INSTITUTE FOR DEFENSE ANALYSES

Advancing the Campaign-level Analysis of Cyberwarfare, Artificial Intelligence and Autonomous Systems, and Battle Command and Control

Al Sweetser
Joe McCarthy
Timothy A. Walton

January 2020

IDA Document NS D-12063
Log: H 20-000031

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted under the IDA Systems and Analyses Center Central Research Project C550N, "Survey of Federal AI/Machine Learning Implementation and Identification of Potential Future IDA Opportunities and Needs." The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information

Al Sweetser, Project Leader
wsweetse@ida.org, 703-575-6609

Richard B. Porterfield, Director, Intelligence Analyses Division
rporterf@ida.org, 703-578-2812

Copyright Notice

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-12063

Advancing the Campaign-level Analysis of Cyberwarfare, Artificial Intelligence and Autonomous Systems, and Battle Command and Control

Al Sweetser
Joe McCarthy
Timothy A. Walton

A. Introduction

The Military Operations Research Society (MORS) conducted its Advancing Campaign Analytics workshop at the Institute for Defense Analyses, November 18–21, 2019. The workshop began with a series of tutorials on Monday. These were followed by a plenary session on Tuesday morning that included a keynote from Mr. Bob Work, former Deputy Secretary of Defense, and a panel with members from the four Services, Office of the Secretary of Defense (OSD) Policy, and OSD Cost Analysis and Program Assessment (CAPE). The remainder of the workshop was devoted to deliberations by six working groups:

1. Campaign Analysis in DoD and Industry
2. Improving Inputs to Campaign Analysis
3. Responsiveness vs. Resolution
4. Representing New Technologies and Capabilities in Campaign Analysis
5. Applying Computer Advances to Campaign Analysis
6. Relationship of Campaign Analysis to Related Fields (Wargaming, Training Exercises, and Experimentation)

This paper primarily contains results from Working Group 4. More information on the other working groups can be found at the MORS website[1] and there will be an in-depth paper containing the results of the workshop in the June issue of *Phalanx.*

Working Group 4 included an assessment of three capability areas of critical importance to future military conflicts: cyberwarfare, artificial intelligence (AI) and autonomous systems, and battle command and control (C2). These emerging areas present unique analytical challenges given the current limitations of campaign-analysis techniques and tools, which are primarily designed to adjudicate attrition-based, force-on-force combat. To improve the representation and analysis of these areas, the working group focused on (1) defining the capability area effects, (2) identifying ways to adjudicate them in wargames and mission-level tools, and (3) determining how to integrate their adjudicated effects into campaign analysis. Ultimately, the working group identified three recommendations to improve the analysis of these areas:

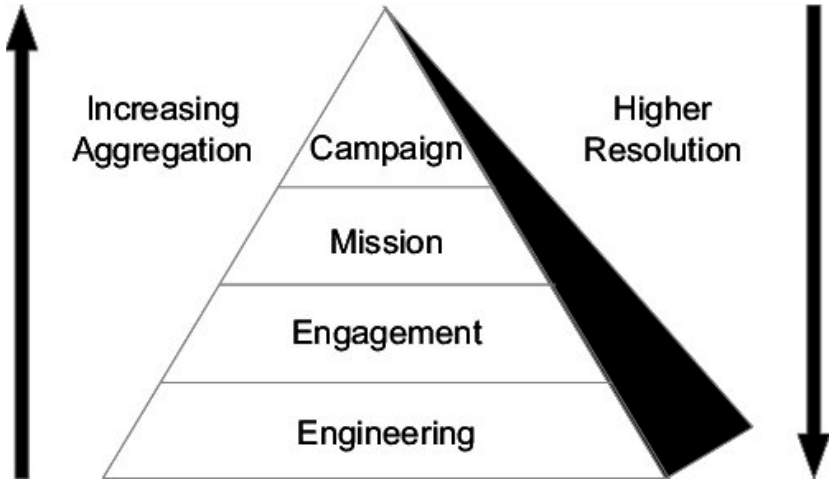
1. Improve campaign modeling techniques and, potentially, tools to better represent effects.
2. Improve analyst understanding of these areas through training (in each of the areas) and development of a shared lexicon for cyberwarfare.

[1] https://www.mors.org/Events/Advancing-Campaign-Analytics-Workshop.

3. Expand the system- and mission-level analyst toolkits to better represent these areas, incorporating emerging tools and decision aids from the acquisition, test, and evaluation and the operational planning/execution communities.

B. Background

One of the important applications of defense analysis is to assess current and future warfighting scenarios to better understand strategic and operational risks and inform the development of capabilities and concepts of operations (CONOPS). Campaign-level analysis provides a comprehensive view of warfighting scenarios, including logistical constraints, C2 relationships, and estimates of combat results. To enhance quality, campaign analysts integrate the results of more detailed engagement, mission, and engineering-level simulations and wargames (Figure 1). After a long period of decline and the demise of DoD's Support to Strategic Analysis program, campaign analysis now enjoys renewed interest and enhanced collaboration among the Military Services. For instance, in a joint memo dated September 6, 2019, the Chief of Naval Operations and Commandant of the Marine Corps announced a plan to update the Department of the Navy's Force Structure Assessment (FSA) using the Joint Force Operating Scenario, which was developed through a Service partnership. The FSA is supported by campaign analysis directed by OPNAV N81 and the USMC Combat Development Command.[2]



Source: John O. Miller, "Combat Modeling/Aggregation," project material, https://www.researchgate.net/project/Combat-Modeling-Aggregation.

Figure 1. Combat Modeling Hierarchy

[2] D. H. Berger and M. M. Gilday, "Integrated Naval Force Structure Assessment," September 6, 2019 (joint memorandum from the Commandant of the Marine Corps and Chief of Naval Operations), https://insidedefense.com/sites/insidedefense.com/files/documents/2019/sep/09272019_fsa.pdf.

Campaign analysis has no shortage of critics.[3] Common concerns include that campaign models are too slow, are not transparent, and provide erroneous results. A detailed rebuttal of these criticisms is beyond the scope of this article. In general, though, campaign analysis can be useful in integrating analyses from many different tools, models, and wargames into a holistic perspective, which can then identify needs for follow-on, more detailed analysis. It provides a structure to incorporate the wisdom of operators, planners, technologists, and intelligence analysts, who typically have years of experience in, or study of, military operations. Used properly, it can offer valuable insights that inform, not replace, military judgment.

Although it is true that instantiating a new scenario in a campaign model can take six months to a year, a significant amount of that time is usually needed to develop an accurate representation of a new scenario's CONOPS with warfighters and planners. Some of this work is required to resolve planning disconnects that occur when a conceptual plan is subjected to constraints like time and distance factors and logistical requirements. These issues may not be readily evident in planning or wargaming until subjected to the discipline of representation in a campaign model. Since campaign analysis is inherently joint, working through organizational processes to assemble, vet, and share data can also be extremely time consuming. Once the up-front work to produce an initial representation of a scenario is completed, conducting analysis over a wide range of cases can often proceed very quickly—in days to weeks.[4]

Making a campaign model's processes and algorithms transparent to customers is an analyst responsibility. The computer code supporting DoD's campaign models is traceable. Campaign model documentation, while voluminous, is readily available. These models are understandable to anyone willing to apply due diligence to the task. Understanding how a particular campaign model works (and doesn't) should be a threshold requirement for any analyst using it.

Judging the value of campaign analysis is clearly subjective. War is an inherently uncertain enterprise. No combat model or analytical approach can reasonably claim to be predictive. Campaign analysis should always include an explicit statement of key assumptions, of which there are often many. It should also include a significant amount of sensitivity analysis devoted to understanding the impact of varying those assumptions. Campaign analysis is best used to support strategic and operational military planning and programming issues by senior military and civilian leaders and their staffs. One positive example is its longstanding support to DoD studies of strategic mobility requirements in

---

[3] See, for example, CAPT John T. Hanley, "Advancing Campaign Analysis," *Phalanx*, December, 2019, 34–40.

[4] Personal experience of Dr. Al Sweetser as Chief, Warfighting Analysis Division, Joint Staff J8, 2002–2005, and Director, OSD CAPE Simulation & Analysis Center, 2005–2011.

the 1990s and 2000s. These studies informed decisions on billions of dollars in DoD investments in strategic airlift, sealift, and infrastructure. Campaign analysis can also certainly be misused. But as the aphorism states, "It's a poor workman that blames his tools." The value of campaign analysis, or lack thereof, is largely an analyst responsibility. It is simply another tool in the analyst's toolkit. When used well and appropriately, campaign analysis can provide valuable insights unavailable through other means.

C. Overview

In 2019, senior analysts from each of the Services directed MORS to conduct a workshop on advancing campaign analytics to

> incorporate the effects of emerging warfighting capabilities, take advantage of advancements in computational capabilities, improve the relationship between campaign analysis and related analytic tools, and methods, increase the responsiveness and analytic rigor of campaign analysis methods, and develop the DoD analytical workforce.[5]

One focus of the workshop was improving the analysis of cyberwarfare, AI and autonomous systems, and battle C2. The 2018 National Defense Strategy highlights these three capabilities for their potential decisive impact on future conflicts.[6] Furthermore, these capabilities are foundational to DoD's Third Offset programs, which emphasize the need for military systems with embedded AI and network-enabled, cyber-hardened capabilities.[7]

Potential U.S. adversaries are growing similar capabilities. A RAND study of Russian military thinking points out Russia's likely focus: "disrupting, degrading, or destroying adversary command and control and enemy power projection capabilities through the use of kinetic fires, cyber/electronic warfare, and direct action by maneuver forces."[8] Similarly, China is pursuing aggressive military modernization, anti-access area denial (A2AD), and "informatized" warfare. China's key AI-enabled military capabilities include unmanned and C2 systems.[9] Both the United States and its competitors realize the need to evolve

---

5 James Bexfield, "Terms of Reference, MORS Workshop: Advancing Campaign Analytics." September 10, 2019, https://www.mors.org/Portals/23/Docs/Events/2019/Campaign/TOR%20Advancing%20Campaign%20Analysis%20MORS%20Workshop%20Sept10.pdf.

6 Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America," 3, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

7 DoD Live, "3rd Offset Strategy 101: What It Is, What the Tech Focuses Are," https://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/.

8 Scott Boston and Dara Massicot, "The Russian Way of Warfare," 2017, https://www.rand.org/pubs/perspectives/PE231.html.

9 Gregory C. Allen. "Understanding China's AI Strategy, Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security," Center for New American Security, February 6, 2019, https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy

capabilities that will surely shape the future battlefield. Thus, modeling these emerging technologies at the campaign level is essential.

Campaign simulations have historically focused on adjudicating the kinetic effects of attrition-based, force-on-force combat. Two major campaign models are currently in use by DoD: the Joint Integrated Contingency Model (JICM) and the Synthetic Theater Operations Research Model (STORM). STORM and JICM have some capability to represent C2 effects, but cyberwarfare effects require scripting. With appropriate performance data and CONOPS, both JICM and STORM have some potential to represent new AI and autonomous capabilities. Neither simulation, however, has the ability to represent learning behavior in AI systems that enable performance characteristics and tactics to evolve dynamically over the course of a campaign. In addition, JICM is primarily used by U.S. Army analysts for ground-combat analysis. STORM is primarily used by the U.S. Air Force, Navy, and Marines for air, maritime, expeditionary operations, and ground-combat analysis. Joint warfighting concepts increasingly emphasize multi-domain operations. Since the effects of cyberwarfare, AI and autonomous systems, and battle C2 cut across domains, acceptance by all Services of a joint model that represents all domains will be essential.

The remainder of this paper will provide a discussion of these three capability areas, focusing on:

- Defining each capability area's effects,
- Identifying ways to adjudicate them in wargames and mission-level tools, and
- Determining how to integrate their adjudicated effects into campaign analysis.

1. Key Effects of Cyberwarfare, AI and Autonomous Systems, and Battle C2

a. Cyberwarfare

To better understand the differences in effects and analysis of conventional versus cyber weapons, consider a Joint Direct Attack Munition (JDAM) versus an offensive cyber implant. JDAMs can be employed against a variety of targets (e.g., air defense, tanks, and bunkers). The quantity available for use at various time steps within a simulation can be estimated. JDAM effects (e.g., probability of hit and probability of kill) against various targets can be determined using physics-based calculations and operational testing. These munitions can be employed as long as targets, delivery systems, and weapons are available. The effects of an offensive cyber implant, in contrast, must often be determined based on logic, heavily supported by assumptions. The implant will usually target a specific system (e.g., an air defense system) or piece of software. It may take months to years for cyber warriors to identify and infiltrate a target and create the conditions for the implant's

employment. The implant may be effective only for a single use or until the exploited vulnerability is closed.

b. AI/Autonomous Systems

AI received a boost across DoD with the announcement of the Third Offset Strategy, which promotes the development of autonomous systems and human-machine teaming to address the increasing military capabilities of China and Russia. Consistent themes across Service AI programs include the development of autonomous systems, big data analysis, reducing operator burden, and support to C2 and decision-making. A critical attribute of these capabilities is learning, adaptive behavior. The U.S. Navy is developing and fielding a range of autonomous systems, including the MQ-25 Stingray aerial refueling drone that will extend the range of the aircraft carrier air wing, and the Sea Hunter unmanned surface vehicle, a prototype with the capability to spend weeks at sea tracking enemy submarines, countering mines, and acting as a communications relay. U.S. Army programs include private cloud computing, software development and cognitive computing for logistics,[10] and the Artificially Intelligent Targeting System (ATLAS). The ATLAS is designed to detect and discriminate potential targets and engage hostile targets with a 50 mm cannon with superhuman speed and accuracy.[11] The U.S. Air Force published its vision for the development of autonomous systems that create effective human-machine teams, including a "robotic wingman" that conducts reconnaissance, electronic warfare, or strike missions in collaboration with manned aircraft.[12]

c. Command and Control

Joint doctrine has long recognized the central role of information to military operations. Through emerging U.S. operational concepts such as Distributed Maritime Operations, Expeditionary Advance Base Operations, Multi-Domain C2, and Multi-Domain Operations, the military services are levying new requirements on the ability of Joint forces to operate in a distributed manner across different domains. DoD is pursuing programs that disaggregate effects chains from monolithic, static processes to dynamic processes that integrate various assets across different parts of effects chains. Context-centric C3 is an emerging approach where local commanders could dynamically command any forces they can communicate with, possibly across domains, thus upsetting more static C2 relationships. The Defense Advanced Research Project Agency (DARPA) has an

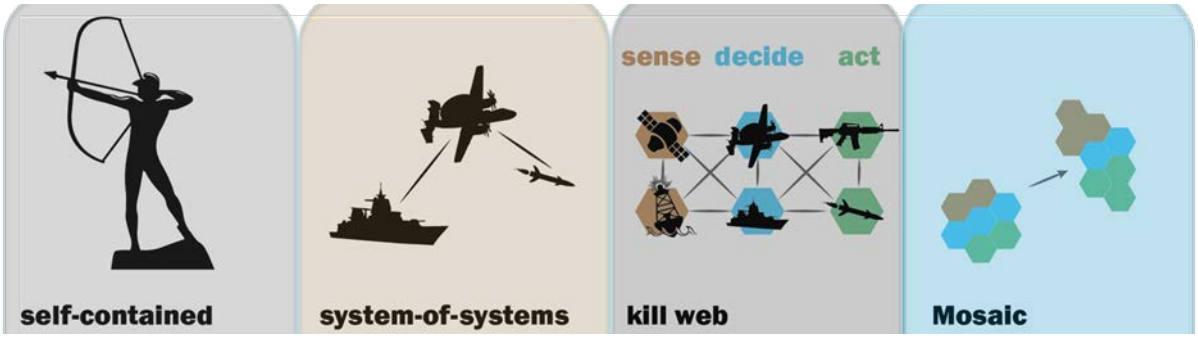
---

[10] Kris Osborn. "Army LOGSA Accelerates Migration to AI Analytics, Private Cloud Computing," September 14, 2017, https://defensesystems.com/articles/2017/09/14/army-logsa-ibm.aspx.

[11] Sydney J. Freedberg Jr., "Army to Test ATLAS Robotic Gun: Bruce Jette," June 5, 2019, https://breakingdefense.com/2019/06/army-to-test-robotic-gun-bruce-jette/.

[12] Andrew Liptak, "The U.S. Air Force's Jet-Powered Robotic Wingman Is Like Something out of a Video Game," March 9, 2019, https://www.theverge.com/2019/3/9/18255358/us-air-force-xq58-a-valkyrie-prototype-robotic-loyal-wingman-drone-successful-test-flight.

ambitious vision of a "mosaic" approach that rapidly composes and recomposes effects webs.[13] The U.S. and its adversaries are developing ways to exercise human command and machine-assisted control with novel tools to further accelerate the tempo of operations, present more complexity to adversaries, and employ forces in new ways.



Source: Figure from Bryan Clark, Whitney Morgan McNamara, and Timothy A. Walton. "Winning the Invisible War Report Rollout Event Presentation." Washington, DC. Center for Strategic and Budgetary Assessments. November 21, 2019. https://csbaonline.org/about/events/winning-the-invisible-war-gaining-an-enduring-u.s-advantage-in-the-electromagnetic-spectrum.

Figure 2. Functional Disaggregation of Capabilities and Novel Effects Chains

2. Adjudication of Cyberwarfare, AI and Autonomous systems, and Battle C2 Effects in Wargames and Mission-Level Simulations

a. Cyberwarfare

Merlin, a cyber wargame developed by the Center for Naval Analyses, is an open-ended, person-in-the-loop wargame. It provides the wargamer with a "You dream it, Merlin can do it" approach.[14] Merlin frames cyberwarfare activities into "Target, Access, Effect, and Outcome" bins. It requires game players to create cyber tradecraft at the point of need, and back-cast the sequence of actions and resources needed to produce that effect. With this approach, Merlin helps the modeler realistically project the potential number of cyberattacks (e.g., magazine depth), their limitations, and prioritize their employment. More important, Merlin facilitates interaction by providing a much-needed common taxonomy that helps cyber experts, operators, and analysts understand and discuss cyberwarfare. Alternatively, an example mission-level cyber simulation is Metron's Cyber

[13] David Ott, "Mosaic Warfare Execution (MWX) Portfolio," presentation to MORS Advancing Campaign Analysis workshop, November 20, 2019. See also: Bryan Clark, Daniel Patt, and Harrison Schramm, "Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations" (Washington, DC: Center for Strategic and Budgetary Assessments, 2020), https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations.

[14] Jeremy Sepinsky, "Wargaming Cyber Operations," presentation to MORS Advancing Campaign Analysis workshop, November 21, 2019.

Assassin. It is a high-fidelity, discrete-event, Monte Carlo simulation tool that explicitly models cyber actors in a scenario as discrete, autonomous agents and provides traceability between cyber activities and mission impacts.[15] Its inputs include networks, systems, device configurations, missions, and CONOPS. Cyber Assassin provides a framework for conducting holistic analyses of cyber threats and Courses of Action. Metron has used it to support SPAWAR (Space and Warfare Command, now Naval Information Warfare Command, or NAVWAR) and OPNAV studies evaluating network security.[16] In the absence of feeder models, other approaches to developing cyber inputs include developing worst case scenarios and soliciting subject-matter-expert input. Developing valid cyber inputs requires collaboration among cyber experts, operators, wargamers, and analysts. Building this collaboration will require the analytical community to facilitate these relationships while developing a common taxonomy and conceptual framework.

b. AI/Autonomous Systems

When performance data and CONOPS can be defined for AI and autonomous systems, these capabilities can be modeled in mission-level simulations like any other combat system. Representing learning behaviors and adaptive tactics remains challenging, however. The Air Force Research Laboratory is assessing options that use the AFSIM mission-level model to assess adaptive tactics. Emerging simulation options may be available from the acquisition and test and evaluation communities. Acquisition practices now highlight the value of "digital twins." Pioneered by NASA, digital twins are virtual representations of real-world systems and processes, increasingly used in DoD acquisition to understand system performance characteristics and improve logistics support.[17] They are highly detailed engineering-level models, sometimes fed by real-world deployed-system sensor data. It may be possible for DoD's analytical community to leverage digital twins to improve the fidelity of mission-level models and campaign-level data. Other tools may emerge from the test and evaluation community's requirement for AI-enabled systems to undergo rigorous hardware and software testing in a system's anticipated operational environment. This may result in unanticipated emergent behavior and adjustments to the system software. Any analysis must consider the legal, moral, and ethical concerns related

---

15 Metron, "Cyber Assassin," https://www.metsci.com/orca/cyber-assassin-ca/.

16 Michael Altamian, "Modeling C2 in the Naval Simulation System (NSS) and Other Mission Level Models," presentation to MORS Advancing Campaign Analysis workshop, November 20, 2019.

17 Phil Goldstein, "Digital Twin Technology: What Is a Digital Twin, and How Can Agencies Use It?" https://fedtechmagazine.com/article/2019/01/digital-twin-technology-what-digital-twin-and-how-can-agencies-use-it-perfcon.

to the employment of AI and autonomous capabilities, as required by DoD Directive 3000.09, "Autonomy in Weapon Systems."[18]

c. Battle C2

Modeling cognitive warfare in a credible manner requires representing information flows, which is better suited for engineering, engagement, or mission-level models, particularly those that incorporate rules-based decision-making tables or cognitive agents. Close integration between mission and campaign-level analysis will be essential, due to inconsistencies in aligning inputs and outputs. A parallel approach could leverage the development of new planning tools and decision aids intended for future operational use. For example, as part of the Resilient Synchronized Planning and Assessment for the Contested Environment (RSPACE) program, DARPA's Strategic Technology Office developed a planning tool for Air Operations Centers.[19] Other DARPA programs, like Adapting Cross-domain Kill-webs (ACK) and Air Combat Evolution (ACE), seek to exploit the convergence of multi-domain DoD simulation and commercial marketplace tools and gaming environments, building from commercial machine-learning programs like AlphaGo and AlphaStar that use adversarial algorithms.[20] These tools, intended to provide rapid, scalable, and automatic planning capabilities, could be repurposed for use in analysis.

3. Integration of the Effects of Cyberwarfare, AI and Autonomous Systems, and Battle C2 into Campaign Analysis

a. Cyberwarfare

Modeling cyber effects at the campaign level is inherently challenging due to the availability and classification of cyber-operation information and the limited understanding of cyber tactics, timelines for employment, resources required, and effects. Cyber analysis benefits hugely from an effective, ongoing dialogue among analysts, cyber experts, and operators. Cyberwarfare campaign simulation inputs must focus on identifying CONOPS, magazine depth (e.g., capacity to target adversary systems), and effects on individual systems. Analysts, ideally alongside cyber experts and operators, must translate this

---

[18] Department of Defense, "Autonomy in Weapon Systems." DoD Directive 3000.09, May 8, 2017 (w/change 1), 7, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.

[19] Kimberly Underwood, "DARPA Offers Advanced Planning System to the Air Force," *SIGNAL Magazine*, June 1, 2019, https://www.afcea.org/content/darpa-offers-advanced-planning-system-air-force.

[20] Dan Javorsek, "Adapting Cross-Domain Kill-Webs (ACK)," DARPA, https://www.darpa.mil/program/adapting-cross-domain-kill-webs; Dan Javorsek, "Air Combat Evolution," DARPA, May 17, 2019, https://www.darpa.mil/attachments/ACE_ProposersDayProgramBrief.pdf.

information into effects, such as impact, probability, and duration. All analysis should be accompanied by robust sensitivity analysis and the overarching intent to find a "campaign break point" (i.e., a point where one side requires a drastic change to CONOPS). The campaign break point can inform resourcing decisions for offensive cyber operations or help develop a minimum cyber-hardening levels for mission assurance and defensive cyber operations.

b. AI and Autonomous Systems

An OPNAV N81 study assessed STORM's ability to represent a range of difficult-to-represent AI-enabled capabilities, including learning behavior; automated, adaptive, and dynamic tactics and force employment; and distributed, coordinated tactics (e.g., swarm attacks).[21] The study recommended a range of modifications to STORM and options for additional modeling at the engagement and mission levels. STORM's data elements are currently input at the beginning of the simulation and remain static throughout a model run; dynamic changes in system performance data can be difficult to implement and, in some cases, cannot be modeled at all. STORM now incorporates a "checkpoint restart" feature that allows the user to pause a model mid-stride and change parameters to represent adaptive behavior. Areas requiring additional investment to upgrade STORM's capabilities include the representation of off-board, tethered systems, naval module enhancements for automated route planning, and further enhancements to represent dynamic, learning behaviors. The Air Force Research Laboratory is exploring STORM modifications to improve swarming tactic representation. The Joint Staff J-8 has pioneered the use of complex rulesets within STORM to model adaptive tactics.

c. Battle C2

In future conflicts, the United States and its adversaries will prioritize targeting specific informatized C2 targets with the goal of creating disproportionate effects. This will likely require the development of new campaign-analysis metrics and timescales (Figure 3). It will require new capability within JICM and increased use of capabilities in STORM to track the difference between "ground truth" (i.e., the actual state of a scenario at a given point in time) and the perceptions of the scenario by each actor. Understanding the discrepancies between ground truth and perceptions and assessing the effects of these disconnects are critical to analysis of informatized warfare. Modeling dynamically evolving C2 is also challenging to current DoD campaign-analysis simulations, where organizations and command relationships are usually defined at the start of a scenario. Campaign analysis tends to segment focus by domains; modeling approaches will need to evolve to fully represent operations and C2 that flow dynamically across domains.

[21] Stew Sharpe, OPNAV N81, "Campaign Modeling of Advanced Technologies," presentation to MORS Advancing Campaign Analysis workshop, November 21, 2019. SECRET

Improvements to modeling techniques and, potentially, enhancements to the current toolset for all-domain, information-based warfare will be essential.

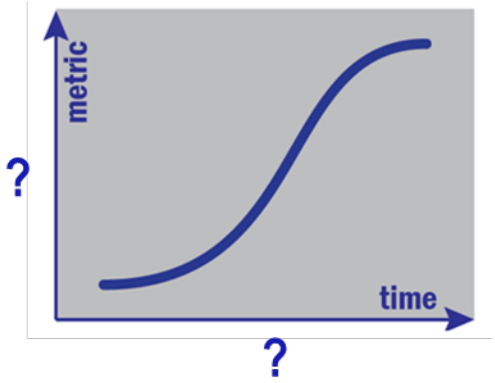


Figure 3. Determining Appropriate Campaign Modeling Metrics for Decision-Centric Approaches to Warfare Will Be Challenging

D. Recommendations/Summary

Improve campaign analysis techniques and, potentially, models to better represent the effects of cyberwarfare, AI and autonomous systems, and battle C2.

STORM and JICM were developed with an emphasis on representing physical effects associated with force-on-force, attrition-based warfare. The information domain, which is critical to the areas of cyberwarfare, AI and autonomous systems, and battle C2, is not well represented in these models. Although analysts are adept at cleverly adapting tools to a study need, their techniques and models lack the ability to represent a range of phenomena, including learning, adaptive behaviors; dynamic changes in sensor, weapon, and engagement performance parameters; dynamic, distributed C2 structures; and ground truth vs. perceived truth. In addition, as forces and C2 flow across domains dynamically, joint use of an all-domain tool will be essential. We recommend a collaborative effort to identify and prioritize campaign model improvements to better represent all domains and improve cyber, AI and autonomous systems, and battle C2 representations.

Improve analyst understanding through training and development of a shared lexicon for cyberwarfare.

The development and deployment of cyber, AI and autonomous, and battle C2 capabilities will impose the need for analysts to understand new CONOPS for Blue and Red forces. Educating analysts should not be left to chance or individual initiative. Training modules on these capabilities should be developed and made available to the analytical community. Currently, cyber is little understood, but will become increasingly important, and perhaps dominant, in future conflicts. A common taxonomy for cyberwarfare is needed

across the training, operational planning, and analytical communities. Senior Service Analysts should work with USCYBERCOM and the DoD training and operational planning communities to establish a common taxonomy for cyberwarfare that facilitates shared understanding among cyber experts, cyber operators, and analysts.

Expand the system and mission-level analyst toolkits to include incorporating emerging tools and decision aids from the acquisition, test and evaluation, and operational planning/execution communities.

Consider tools like CNA's Merlin and Metron's Cyber Assassin as possible candidates for the adjudication of cyberwarfare effects. Assess the possibility of incorporating digital twins and test and evaluation models. Leverage emerging C2 tools from DARPA programs like RSPACE and ACK.

When assessing AI-enabled and autonomous capabilities, analysts must remember that campaign models can be blunt analytical tools. Effectively incorporating these capabilities will require CONOPS changes for Blue and Red forces that must be closely coordinated with operators, planners, intelligence analysts, and technologists. It will require new approaches to mission-level analysis to reflect evolving performance characteristics and emergent behavior. It is likely to require the development of new metrics, analytical techniques, and enhancements to campaign-level models to better reflect the information environment and synergies across domains. Skilled, thoughtful analysts will adapt to these needs and ensure their work continues to help decision-makers make the best possible decisions for national security.

Bibliography

Allen, Gregory C. "Understanding China's AI Strategy, Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security." Center for New American Security, February 6, 2019. https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

Altamian, Michael. "Modeling C2 in the Naval Simulation System (NSS) and Other Mission Level Models." Presentation to MORS Advancing Campaign Analysis workshop, November 20, 2019.

Berger, D. H., and M. M. Gilday. "Integrated Naval Force Structure Assessment," September 6, 2019. Joint memorandum from the Commandant of the Marine Corps and Chief of Naval Operations.

https://insidedefense.com/sites/insidedefense.com/files/documents/2019/sep/09272019_fsa.pdf. FOR OFFICIAL USE ONLY

Bexfield, James. “Terms of Reference, MORS Workshop: Advancing Campaign Analytics,” September 10, 2019. https://www.mors.org/Portals/23/Docs/Events/2019/Campaign/TOR%20Advancing%20Campaign%20Analysis%20MORS%20Workshop%20Sept10.pdf.

Boston, Scott, and Dara Massicot. “The Russian Way of Warfare,” 2017. https://www.rand.org/pubs/perspectives/PE231.html.

Clark, Bryan, Daniel Patt, and Harrison Schramm, “Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations” (Washington, DC: Center for Strategic and Budgetary Assessments, 2020), https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations.

Department of Defense. “Autonomy in Weapon Systems.” DoD Directive 3000.09, May 8, 2017 (w/change 1). https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

Department of Defense. “Summary of the 2018 National Defense Strategy of the United States of America.” https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

DoD Live. “3rd Offset Strategy 101: What It Is, What the Tech Focuses Are.” https://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/.

Freedberg Jr., Sydney J. “Army to Test ATLAS Robotic Gun: Bruce Jette,” June 5, 2019. https://breakingdefense.com/2019/06/army-to-test-robotic-gun-bruce-jette/.

Goldstein, Phil. “Digital Twin Technology: What Is a Digital Twin, and How Can Agencies Use It?” https://fedtechmagazine.com/article/2019/01/digital-twin-technology-what-digital-twin-and-how-can-agencies-use-it-perfcon.

Javorsek, Dan. “Adapting Cross-Domain Kill-Webs (ACK).” DARPA. https://www.darpa.mil/program/adapting-cross-domain-kill-webs.

Javorsek, Dan. “Air Combat Evolution.” DARPA, May 17, 2019. https://www.darpa.mil/attachments/ACE_ProposersDayProgramBrief.pdf.

Liptak, Andrew. “The U.S. Air Force’s Jet-Powered Robotic Wingman Is Like Something out of a Video Game,” March 9, 2019. https://www.theverge.com/2019/3/9/18255358/us-air-force-xq58-a-valkyrie-prototype-robotic-loyal-wingman-drone-successful-test-flight.

Metron. “Cyber Assassin.” https://www.metsci.com/orca/cyber-assassin-ca/.

Osborn, Kris. “Army LOGSA Accelerates Migration to AI Analytics, Private Cloud Computing,” September 14, 2017. https://defensesystems.com/articles/2017/09/14/army-logsa-ibm.aspx.

Ott, David. “Mosaic Warfare Execution (MWX) Portfolio.” Presentation to MORS Advancing Campaign Analysis workshop, November 20, 2019.

Sepinsky, Jeremy. “Wargaming Cyber Operations.” Presentation to MORS Advancing Campaign Analysis workshop, November 21, 2019.

Sharpe, Stew. OPNAV N81. “Campaign Modeling of Advanced Technologies.” Presentation to MORS Advancing Campaign Analysis” workshop, November 21, 2019. SECRET

Underwood, Kimberly. “DARPA Offers Advanced Planning System to the Air Force.” *SIGNAL Magazine,* June 1, 2019. https://www.afcea.org/content/darpa-offers-advanced-planning-system-air-force.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED *(From–To)*
January 2020	FINAL	

4. TITLE AND SUBTITLE

Advancing the Campaign-level Analysis of Cyberwarfare, Artificial Intelligence and Autonomous Systems, and Battle Command and Control

5a. CONTRACT NUMBER
HQ0034-14-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Sweetser, Al
McCarthy, Joe
Walton, Timothy A.

5d. PROJECT NUMBER
CRP C550N

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER

IDA Document NS D-12063

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

10. SPONSOR/MONITOR'S ACRONYM(S)

IDA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited (17 March 2020).

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Military Operations Research Society (MORS) conducted its Advancing Campaign Analytics workshop at the Institute for Defense Analyses, November 18–21, 2019. This paper primarily contains results from Working Group 4, Representing New Technologies and Capabilities in Campaign Analysis. Working Group 4 included an assessment of three capability areas of critical importance to future military conflicts: cyberwarfare, artificial intelligence and autonomous systems, and battle command and control. Ultimately, the working group identified three recommendations to improve the analysis of these areas: (1) Improve campaign modeling techniques and, potentially, tools to better represent effects. (2) Improve analyst understanding of these areas through training (in each of the areas) and development of a shared lexicon for cyberwarfare. (3) Expand the system- and mission-level analyst toolkits to better represent these areas, incorporating emerging tools and decision aids from the acquisition, test, and evaluation and the operational planning/execution communities.

15. SUBJECT TERMS

artificial intelligence (AI); autonomous systems; battle command and control (C2); campaign analysis; cyberwarfare; wargames

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Major, Philip
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
Uncl.	Uncl.	Uncl.	SAR	18	703-845-2201

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18