVC is real while training costs are increasing and threat environments are complex. In particular, realistic training for anti-access/area-denial environments is not available." After reporting on the success of LVC demonstrations, he concluded that "LVC S&T has the capability to provide greater focused training for our warfighters across a range of operational domains such as tactical air, special operations, cyber, [intelligence, surveillance, and reconnaissance] ISR, and C2."[79]

78 The DMON is a high-performance wide-area network used for inter-team training for combat air forces. For more information, see "Distributed Mission Operations Network (DMON)," Northrop Grumman brochure, 2013, available at http://www.northropgrumman.com/Capabilities/LiveVirtualConstructive/Documents/DMON_brochure.pdf. For more on distributed simulation exercises, see S. K. Numrich and Amy Henninger, *Need for Agility in Security Constraints for Distributed Simulation*, submission to the 19th International Command and Control Research and Technology Symposium (Alexandria, VA: Institute for Defense Analyses, June 2014), available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a606952.pdf. Of note, the Army's planned future synthetic training environment incorporates the LVC environments with gaming and mixed reality. See TRADOC/Combined Arms Center—Training (CAC-T), *Synthetic Training Environment White Paper*, draft (Fort Eustis, VA/Fort Leavenworth, KS: TRADOC/CAC-T, 2017), available at https://usacac.army.mil/sites/default/files/documents/cact/STE_White_Paper.pdf.

79 Dr. David E. Walker, prepared statement to the Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, hearing on Department of Defense Authorization for Appropriations for Fiscal Year 2015 and the Future Years Defense Program, April 8, 2014, available at https://www.govinfo.gov/content/pkg/CHRG-113shrg91190/html/CHRG-113shrg91190.htm.

Large-scale exercises currently include a range of synthetic assets that increase the fidelity of tactical and operational training events. Indeed, 2017's exercise NORTHERN EDGE linked the USAF's DMON with the Navy's network, thus integrating approximately 6,000 participants located across the United States operating LVC assets. The exercise sought to strengthen participants' tactical combat skills, C2, and communications, with the aim of cultivating interoperable plans and programs across the joint force.[80] Other exercises, like the USAF's COALITION VIRTUAL FLAG and the RAF's RED KITE fulfill a similar function—integrating geographically remote participants in a complex and contested virtual environment.[81] Modeling and simulating cyber effects over these synthetic assets or in a broader synthetic training exercise should provide warfighters some insight into how a cyber or informationized attack will impact their system or mission. However, modeling and simulating a constructive cyberattack is not a straightforward process.

The Difficulties and Sensitivities Associated with Modeling and Simulating Cyber Effects

The effects of a cyberattack, unlike a conventional weapon, are not dependent on the weapon or, more specifically, malware; the effects of a cyberattack are based on the system the malware is targeting.[82] This calls for deep knowledge of how the system works, its specifications, and how it fits into its broader battle network.[83] These insights would need to evolve as the platform changes with each software update and each new interconnection.[84] This information is often highly classified, particularly on the military's more exquisite platforms. However, many training simulations that replicate different warfighting tasks in use by the military are unclassified. As a result, such expertise may not be readily available to inform the modeling and simulation of cyber effects. Moreover, cyber exploits are continuously evolving to reflect the tacit knowledge gained by the hacking community. What an adversary chooses

80 For more information on exercise NORTHERN EDGE, see Steven Doty, "Believe the Unbelievable: Exercise NORTHERN EDGE 17 Enhances Interoperability with Live, Virtual, Constructive Training," *Eielson Air Force Base News,* May 4, 2017, available at http://www.eielson.af.mil/News/Article-Display/Article/1173704/believe-the-unbelievable-exercise-northern-edge-17-enhances-interoperability-wi/; and Alaskan Command Office of Public Affairs, "Alaskan Command Announces Exercise Northern Edge 2017, May 1-12," *U.S. Indo-Pacific Command News*, April 24, 2017, available at http://www.pacom.mil/Media/News/News-Article-View/Article/1158423/alaskan-command-announces-exercise-northern-edge-2017-may-1-12/.

81 For more on exercises VIRTUAL FLAG and RED KITE, see Srivari Aishwarya, "US, UK, Australia and Canadian Air Forces Conduct Coalition Virtual Flag Exercise," *Air Force Technology*, September 15, 2016, available at http://www.airforce-technology.com/uncategorised/newsus-uk-australia-and-canadian-air-forces-conduct-coalition-virtual-flag-exercise-5007228/; and "QinetiQ Enables Largest Synthetic Training Exercise at RAF Waddington," *QINETIQ blog*, June 19, 2017, available at https://www.qinetiq.com/blogs/2017/06/qinetiq-enables-largest-synthetic-training-exercise-at-raf-waddington.

82 This does not include DDoS and border gateway protocol (BGP) hijacking. For more on BGP hijacking, see Zach Julian, "An Overview of BGP Hijacking," *Bishop Fox Blog,* August 17, 2015, available at https://www.bishopfox.com/blog/2015/08/an-overview-of-bgp-hijacking/.

83 For more on battle networks, see John Stillion and Bryan Clark, *What it Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, DC: Center for Strategic and Budgetary Assessments, 2015).

84 Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016), p. 129 and 148.

to target and how they have structured an exploit will have different effects on a system. Perhaps more importantly, if the military is aware of a vulnerability in a platform or system, they will not leave that vulnerability open on a system for training purposes, choosing instead to immediately patch it. Therefore, it is likely impossible to model all the possible effects of a cyberattack on a system with accuracy.

Given these challenges, simulating cyber effects for the non-cyber warfighter have been rare experiments.[85] To date, experiments such as the Cyber Operational Architecture Training System (COATS) and the Cyber Operations Battlefield Web Services (COBWebS) have replicated the effect of a cyberattack on traditional command-level training simulations.[86] Although useful first steps, these experiments have yet to integrate tactical-level cyber effects on warfighter platforms. Moreover, automated approaches, an essential facet of CGFs, that integrate simulated cyber effects are still in their infancy. As a result, leading industry defense training corporations are not yet integrating cyber effects into their simulations for conventional warfighters. As Gene Colabatistto, the Group President of CAE's Defense and Security group recently noted, "At the moment, we don't do that. We are looking, as part of our business, and in particular as a training company, at the cyber environment as another domain we would like to actually be training operators in—but we don't do that today."[87]

Despite these difficulties, as we will see in greater depth in the following chapter, developing a suite of simulated cyber effects is still helpful, even if the CGFs are slightly divorced from reality. Training emphasis should not be placed on rote memorization in the face of adversary cyber operations, but instead on the warfighter finding a new or creative route to victory.

Current Training for Multi-Domain Operations

Integrating cyber events into non-cyber warrior training does not just require simulating the effect of an adversary's cyber operations in a synthetic training environment. Warfighters must also understand the unique attributes that cyber brings to the fight when prosecuting multi-domain operations (see appendix). Training opportunities must support non-cyber warfighters to train alongside cyber warriors in a synthetic training environment to exploit cyber advantages. Indeed, as former Secretary of Defense James Mattis directed, warfighters

85 More broadly, challenges associated with integrating different synthetic environments have created difficulties. For instance, interoperability constraints with legacy simulators, non-consistent standards, and security and classification concerns pose challenges when linking synthetic environments together. For more information, see Jerry M. Couretas, *An Introduction to Cyber Modeling and Simulation* (Hoboken, NJ: John Wiley & Sons, 2019), loc. 2099; and James Rapp, "LVC Training to Enhance Operational Readiness," Presentation to the Williams Foundation, Canberra, Australia, August 10, 2016, available at http://www.williamsfoundation.org.au/resources/Documents/WF_AIRSEA_160810_Rapp.pdf.

86 See Wells and Bryan, "Cyber Operational Architecture Training System"; and Marshall et al., *Cyber Operations Battlefield Web Services (COBWebS)*.

87 CAE was formerly known as Canadian Aviation Electronics. Batey, "Military Cyber Training Still Tough Problem to Solve."

should experience 25 realistic bloodless battles in simulators before the first fight.[88] These bloodless battles should mimic current and future multi-domain operations.

Synthetic environments exist for cyber and informationized training, but these environments are often siloed. They are incompatible with conventional simulations employed to train non-cyber warfighters and battle staff.[89] Synthetic training environments for cyber and information operations 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, the United States has developed realistic, closed-network cyber ranges (the DoD Cybersecurity Range, the Joint Information Operations Range (JIOR), and the National Cyber Range) to train cyber warriors in a range of tactics, techniques, and procedures for offensive and defensive computer network operations.[90] The aim of the nascent Persistent Cyber Training Environment (PCTE) is to provide a cloud-based continual and realistic environment to better train the cyber mission force.[91] While these ranges provide valuable training opportunities for the cyber mission force, they operate independently of traditional kinetic mission training programs for the conventional warfighter and battle staff. As a result, synthetic training for cyber operators often concentrates solely on the cyber components of operations, at times to the detriment of the broader battlefield picture.[92] Likewise, little insight is provided to warfighters and commanders on how the cyber domain may influence their mission. Overall, few opportunities exist for conventional warfighters to develop an understanding of what cyber can bring to the fight.

88 Mattis' comments were directed towards the infantry, but naturally, such a statement could have a wider application. Jen Judson, "25 Bloodless Battles: Synthetic Training Will Help Prepare for Current and Future Operations," *Defense News*, September 5, 2018, available at https://www.defensenews.com/smr/defense-news-conference/2018/09/05/25-bloodless-battles-synthetic-training-will-help-prepare-for-current-and-future-operations/.

89 Wells and Bryan, "Cyber Operational Architecture Training System," p. 1.

90 For an overview of cyber ranges, in particular U.S. cyber ranges, see Jon Davis and Shane Magrath, *A Survey of Cyber Ranges and Testbeds* (Edinburgh, Australia: Australian Department of Defence, Defence Science and Technology Organisation [DSTO], 2013), available at https://pdfs.semanticscholar.org/687f/f7737f9e32b85cf885db88341b73892aa8ae.pdf.

91 Contracts for the initial prototype of the PCTE were awarded in June 2018. Mark Pomerleau, "4 Companies Start Work on the Army's Cyber Training Platform," *Fifth Domain*, June 19, 2018, available at https://www.fifthdomain.com/dod/army/2018/06/19/4-companies-start-work-on-the-armys-cyber-training-platform/.

92 Brett Lindberg, Stephen Hamilton, Brian Lebiednik, and Kyle Hager, "Cyber Integrating Architecture," *Small Wars Journal*, July 27, 2018, available at http://smallwarsjournal.com/index.php/jrnl/art/cyber-integrating-architecture.

Simulations for information operations also present similar problems. At present, two approaches are commonly employed when modeling and simulating information operations: a technical and social science approach.[93] The technical approach tends to focus on the information dimension of the information environment, placing technical emphasis on the means by which information can be disrupted between the physical and information layers of cyberspace for activities like C2. Since information operations can be employed via cyber or electronic means, these simulations could include cyber ranges or synthetic environments that train for electronic attack.

The social science approach focuses on the cognitive dimensions of the information environment. Simulations under this approach are centered on building warfighter cultural understanding, raising awareness of personal assumptions and biases, or helping to clarify adversary intent in gray zone conflicts.[94] For example, the Defense Advanced Research Projects Agency (DARPA) developed a video-game called *Tactical Iraqi*, which sought to train soldiers on Baghdad Arabic, Iraqi culture, and non-verbal messaging.[95] Aptima's Cultural Awareness for Marines Operation (CAMO) program and the University of Southern California's Bilateral Negotiation Trainer (BiLAT) provide immersive synthetic environments to build cultural understanding and engagement whether a warfighter is stationed at their home base or deployed.[96] The Jet Propulsion Laboratory's Athena simulation software has been paired with a Joint Communication Simulation System (JCSS) to model the second- and third-order effects of an alleged U.S. cyberattack against critical infrastructure on local perceptions and subsequent actions.[97] DARPA's Compass program seeks to reduce ambiguity

93 See A. Tolk, "Modeling Communications, Command, and Control," and S. K. Numrich and P. M. Picucci, "New Challenges: Human, Social, Cultural, and Behavior Modeling," in Andreas Tolk, ed., *Engineering Principles of Combat Modeling and Distributed Simulation* (New York: Wiley and Sons Inc., 2012); Ariane Bitoun, Antony Hubervic, and Yann Prudent, "M&S for Influence Operations," NATO STO-MP-MSG-149-07, NATO Modeling and Simulation Group (NMSG) Symposium, Lisbon, Portugal, October 19–20, 2017; and Sean Deller et al., "Applying the Information Age Combat Model: Quantitative Analysis of Network Centric Operations," *The International C2 Journal* 3, no. 1, 2009 (Special Issue: Modeling and Simulation in Support of Network-Centric Approaches and Capabilities). The ideas discussed in these paragraphs were developed in part through a review of these sources and an exchange of ideas with information warfare expert LtCol James Rob McGrath.

94 For more on the need to build cultural understanding for military operations, see Barak Salmoni and Paula Holmes-Eber, *Operational Culture for the Warfighter: Principles and Applications* (Quantico, VA: Marine Corps University, 2008), p. 6; and Bitoun, Hubervic, and Prudent, "M&S for Influence Operations," p. 7-2.

95 Mead, *War Play*, p. 54.

96 See "Aptima Develops Cultural Awareness Trainer for Marine Corps Operations," *ASDNews*, May 20, 2013, available at http://www.asdnews.com/news-49140/aptima_develops_cultural_awareness_training_for_marine_corps_operations.htm; and "Bilateral Negotiation Trainer," *USC Institute for Creative Technologies*, June 2012, available at http://ict.usc.edu/wp-content/uploads/overviews/BiLAT_Overview.pdf.

97 Tony Cerri and Neil Sleevi, "Simulation of Cyber Impacts on PMESSII-PT Variables," Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), paper no. 16113, 2016. For more on the Athena PMESII simulation, see Brian Kettler and Jennifer Lautenschlager, "Expeditionary Modeling for Population-Centric Operations in Megacities: Some Initial Experiments," in Sae Schatz and Mark Hoffman, eds., *Advances in Cross-Cultural DecisionMaking*, Proceedings of the AHFE 2016 International Conference on Cross-Cultural Decision Making (Basel, Switzerland: Springer International Publishing, 2017), pp. 6–7.

around adversary intentions in complex gray zone theaters of operations.[98] Other simulations have sought to emulate the evolving nature of the information environment by mimicking social media applications. VATC's Epic Division and Nusura have designed synthetic training environments that replicate social media, to include Facebook, Twitter, YouTube, and blogs, among other digital platforms.[99] Their training applications to date have focused on training special operations forces (SOF) and military intelligence and public affairs personnel, among others, to respond to changing open-source information dynamics in an area of operations.

While each simulation is useful for discrete tasks, both the technical and social science approaches are constrained in their scope. They do not reflect the entirety or the changing nature of the information environment.[100] More importantly, in regards to simulating future multi-domain operations, there are currently no significant information operations simulations that are well-integrated with other combat simulations or emerging operational LVC training systems.[101]

In short, few training opportunities exist for the conventional warfighter to build an understanding of how they may best exploit offensive cyber or informationized capabilities at the tactical or operational level. Current training techniques fail to train non-cyber warriors for the potential opportunities of exploiting the cyber domain in conjunction with conventional operations in the pursuit of mission assurance.

98 "Making Gray-Zone Activity More Black and White," *Defense Advanced Research Projects Agency (DARPA) News and Events*, March 14, 2018, available at https://www.darpa.mil/news-events/2018-03-14.

99 For examples, see VATC's Digital Media Replicator at http://www.vatcinc.com/digital-media-replicator/ and Nusura's Simulation Deck at http://simulationdeck.com/.

100 For more on the information environment and information operations, see Isaac R. Porche III et al., *Redefining Information Warfare Boundaries for an Army in a Wireless World* (Santa Monica, CA: RAND Corporation, 2013).

101 Bitoun, Hubervic, and Prudent, "M&S for Influence Operations"; Tolk, "Modeling Communications, Command, and Control," and Numrich and Picucci, "New Challenges: Human, Social, Cultural, and Behavior Modeling," in Tolk, ed., *Engineering Principles of Combat Modeling and Distributed Simulation*; and Deller et al., "Applying the Information Age Combat Model: Quantitative Analysis of Network Centric Operations." Service level integration of information operations mirror these same problems. The Navy and Air Force place greater salience on the physical and information dimensions of the information environment, favoring technical solutions aimed at defeating adversary systems over tools that target the cognitive dimension of warfare. The Army and Marine Corps, similarly, target the physical dimensions of the information environment through conventional assets. Information operations aimed at content or cognitive decision making are discounted. These ideas are the result of a review of these and other sources and an exchange of ideas with information warfare expert LtCol James Rob McGrath.

Initial Scientific Work Toward a Multi-Domain Synthetic Training Environment

A synthetic training environment that perfectly integrates simulations across cyber, informationized, and traditional kinetic operations does not yet exist. The scientific community, however, has demonstrated the plausibility of such a multi-domain training environment.

Indeed, in 2016 at I/ITSEC, the largest military modeling, simulation, and training conference in the world, Carnegie Mellon University's Software Engineering Institute showcased their Cyber Kinetic Effects Integration (CKEI) system. CKEI links Carnegie's STEPfwd cyber training environment to a developed third-party kinetic mission simulator through an application programing interface, allowing effects to propagate across environments.[102] CKEI can detect changes in the cyber environment, like the triggering of an alarm, and then reflect that change in a kinetic mission training program. This integrated environment allows cyber operators to work in support of an operational mission by providing conventional warfighters real-time intelligence, conducting cyberattacks on local power stations, and sabotaging security camera feeds, among many other activities.[103] Building on this research, the Army has funded an architectural prototype that links Carnegie's STEPfwd cyber training environment with the government's One Semi-Automated Forces (OneSAF) simulation for CGFs and semi-automated forces applications. The prototype has been applied to a SOF hostage rescue mission scenario, and future works include the incorporation of GPS jamming, camera spoofing, and a cyber terrain, among other capabilities that could improve cyber-kinetic interactions.[104]

Likewise, the previously mentioned COATS program links current cyber range environments to traditional battle staff training architectures. This provides U.S. battle staff some understanding of how blue (friendly) cyberattacks can impact red (adversary) systems and, similarly, how traditional conventional operations can impact the cyber domain. In essence, COATS takes advantage of existing cyber ranges, traditional battle staff training architectures, operational networks, and an accredited cyber emulation tool to integrate cyber, kinetic, intelligence, and EW effects across the training audience.[105] To make this possible, a network guard is employed to assure and secure data flows between the two synthetic environments, and a

102 Carnegie integrated several kinetic training programs through the CKEI training interface, including Bohemia Interactive's Virtual Battlespace 3 (VBS3). For more on the Carnegie Computer Emergency Response Team (CERT) STEPfwd cyber training environment, visit https://stepfwd.cert.org/lms.

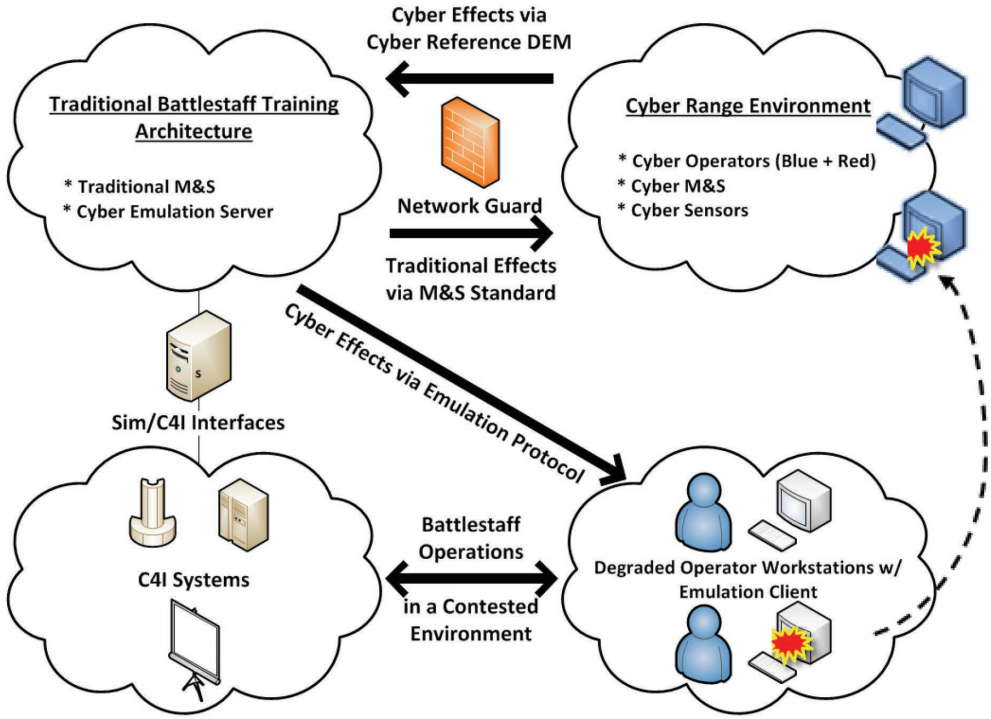
103 Rotem Guttman, "Combined Arms Cyber-Kinetic Operator Training," *Carnegie Mellon University Software Engineering Institute (SEI) Blog*, March 20, 2017, available at https://insights.sei.cmu.edu/sei_blog/2017/03/combined-arms-cyber-kinetic-operator-training.html.

104 Christopher Daiello, Kyle Hancock, John Surdu, and Daniel Lacks, "Cyber Effects within a Kinetic Model," I/ITSEC, paper no. 17181, 2017.

105 The accredited cyber emulation tool allows network and host cyber effects to be emulated on training audience workstations that have been identified from within the cyber range environment. See Wells and Bryan, "Cyber Operational Architecture Training System," especially p. 4.

new unique cyber data exchange model is employed to facilitate interoperability (see Figure 2).

FIGURE 2: CYBER OPERATIONAL ARCHITECTURAL TRAINING SYSTEM (COATS) HIGH-LEVEL OPERATIONAL CONCEPT GRAPHIC



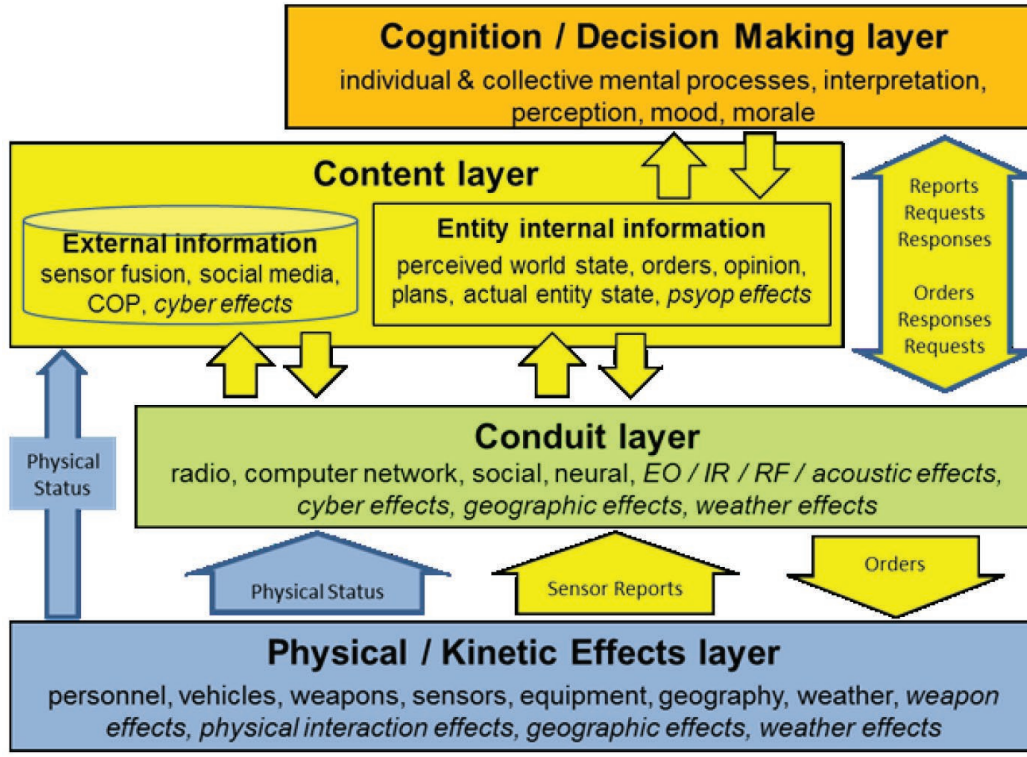
David Wells and Derek Bryan, "Cyber Operational Architecture Training System—Cyber for All," *Journal of Cyber Security and Information Systems* 6, no. 2, July 2018, p. 33.

COATS has generated some initial success. The program architecture and associated technologies have been tested at annual command post exercises with U.S. Forces Korea (USFK) and the 7th Air Force during exercises Ulchi Freedom Guardian (UFG) 2014, Key Resolve 2015, and UFG 2015.[106]

Finally, the Canadian government in partnership with industry has also sought to develop an initial model of the information environment, with the goal of integrating informationized effects into constructive simulations (see Figure 3).

106 Ibid.

FIGURE 3: INFORMATION WARFARE ENGAGEMENT MODEL ARCHITECTURE SHOWING THE LOCATION OF CYBER EFFECTS



Mark G. Hazen, Evan Harris, and Tab Lamoureux, *Use Case Analysis of the Information Warfare Engagement Model Architecture* (Dartmouth, Nova Scotia: Defence Research and Development Canada, September 2017), p. 8-4.

In this model, information operations are triggered by blue decision-makers in the cognitive layer but implemented by military units operating at the physical layer. The effects of the information operation manifests at the conduit layer (jamming, DDoS, etc.) or at the content layer through the manipulation of information and data. The goal of the information operation is to change red perceptions and decisions at the cognitive layer, with effects that can be demonstrated at the physical layer through changes in the behavior of military units.[107]

These ongoing scientific programs and models are certainly steps in the right direction. What is needed is a sandbox—a place where warfighters and commanders can experiment and begin to brainstorm what these multi-domain operations could look like. Just as the DoD innovated in the early 1980s when designing the SIMNET (SIMulator NETworking Project, the first distributed interactive simulation that allowed for collective training and experimentation), a

107 Mark G Hazen, Evan Harris, and Tab Lamoureux, *Use Case Analysis of the Information Warfare Engagement Model Architecture* (Dartmouth, Nova Scotia: Defence Research and Development Canada, September 2017), pp. 8-2, 8-4.

similar innovation in integrated training environments needs to take place today.[108] An integrated training environment must support future multi-domain operations.

At present, programs like CKEI, COATS, and the Information Warfare Engagement Model are just experiments and initial demonstrations. They act as initial testbeds to evaluate the plausibility of a multi-domain training environment. Developing an ideal interoperable synthetic training environment is not just a technical challenge. These different integrated architectures must be evaluated for performance and the delivery of multi-domain training. This naturally requires scenario development.

Chapter three will provide initial scenarios for multi-domain operations that can act as a mechanism for the test and evaluation of future integrated synthetic architectures.

108 The SIMNET program aspired to create a virtual world that was modeled as a collection of objects. Each object interacted with the others through a series of events. This allowed the possibility that an event could change one or more of these objects (for instance, destroying a bridge or another military platform). For more on the creation of SIMNET, see Duncan Miller and Jack Thorpe, "SIMNET: The Advent of Simulator Networking," *Proceedings of the IEEE*, 83.8, August 1995.

CHAPTER 3

Initial Recommendations and Conclusions

The cyber environment is going to become as important for realistic training in the synthetic world as an accurate representation of weather events.

Royal Air Force Wing Commander (ret.) David Waddington[109]

Modeling and simulation is focused on the physical, not the information environment. We need to think about information rounds, not just weapon rounds.

USAF Senior Civilian Leader[110]

This chapter provides initial recommendations on how best to develop cyber training for the non-cyber warrior. First, it briefly demonstrates how an information assurance framework can be utilized to develop a suite of tactical cyber and informationized effects for injection into training scenarios. Second, through a high-level assessment of potential adversary cyber and informationized strategies and capabilities, it identifies four guidelines that can be used as the basis for simulating red tactics and operations during scenario development. Finally, it provides a series of multi-domain scenarios that can support the test and evaluation of future integrated synthetic architectures.

Simulating Cyber and Informationized Effects for Tactical Training

Developing cyber and informationized effects for simulation in synthetic tactical trainers should be a function of platform capabilities and their potential vulnerabilities. Indeed, the effects of a cyberattack, unlike a conventional weapon, are not dependent on the malware

109 Author interview with Royal Air Force Wing Commander (ret.) David Waddington, October 2017.

110 Quote paraphrased by author from discussion in "Narratives in Information Warfare," a program of I/ITSEC, Orlando, FL, November 29, 2017.

itself. Instead, the effects of a cyberattack are based on the details of the system or platform that the malware is targeting. This calls for deep knowledge of how the system or platform works and how it fits within its broader battle network that can, at times, be highly classified. However, many tactical trainers that simulate different warfighting functions in use by the military are unclassified. As a result, the requisite information and expertise may not be available to inform the development and simulation of tactical-level cyber effects.

Notwithstanding this limitation, developing a suite of simulated cyber or informationized effects is still helpful, even if it is slightly divorced from reality. Given the number of ways that a cyber or informationized attack can impact a system, the goal should be to get the trainee to troubleshoot a diverse range of effects and creatively identify ways to maintain mission assurance despite the attack. The onus should be, first and foremost, on nurturing reactivity and adaptability in the face of a constant stream of cyber or informationized attacks.

Information assurance professionals often refer to the CIA triad as the guiding construct for organizational information security.[111] 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 simple conceptual point of departure to extrapolate the effects of adversary cyber or informationized operations on military platforms and systems. By assessing key platform capabilities against each component of the triad, one can begin to design effects that simulate with a measure of fidelity the full impact of those operations. The focus should be on identifying what effects are unique to cyber when developing tactical-level training for the non-cyber warrior. These effects could then be used as the basis for modeling MSEL events/injects.[112] The following sections describe this process across the three components of the CIA triad.

Confidentiality: Preventing Unauthorized Access and Disclosure of Information

The loss of information confidentiality could result from the compromise of mission or system information at the tactical level. For instance, an adversary could gain intelligence on the location of a military platform via computer network exploitation. Such an effect could be made clear to a platform operator in training by having the MSEL event trigger other events such as the adversary suddenly moving assets (for instance, a weapons cache) that were part of the platform's targeting plans. The goal of the training event would be to get the warfighter and broader battle network to recognize that their mission may have been compromised and, therefore, they should weigh the loss of confidentiality against mission outcomes. This type of behavior is expected of those in tactical mission command roles and could be expanded to include cyber and informationized effects.

111 "CIA Triad," *InfoSec Institute*, http://resources.infosecinstitute.com/cia-triad/#gref.

112 The Joint Staff defines a MSEL as "a collection of pre-scripted events intended to guide an exercise toward specific outcomes." See CJCS, *Joint Training Manual for the Armed Forces of the United States*, CJCSM 3500.03D (Washington, DC: CJCS, August 15, 2012), p. E-8.

Integrity: Guarding Against Adversarial Information Modification or Destruction

The loss of information integrity is a particularly insidious threat. At the tactical level, an adversary could manipulate system or platform information with the goal of subsequently sabotaging the mission or the platform. For instance, through a cyberattack, an adversary could manipulate the pre-planned flight path of a UAV, causing it to fly into restricted airspace. Such a simulated effect should prompt the trainee to take over manual control, subsequently trouble-shooting what may have occurred, while also assessing whether the action warrants the UAV returning to base or whether the operator can still maintain mission assurance. Likewise, MSELS that simulate informationized threats at the tactical level could include a constructive adversary creating a false but seemingly legitimate persona on a multi-user internet relay chat (mIRC), or multi-user Internet relay chat, employing social engineering techniques to confuse the trainee.[113] Such an effect would ideally force the trainee to critically assess the information, correlating it against previously outlined mission objectives and other sources of information to appraise the veracity of that information. Integrity threats are unique, and a suite of cyber and informationized MSELs could be designed to prompt critical thinking, creativity, and quick system-based interactions in warfighters.

Availability: Ensuring Timely and Reliable Access to Information

The compromise of the availability of system or platform information is already simulated at the tactical level. A cyberattack that sabotages key platform functionality would have similar simulated effects to an equipment malfunction due to, for instance, mechanical or electrical failure. Training and education should be developed to build warfighter understanding that a cyberattack could lead to platform or system sabotage. However, it is unlikely that a new suite of MSELs need to be developed to support this end, as warfighters already train for the loss of availability of key system or platform functions. The unique aspect of cyber, when assessing availability threats, stems from the somewhat transitory nature of cyberattacks.[114] For instance, much like jamming, the effects of a DDoS attack is not permanent. Moreover, to the extent a system or platform vulnerability is exploited by a cyberattack, system administrators can patch those same vulnerabilities, subsequently restoring system functionality.

While the CIA triad can act as the starting point for the development of tactical-level cyber and informationized effects, much more needs to be done to train non-cyber warriors to maintain mission assurance in the face of adversary cyber and informationized operations. Tactical and operational scenarios must also depict a contested and complex battlespace.

113 mIRC chat allows classified, concise, and recorded real-time communication between ground control station pilots and the end-users in areas of current combat operations, including in-theater troops and commanders in AOCs. UAV crews consistently monitor upward of eight to twelve discussions simultaneously—and, at times, as many as twenty. For more information, see Timothy Shultz, *The Problem with Pilots: How Physicians, Engineers, and Airpower Enthusiasts Redefined Flight* (Baltimore, MD: John Hopkins University Press, 2018), p. 229; and David Mindell, *Our Robots, Ourselves: Robotics and the Myths of Autonomy* (New York: Penguin Random House LLC, 2015), pp. 145–146.

114 For an overview of the "transitory" nature of cyber weapons, see Max Smeets, "A Matter of Time: On the Transitory Nature of Cyber Weapons," *Journal of Strategic Studies* 41, 2018.

Simulating Adversarial Cyber and Informationized Operations for Scenario Development

Scenarios should reflect adversary cyber and informationized strategies and capabilities. As OSD noted in a 2018 report, "DoD red teams must become capable of portraying cyber adversaries in accordance with known doctrine, tactics, and capabilities in both offensive and defensive operations."[115] This can be particularly difficult to assess, as cyber capabilities by their very nature must remain secret. Once a cyber exploit is employed, the targeted system or network's administrator can respond, patching vulnerabilities to render that same exploit unusable. Additionally, cyber capabilities are ripe for deception and misinformation. Given that cyber capabilities cannot be revealed, it could be in an adversary's interest to misrepresent the size and scale of their cyber "arsenal." Indeed, unlike conventional weapons, one cannot show strength and engage in deterrent signaling through demonstrative displays of exquisite cyber means. Instead, misinformation can be strategically employed to mislead an adversary on one's cyber capabilities, to include the number and skill of personnel, zero-day stockpiles, and other potential indicators of strength. Finally, the most compelling information the United States has on adversary cyber capabilities are likely to remain classified, as they are presumably the result of hidden and ongoing intrusions into potential adversary's networks and systems. For these reasons, any open-source study that examines adversary cyber capabilities is bound to suffer from certain limitations.

Despite these challenges, most potential adversaries (China, Russia, Iran, and North Korea) do publish some strategic or doctrinal documents that provide some indication of how they may employ cyber capabilities in a conflict. Moreover, by drawing on historic open-source case studies of past cyber operations, one can begin to surmise what an adversary's tactics, techniques, and procedures may be in an informationized conflict. Indeed, while each country's cyber strategies and capabilities differ, there are certain commonalities. Through a high-level examination of each country's cyber strategies and capabilities, four guidelines regarding adversaries' cyber objectives were identified and can serve as the basis for simulating red tactics and operations during scenario development.

Targeting key nodes

U.S. adversaries prioritize the targeting of key nodes prior to or at the onset of hostilities. Key nodes include military communications systems, command facilities, combat support functions, logistics systems, satellites, and ground stations, among other assets that are integral to the communication and prosecution of military operations.

Training-level-dependent, simulated events could emulate the loss of the command and coordination systems necessary for combined arms or joint functions. Likewise, the loss of GPS satellites could compromise precision strike and timing signals for a range of functions such

115 OSD, DOT&E, *FY 2017 Annual Report*, p. 320.

as frequency hopping radio or other secure communications methods. The loss of battlefield support systems could result in the loss of meteorological, hydrographic, and other information regarding the physical or electromagnetic elements of the battlefield.

When selecting key nodes that are targeted in a cyber scenario event, efforts should be employed to identify cascading effects. For instance, a cyberattack that sabotages a satellite ground terminal responsible for beyond visual line of sight communications could have broader cascade effects across a mission, to include degraded or denied communications, the inability to call in support for a counter-attack, and the increased risk of fratricide.[116]

Emphasizing informationized or psychological operations to cause loss of trust in systems or networks

U.S. competitors emphasize informationized or psychological operations in their warfighting strategies. Information operations can be employed at the strategic, operational, or tactical level of warfare for geostrategic effect. At the strategic level of warfare, information operations could be employed to target key political decision-makers in an attempt to sow division within allied military structures or to inject confusion and discord over the conduct of military strategy. At the operational level of warfare, information operations might include mass propaganda efforts against target populations in areas of military operations or disinformation injected into military planning. At the tactical level, information or psychological operations can take place via electronic means or a combination of cyber and information operations. This could include spoofing weapon platform's GPS coordinates or injecting false information on friendly or adversary force locations.

Information operations at the strategic level of warfare can be reflected in background scenario information, helping to provide a broader geopolitical context for the exercise. At the operational level of warfare, JMETLs should include training goals that provide warfighters experiential learning on adversary deception and information operations.[117] These training goals should force warfighters to critically assess information and question its validity while correlating that information against multiple sources. Meanwhile, at the tactical level, a simulated MSEL event could include a red cyber warrior spoofing the EO/IR sensors on an ISR platform, resulting in faulty targeting data and/or threat assessments.[118]

116 See Ruben Santamarta, *A Wake-Up Call for SATCOM Security*, Technical White Paper (Seattle, WA: IOActive Inc., 2014), p. 11, available at https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf.

117 JMETLs are a joint commander's list of priority joint tasks or joint mission essential tasks. JMETLs are derived from the assigned mission, joint doctrine, military orders and planning, available resources, and other training tools. JMETLs guide training scenario development. For more information, see JCS, *Joint Mission Essential Task List (JMETL) Development Handbook* (Washington, DC: JCS, December 1995); and John Ballard and Steve Sifers, "JMETL: The Key to Joint Proficiency," *Joint Forces Quarterly*, Autumn, 1995.

118 For more on modeling and simulating information operations, see James Rob McGrath, "Twenty First Century Information Warfare and the Third Offset Strategy," *Joint Forces Quarterly* 82, July 2016.

Employing cyber as force multipliers in A2/AD bubbles

U.S. rivals have developed A2/AD strategies with varying levels of sophistication that employ a range of conventional capabilities that will be augmented by cyber operations.[119] These regional reconnaissance-strike complexes are designed to deny hostile access to their near abroad and/or sovereign territory. Apart from targeting key nodes, it is likely that an adversary's cyber operations will also prioritize the sabotage of platforms and systems expressly designed to infiltrate its A2/AD bubbles, such as U.S. and allied stand-off weaponry, cyber and electronic systems, and "access-insensitive" platforms like submarines.[120]

When developing scenarios for JMETLs, emphasis should be placed on mimicking adversary A2/AD capabilities and their operational impact on U.S. forces. This should include the attrition of U.S. physical and virtual forward sanctuaries, to include space, cyberspace, and the EMS. Initial MSEL cyber events could target critical nodes for sabotage, with follow on events targeting key power projection platforms. The goal of the MSEL events should be to guide the warfighters toward regaining the initiative across all warfighting domains.

Conducting cyber operations that will likely follow the logic of conventional capabilities

States will likely employ cyber capabilities to enhance and ensure the success of their traditional kinetic weapons systems. States that place a strategic emphasis on ballistic missile operations, will likely employ their cyber capabilities to degrade ballistic missile defense systems. Likewise, states that emphasize air dominance in their warfighting strategies will likely engage in cyberattacks against U.S. and allied integrated air defense systems (IADS).

MESLs that simulate cyber operations should also pull from current intelligence on adversary kinetic weapon capabilities. These capabilities should help to inform assessments of the *blended* strategies, combining kinetic and non-kinetic attacks, that adversaries may adopt in the event of conflict. For instance, a scenario in the Persian Gulf could include Iran employing

119 The DoD defines anti-access as an "action, activity, or capability, usually long-range, designed to prevent an advancing enemy force from entering an operational area." Area denial is defined as an "action, activity, or capability, usually short-range, designed to limit an enemy force's freedom of action within an operational area." DoD, *DoD Dictionary of Military and Associated Terms* (Washington, DC: DoD, November 2018), pp. 19–20. On potential adversary A2/AD investments, see Roger Cliff et al., *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States* (Santa Monica, CA: RAND Corporation, 2007); Jan van Tol et al., *AirSea Battle: A Point of Departure Operational Concept* (Washington, DC: Center for Strategic and Budgetary Assessments, May 2010); Evan Braden Montgomery, "Contested Primacy in the Western Pacific: China's Rise and the Future of U.S. Power Projection," *International Security* 38, no. 4, Spring 2014; Mark Gunzinger and Chris Dougherty, *Outside-In: Operating from Range to Defeat Iran's Anti-Access and Area-Denial Threats* (Washington, DC: Center for Strategic and Budgetary Assessments, January 2012); Christopher Bowie, *The Anti-Access Threat and Theater Air Bases* (Washington, DC: Center for Strategic and Budgetary Assessments, 2002); and Andrew Krepinevich, Barry Watts, and Robert Work, *Meeting the Anti-Access and Area Denial Challenge* (Washington, DC: Center for Strategic and Budgetary Assessments, 2003).

120 Iskander Rehman, "Great Power Rivalry: Anti-Access and the Threat to the Liberal International Order," *War on the Rocks*, October 13, 2015, available at https://warontherocks.com/2015/10/great-power-rivalry-anti-access-and-the-threat-to-the-liberal-order/.

their Shabab 1, Fateh-110, or Shabab 2 ballistic missiles against U.S. bases and forces within shorter range (roughly 500 km or less) in the region. MSEL cyber events in such a scenario could include Iranian cyber warriors targeting U.S. PAC-3 batteries in Bahrain, Kuwait, Qatar, and the United Arab Emirates, in addition to targeting U.S. Navy Aegis destroyers armed with SM-3 interceptors.[121]

Applying these four principles when simulating red forces should inject some fidelity into cyber and informationized training scenarios.

Initial Training Scenarios for the Test and Evaluation of Multi-Domain Synthetic Training Architectures

Integrating cyber events into non-cyber warrior training does not just require simulating the effect of an adversary's cyber operations in a synthetic training environment. Warfighters must also understand the unique attributes that blue cyber operators bring to the fight when prosecuting multi-domain operations. Training opportunities must support non-cyber warfighters to train alongside cyber warriors in a synthetic training environment to exploit cyber advantages.

Although an integrated training environment does not yet exist, that should not preclude commanders and exercise planners from designing multi-domain scenarios for the test and evaluation of future integrated training architectures.[122] Indeed, designing a solid story line is important, as it allows for more dynamic play and less scripted events while meeting the exercise objectives.[123] Scenarios should be used as an initial point of departure for the test and evaluation of future integrated synthetic training architectures and contribute to multi-domain JMETL and MSEL development.[124] When developing scenarios for multi-domain training, careful consideration of the unique attributes of cyberspace and the information

121 Michael Elleman and Wafa Alsayed, "Ballistic Missile Defense Cooperation in the Arabian Gulf," in Catherine McArdle Kelleher and Peter Dombrowski, eds., *Regional Missile Defense from a Global Perspective* (Stanford, CA: Stanford University Press, 2015), pp. 161–167; "Aegis Ballistic Missile Defense," Missile Defense Agency, available at http://www.mda.mil/system/aegis_bmd.html; and Gunzinger and Dougherty, *Outside-In*.

122 For more on the test and evaluation of new military systems, see James G. Wilson, *Examining the Statistical Rigor of Test and Evaluation Results in the Live, Virtual, and Constructive Environment* (Wright-Patterson AFB, OH: Air Force Institute of Technology, June 2011), available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a547321.pdf.

123 This should include a dynamic white cell that can increase or decrease the tempo of training events based on trainee performance. See Krisjand Rothweiler, "Train Like You Fight and the Command Post Exercise," *Strategy Bridge*, June 7, 2016, available at https://thestrategybridge.org/the-bridge/2016/6/7/train-like-you-fight-and-the-command-post-exercise.

124 For other scenarios that include a cyber component, see Lindberg, Hamilton, Lebiednik, and Hager, "Cyber Integrating Architecture."

environment should be taken into account.[125] Depending on the exercise, this may also include mimicking some of the more particular challenges (timing, classification, etc.) that cyber or informationized operations may bring to the fight (see appendix).

Scenario One: Simulating Multi-Domain Operations in Support of Eradicating ISIS in Syria

Mission: Eradicate ISIS in Syria

Level of Command: Joint Force Command at the tactical level of war

Example Joint Mission Essential Tasks: Employ fires, engage time-sensitive targets

A hypothetical training scenario to support the ongoing mission to eradicate ISIS in Syria could include two tactical JMETLs designed to train for the employment of joint fires to eliminate a time-sensitive target. In this scenario, an Army Cyber Electromagnetic Activities (CEMA) team is working in conjunction with USAF MQ-9 operators and Special Forces equipped with a hand-launched RQ-20A Puma. The combined group of warfighters is tasked with striking a high-level ISIS official that is in movement between safe houses located in Al Bukamal. The RQ-20A Puma UAV is originally employed for surveillance and intelligence purposes. However, the UAV is quickly jammed and apprehended by members of ISIS.[126]

Several tasks could fall under this training scenario. The warfighters need to identify how best to collect and share the information on the ISIS official in movement for deliberate or dynamic targeting. ISR tasks fall on the MQ-9 operators; however, visibility proves challenging when operating above a dense urban environment. As a result, a CEMA team employs electronic and cyber operations in tandem, utilizing electronic attack (EA) to gain access to the ISIS official or his entourages' mobile devices through WiFi, subsequently surreptitiously installing malware via the radio-frequency (RF) link to monitor location data.[127] This information is then fed to the special forces team to eliminate the target.

125 Each scenario is based off a joint mission essential task found in the Universal Joint Task List (UJTL). The scenarios are not adapted to a specific training audience. They are instead meant to highlight unique attributes of cyber and informationized operations that should be accounted for during the exercise planning process and when testing and evaluating integrated synthetic training architectures. For more on the UJTL, see "Universal Joint Task List (UJTL)," JCS database, updated as of October 19, 2018, available at https://www.jcs.mil/Portals/36/Documents/Doctrine/training/ujtl_tasks.pdf?ver=2018-10-19-084613-470.

126 This could be the result of Russian soldiers inadvertently losing or leaving behind the equipment they use to jam American hand-launched and catapult UAVs. Joseph Trevithick, "The Russians Are Jamming US Drones in Syria Because They Have Every Reason to Be," *The Drive*, April 10, 2018, available at http://www.thedrive.com/the-war-zone/20034/the-russians-are-jamming-us-drones-in-syria-because-they-have-every-reason-to-be.

127 This could pose challenges to some authorities. Various models are currently under examination to increase the efficiency of tactically employing cyber. See Isaac R. Porche III et al., *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below* (Santa Monica, CA: RAND Corporation, 2017).

While cyberspace is a warfighting domain, in many tactical situations where no physical data-links exist, exploiting connections via the EMS may prove more beneficial. Indeed, during CEMA training and experimentation exercises, the Army has rapidly realized that any device utilizing WiFi or cellular connections should be targeted via electronic warfare over cyber means.[128] Training scenarios should allow warfighters and commanders the opportunity to think creatively about what tool is best suited to achieve an effect. This should require deeper integration across the force, as a given tool may not be readily available within a single Service or functional area.

Scenario Two: Simulating Multi-Domain Operations to Liberate Taiwan and Neutralize People's Liberation Army (PLA) Forces

Mission: Liberate Taiwan and neutralize PLA forces

Level of Command: Joint Force Command at the operational level of war

Example Joint Mission Essential Task: Establish air superiority

In the event of a Chinese attack on Taiwan, a hypothetical training mission designed to liberate Taiwan and neutralize PLA forces might include an operational JMETL focused on gaining and maintaining air superiority over Taiwan, the Taiwanese Strait, and portions of the East and South China Seas.[129] Such a scenario would likely employ integrated offensive cyber, electronic, and conventional operations.

To support this JMETL a series of training events take place. For instance, intelligence is collected on operational targets at the onset of hostilities. A cyber combat mission team gains access to a PLA Air Force (PLAAF) air operations center (AOC), enabling the monitoring of the PLAAF's deployment of air power in theater. In tandem—or shortly thereafter—U.S. forces engage in the suppression of enemy air defenses (SEAD), engage in offensive counter-air operations, and conduct precision strikes against a variety of other targets from PLAAF aircraft to basing and logistics hubs and C2 centers.

These actions would need to be carefully synchronized. For example, assuming the U.S. cyber combat mission team's connection to the PLAAF's AOC is via a fiber optic cable, U.S. forces could lose that vital source of intelligence if it that cable was damaged during combat operations. That same fiber optic cable could, however, run across a PLAAF base that is a focal point of the air interdiction operation. This would require careful campaign planning that weighed the intelligence gain-loss factor of carrying out conventional strikes on targets that

128 Mark Pomerleau, "Where Do Cyber and EW Fit at the Theater Level?" *C4ISRNet*, October 12, 2017, available at https://www.c4isrnet.com/show-reporter/ausa/2017/10/12/where-do-cyber-and-ew-fit-at-the-theater-level/.

129 For a range of contingencies that may be involved in a conflict over Taiwan, see Jim Thomas, John Stillion, and Iskander Rehman, *Hard ROC 2.0: Taiwan and Deterrence through Protraction* (Washington, DC: Center for Strategic and Budgetary Assessments, 2014), pp. 10–24.

intersect with the physical layer of cyberspace used for intelligence collection purposes. Is intelligence on PLAAF planning of greater importance than the air base? If so, a strike may be deemed unwise at that given moment: if not, a strike may take place. A similar decision-making process, or debate over neutralization versus exploitation, must also occur when mulling the employment of cyberattacks on C2. Causing permanent damage to a C2 center through conventional operations or a cyberattack also removes a potentially invaluable source of intelligence.

Cyberspace relies on a man-made physical architecture (as well as the EMS) for its functionality. During campaign planning, careful consideration of the physicality of cyberspace must take place. Operations that degrade, destroy, or disrupt elements of the physical, or even logical, layer of cyberspace may have unintended consequences on other elements of the military operation, whether intelligence, influence, or fires. Depending on the JMETL, other cross-domain effects could be called in to ensure mission assurance while preserving the physical nature of cyberspace. For instance, SOF interdiction of adversary operational targets could take place in lieu of an air interdiction operation on a PLAAF base.

Scenario Three: Simulating the Information Environment to Train for Russian Political Interference in their Near-Abroad

Mission: Countering Russian political interference in their near-abroad

Level of Command: Joint Forces Command at the operational level of war

Example Joint Mission Essential Task: Counter insurgent propaganda

A hypothetical training scenario could be designed around Russia's predilection to foment ethnic unrest in the Baltic states, particularly within Estonia and Latvia, which possess large Russian minorities.[130] The broader purpose of this training exercise is to learn how to better counter Russian political interference and disinformation campaigns throughout their near abroad. A JTMEL for this mission type includes countering insurgent propaganda.

Given the multi-faceted nature of information operations, several training events take place to support such a scenario. Military intelligence is tasked with monitoring social media sites such as Twitter and VKontakte. Intelligence collected via social media is fed back to the force, serving two subsequent purposes. First, troll and bot accounts spreading false information are identified and flagged. These accounts are then targeted via DDoS or other offensive cyber

130 For a hypothetical scenario that addresses Russia's disinformation efforts among Russian minority populations in their near abroad and how these may be blended with conventional and hybrid operations, see Iskander Rehman, "Radioactive in Riga: The Latvian Nuclear Standoff in 2018: Part I," *War on the Rocks*, November 27, 2015, available at https://warontherocks.com/2015/11/radioactive-in-riga-the-latvian-nuclear-standoff-of-2018-part-i/.

operations to deny the accounts the ability to post future information.[131] Additionally, the false information is used as the basis for public affairs and military information support operations (MISO).[132] In tandem with allied and partner governments in the region, counter narratives are crafted, tested for virality, and deployed via the same social media sites. Public affairs teams contact media outlets that are extensively read by the Kremlin's target population and debunk the disinformation. For instance, efforts are made to highlight the lack of veracity in doctored photographs.[133] Throughout the operation, efforts should gauge the overall effectiveness of the information operations.[134] This constitutes a challenging undertaking, as sudden psychosocial changes and opinion shifts in populations are not necessarily easily measured in real time. However, tools that measure the virality of a post or narrative can be used as one indication of whether the message is effectively reaching the target audience. Moreover, if the Kremlin's goal is fomenting public unrest, changes in the size of protests could also be indicative of changing perceptions among the target population.

In such a scenario, different synthetic environments can be linked to provide warfighters with the opportunity to respond in real time. Disinformation can be injected into simulated social media environments, forcing military intelligence analysts to use analytic skills and automation tools to flag Kremlin propaganda. Once flagged, the simulated environment can alert those operating in a virtual C2 center, providing them the opportunity to direct cyber warriors located in a virtual cyber range. Likewise, C2 could task a virtual military information support command to develop and employ an integrated information operations plan. The deployment of the information operations plan could take place in a synthetic environment, allowing warfighters to gauge the impact of the operation on a constructive computer-generated population. By modeling how information operations move through the information environment, constructive models can better gauge the impact of the operation on the target synthetic populace.

131 It's likely that such a strategy will cause new accounts to be developed by the Kremlin or Kremlin proxies, creating a "whack a mole" situation. As a result, such a strategy cannot be used in isolation and must be augmented with other information operations.

132 For an overview on the differences between public affairs and military information support operations (MISO), see Porche et al., *Redefining Information Warfare Boundaries*, pp. 57–64.

133 DARPA's Media Forensics (MediFor) program uses automation to identify "deep fakes"—images that appear real but are doctored. If successful, the MediFor platform will automatically detect manipulations and provide detailed information about how these manipulations were performed. Such information could be deployed as a mechanism to counter disinformation. See "Media Forensics," DARPA, available at https://www.darpa.mil/program/media-forensics.

134 DARPA's Compass Program could be a key facet of this training exercise; Compass seeks to understand adversary intent in the midst of a gray zone conflict by gauging an adversary's reaction to various stimuli. For more information, see "Making Gray-Zone Activity More Black and White," *Defense Advanced Research Projects Agency (DARPA) News and Events*.

Conclusion

These scenarios pinpoint a key challenge: the battle for information dominance will be a key feature of any future conflict. The adaptation and integration of ICTs into weapons platforms, military systems, and in concepts of operation has put the battle for information control at the heart of great power competition. While the use of ICTs exponentially increases the U.S. military's lethality, the dependence on these technologies, in many ways, is also a vulnerability. U.S. and allied military forces must be prepared to fight as an integrated whole in and through an increasingly contested and complex informationized environment.

The U.S. military's ability to prevail in a future high-end informationized conflict will not solely be a function of wielding superior technology. History demonstrates that technology alone is a poor predictor of military prowess.[135] Ultimately, combat effectiveness is the result of a judicious combination of technology, training, and other attributes of military readiness.[136] At present U.S. military training has failed to adequately adapt to this change in combat. Cyber and informationized training is not fully integrated across the force.

Although nothing can replace the physicality of live training, when preparing for the future information-saturated battlespace, the synthetic environment can inject a much-needed degree of realism. If the U.S. and its allies wish to prevail in future multi-domain operations, they will need to develop simulation-based architectures that are sufficiently robust and sophisticated to adequately reflect the complexities of a rapidly evolving combat environment. Synthetic training systems, scenarios, and models must therefore evolve to support this future, while continuously sharpening the warfighting edge of both the cyber and non-cyber warrior.

135 Stephen D. Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004), p. 4.

136 For more on military readiness, see Richard K. Betts, *Military Readiness: Concepts, Choices, Consequences* (Washington, DC: The Brookings Institution, 1995).

APPENDIX

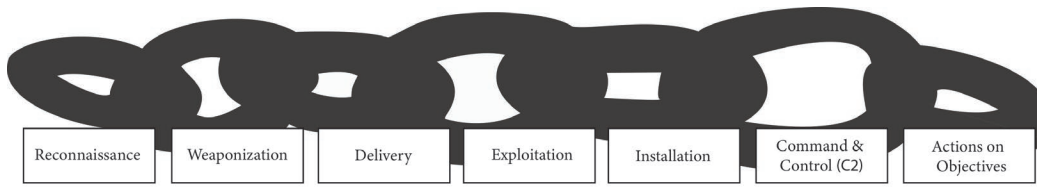
UNIQUE ATTRIBUTES OF CYBER OPERATIONS

Warfighters should understand the strengths and weaknesses that cyber operations bring to the fight. Cyber operations have unique attributes that differ from traditional kinetic operations. Dependent on the training goals, these characteristics should be considered during scenario development.

Timing

While the timing and sequencing of joint operations has always presented unique challenges, cyber adds a new dimension. Conventional wisdom holds that offensive cyber operations operate at a speed that transcends traditional kinetic warfighting capabilities. In reality, targets cannot necessarily be prosecuted instantaneously via a cyberattack. Operational planning to conduct a cyberattack is a time-consuming process, forcing cyber planners to articulate the effects of a cyberattack on both the immediate target and secondary systems or networks. Moreover, while such planning is also required for conventional operations, the time frame for conventional targeting is significantly compressed. Fixed physical targets that are prosecuted during conventional operations, like military installations, do not change. Once they are on a conventional targeting list, they will presumably remain on the list. Systems and networks, however, change frequently because of software updates, patches, and new interconnections or because, at times, they are simply turned off. As a result, the process to target a system or network is significantly expanded.[137] Furthermore, cyber operators often take months or even years to work through the cyber kill chain to finally achieving their objectives (see Figure 4).[138] The more crucial a system is to an adversary, the more likely it is strongly protected, increasing the time needed for exploitation. Furthermore, at any point during the kill chain, the adversary could discover the operation or simply patch the vulnerability, breaking the chain.

FIGURE 4: THE STAGES OF THE CYBER KILL CHAIN



137 James E. McGhee, "Liberating Cyber Offense," *Strategic Studies Quarterly*, Winter 2016, pp. 49–50.

138 For a detailed description of each facet of the cyber kill chain, see Eric M. Hutchins, Michael J. Cloppert, and Rohan M Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (Bethesda, MD: Lockheed Martin Corporation, 2011), p. 4, available at https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

However, once a system is exploited, the effects of a cyberattack can be nearly instantaneous, requiring rapid action on the part of more conventional warfighters. In such a case, if the success of a conventional operation is dependent on the success of the cyber operation, the conventional warfighters may need to advance before the cyber warriors successfully exploit a system or network. Such a decision injects a degree of friction into the operation, as the conventional forces would be moving into action before knowing the effects of the cyber operation on adversary systems or networks, potentially exposing them or inserting them into a lethal situation. Likewise, cyber warriors could design the malware to exploit system vulnerabilities at a predetermined time. Campaign planning would then need to reflect the selected time for the conventional operation. However, pre-determining times for conventional operations can be challenging. The conditions may not be ripe for a conventional attack, just as the weather nearly stalled the planned D-Day invasion by a fortnight in 1944. The malware could also be fashioned to respond to ongoing external events that are reflected in the adversary's network. For instance, text within an email message or a pattern of traffic within a network could act as a trigger for the malware's deployment. This could induce even greater friction into the planning process, as malware could be cued by other seemingly innocuous network events.[139]

Authorities and Restrictive Rules

Complicating timing problems are the requisite authorities for cyber operations. The authorities to conduct cyber operations are far higher than conventional operations, even when they generate non-kinetic effects. Cyber operations can only be employed if an execute order (EXORD) is issued.[140] An EXORD is an order issued by the Chairman of the Joint Chiefs of Staff at the direction of the Secretary of Defense to carry out a Presidential decision to initiate military operations. On top of the EXORD, the intended cyber target would also need to be on a cyber targeting list, and appropriate reconnaissance and preparation of the adversary's targeted network would need to have taken place. Depending on the target, international deconfliction may also need to occur prior to exploitation. While conventional operations also require an EXORD, additional authorizations tend to be easier to attain. In the absence of an EXORD for a cyber operation, a commander can apply for its use through the review and approval process for cyber operations (RAPCO). However, RAPCO is a cumbersome interagency review and approval process. Cyber operations in the RAPCO process are often overtaken by ongoing operational events or circumvented in lieu of conventional operations.[141] Information operations, depending on the tool in question, can mirror the authorities process required for cyber operations, as they can have strategic effect. For instance, when psychological operations are employed as part of an information operation, combatant commanders

139 Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016), p. 50.

140 McGhee, "Liberating Cyber Offense," p. 48.

141 Ibid.

must submit their operational plans to the Joint Staff for review. These plans are then forwarded to OSD for appropriate review and interagency coordination.[142]

This authorities process is also applicable to cyber operations conducted at the tactical level, for instance via the Army's CEMA. The U.S. military is currently considering possible authorities changes to provide some adaptability at the tactical level for the employment of cyber operations; in the near term, requests will need to be granted from strategic and operational planners. Experimenting with various "reach-back" models during training, where cyber teams are tethered to national-level agencies for authorizations, may provide some flexibility to act.[143]

Predicting the Effects of a Cyber Operation

Warfighters and commanders must also have some capacity to anticipate what a cyberattack may do to a target. In the United States, the Services employ Joint Munitions Effectiveness Manuals (JMEMs) to model and simulate offensive operations; they provide details on weapon damage effectiveness. JMEMs allow operational planners to predict with some accuracy the effectiveness of their weapon systems against a variety of targets. However, the effects of a cyberattack, unlike a conventional weapon, are not dependent on the weapon, or more specifically malware; the effects of a cyberattack are based on the system the malware is targeting. Therefore, it is likely impossible to precisely know the exact effects of a cyberattack on a system.[144] Instead, what is required is the ability to quickly conduct battle damage assessments and feed that information back to the commander or warfighter for their subsequent decision or action.[145]

Predicting the effects of an information operation can prove even more challenging. Indeed, much like military deception (MILDEC) operations in the past, information operations can have unintended cascade effects.[146]

142 JCS, *Doctrine for Joint Psychological Operations,* Joint Publication 3-53 (Washington, DC: JCS, September 5, 2003), p. V-I, available at https://www.hsdl.org/?abstract&did=472329.

143 Porche et al., *Tactical Cyber*, pp. xvii–xviii.

144 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 OSD, DOT&E, *FY 2017 Annual Report*, p. 317.

145 Conducting a strong battle damage assessment for a cyberattack, however, is not simple. See Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016), p. 148.

146 See, for example, the debate about whether a WWII Ghost Army tactical deception operation may have contributed to Company D casualties on August 25, 1944. Jennifer McArdle, "Pioneers of Deception: Lessons from the Ghost Army," *War on the Rocks*, May 8, 2018, available at https://warontherocks.com/2018/05/pioneers-of-deception-lessons-from-the-ghost-army/.

Classification

Cyber capabilities pose challenges when attempting to integrate their effects across the force. Many cyber capabilities are classified and strictly compartmentalized through special access programs limited to a select number of people. As a result, even in classified wargames, many participants will not have access to the full range of effects that a cyber operation can bring to bear. As one wargamer noted, these capabilities often appear as "magic pixie dust."[147] Participants remain in the dark about the actual capabilities of certain cyber operations but are expected to trust that the capability exists and will function when called upon.

Moreover, in the event of a high-tempo cyber conflict against a near-peer competitor, the United States will likely fight alongside partners and allies. However, current classification restrictions may degrade operational effectiveness as limitations may apply to information-sharing on ongoing cyberattacks, the status of networks and systems, and U.S. vulnerabilities. These constraints currently filter down to coalition-level training, reducing the benefits of integrated training operations and leaving coalition partners unprepared to face a near-peer competitor that employs cyber operations.[148]

147 Brendan Rittenhouse Green and Austin Long, "Invisible Doomsday Machines: The Challenge of Clandestine Capabilities and Deterrence," *War on the Rocks*, December 15, 2017, available at https://warontherocks.com/2017/12/invisible-doomsday-machines-challenge-clandestine-capabilities-deterrence/.

148 OSD, DOT&E, *FY 2017 Annual Report*, p. 321.

LIST OF ACRONYMS

A2/AD	anti-access/ area denial
AOC	air operations center
BiLAT	Bilateral Negotiation Trainer
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAMO	Cultural Awareness for Marines Operation
CEMA	Cyber Electromagnetic Activities
CGF	computer generated forces
CKEI	Cyber Kinetic Effects Integration
COATS	Cyber Operational Architecture Training System
COBWebS	Cyber Operations Battlefield Web Services
COCOM	combatant command
CTC	Combat Training Center
DARPA	Defense Advanced Research Projects Agency
DDoS	distributed denial of service
DMON	distributed misions operations network
DoD	Department of Defense
DOT&E	Director, Operational Test and Evaluation
EA	electronic attack
EO/IR	electro-optical/infrared
EMS	electromagnetic spectrum
EXORD	execute order
GPS	Global Positioning System
I/ITSEC	Interservice/ Industry Training, Simulation, and Education Conference
IADS	integrated air defense systems
ICT	information communication technology
ISIS	Islamic State of Iraq and Syria
ISR	intelligence, surveillance, and reconnaissance
JCSS	Joint Communication Simulation System
JIOR	Joint Information Operations Range
JMEM	Joint Munitions Effectiveness Manuals
JMETL	joint mission essential task lists
LVC	live, virtual, constructive
MILDEC	military deception
mIRC	multi-user internet relay chat
MISO	military information support operations
MSEL	master scenario event list
NDAA	National Defense Authorization Act

OneSAF	One Semi-Automated Forces
OPFOR	opposing force
OSD	Office of the Secretary of Defense
PAC-3	Patriot Advanced Capability-3
PCTE	Persistent Cyber Training Environment
PGM	precision guided munition
PLA	People's Liberation Army
PLAAF	PLA Air Force
RAF	Royal Air Force
RAPCO	review and approval process for cyber operations
RF	radio-frequency
S&T	science and technology
SEAD	suppression of enemy air defenses
SIMNET	simulator networking
SOF	special operations forces
TRADOC	U.S. Army Training and Doctrine Command
UAV	unmanned aerial vehicle
UFG	Ulchi Freedom Guardian
USAF	U.S. Air Force
USFK	U.S. Forces Korea
VATC	Visual Awareness Technologies Consulting Inc.

CSBA

Center for Strategic and Budgetary Assessments

1667 K Street, NW, Suite 900
Washington, DC 20006
Tel. 202.331.7990 • Fax 202.331.8019
www.csbaonline.org