MAY 16, 2019MAY 16, 2019 BY USER

145. Future OE Mission Command and Future OE Decision Cycles

[**Editor's Note:** Today's guest blog post by **Dr. John James** is the second in the Mad Scientist Laboratory's two-part discussion addressing the Army's network requirements for rapidly and continuously integrating multi-domain capabilities, enabling effective mission command, and facilitating disciplined initiative against near-peer threats in the future. In his post, Dr. James focuses on the complementary impacts that the Internet of Things (IoT) and Fifth Generation (5G) telecommunications will have on mission command in the Future Operational Environment (OE), the opportunities they will present our commanders in seizing and exploiting the cyberspace high ground, and their associated vulnerabilities — Enjoy!]

"*Plans are worthless, but planning is everything*" — **General Dwight David Eisenhower** describing planning for military operations[4], [5]

INTRODUCTION

Enormous commercial, academic, and governmental resources are being expended to build machines which can autonomously assist humans in a variety of complex tasks (e.g., drive cars, fly aircraft, engage targets, manage distributed operations). This post asserts that the technologies being developed and deployed by these efforts will eventually force future mission command capabilities to include abilities to detect, analyze, and react to man-machine interface deception / surprise events at all echelons of command. The need for these new / improved decision support capabilities will be driven by the challenges of creating accurate Intelligence, Surveillance, and Reconnaissance (ISR) estimates while encountering increased deception / surprise technologies. These deception technologies are appearing at every echelon of mission command and are being driven, in part, by the ongoing commercial integration of the international network of Information Technology (IT) systems and the international network of Operational Technology (OT) systems.

A lesson learned from the use of the Stuxnet malware to cause Iranian centrifuges to self-destruct[1] is that malware can be used to achieve tactical surprise of human operators. The centrifuge control man-machine interface was exploited to **deceive human operators** concerning the true state of the autonomous control system as the machines were being commanded to destroy themselves. The Iranian operators were unaware for a lengthy period that they were being deceived by their monitoring software and they were surprised when they discovered the extent of the damage to the centrifuges. The centrifuge-control, man-machine interface was informing the human operators that everything was proceeding as commanded when in fact the machines were shaking themselves apart.

It is apparent from many recent events / results, [2], [3], [7], [8], [9], [10] that similar outcomes are now possible at each echelon of command (individual deception outcomes at the “tip of the spear,” as well as tactical surprise outcomes, operational surprise outcomes, and strategic surprise outcomes). This note provides a summary of some results in achieving distributed state estimation and control of complex, networked systems. This post asserts that a wide variety of distributed control systems, including national infrastructure systems and possibly military command and control systems are subject to deliberate and inadvertent cyber and physical anomalies (failure modes) and states the author’s opinions regarding the implications of the ongoing integration of IT and OT for future Mission Command decisions and future OE state estimation results.

DISCUSSION

By the end of WWII, one result of the years of repeated iterations of division command and staff interactions producing and executing operations orders (OPORDs) was the ability to rapidly (in less than 24 hours) generate and execute a one-page division OPORD to meet command intent at the operational level. At the end of the Army XXI development and fielding exercises shortly before Operation Desert Storm, a capability was demonstrated to generate and modify / execute a division OPORD in less than eight hours to meet command intent. When NATO and other nations supported the United States in responding to the 9-11 attacks by removing the Taliban from power in Afghanistan, one of the systems deployed to assess the situation regarding Afghan hamlet and village support for the new government was the Effects-Based Assessment Support System (E-BASS).[6] E-BASS enabled the rapid assessment of national-level outcomes regarding the status of meeting command intent at the strategic level.

Figure 1. Plans are worthless, but planning is everything[5]

An assessment repeatedly mentioned by President Eisenhower regarding military planning is that “Plans are worthless, but planning is everything”[4], [5] (Figure 1). The planning process is necessary for successful operations, but plans created through the planning process are usually not executed as written. Given the current dramatic changes in the OE driven by IT/OT integration, that assertion has probably never been truer. The current and **future challenge** is to speed up the processes of incrementally adjusting plans so that commanders at each echelon can consistently stay “inside the decision cycle” of opposing commanders (i.e., not be surprised by opposing force actions / activities) and successfully “adjust fire” to meet command intent as the situation evolves.

As the Army works to create crew-served weapons systems and organizations for executing future operations, the wide range of OE to be encountered by these organizations remains largely unknown. What is known is the certainty of the continued expansion of the Internet of Things (IoT) capabilities of the interdependent networks of sensors and actuators and the continued deployment of the Fifth Generation (5G) of the long-term evolution (LTE) cell-based communications capabilities.

The rest of this post attempts to provide a summary of the expected technical implications of these two ongoing evolutions for future mission command decision support applications and operational environment ISR state estimation applications. The assertions made in the note are dependent upon the assumptions below regarding these two dominant technical trends:

1. The IoT will continue to expand and will result in billions of vulnerable sensors and actuators subject to being exploited to surprise individual, tactical, operational, and strategic echelons regarding the state of the OE. Distributed clocks can now be routinely synchronized to within 1 nanosecond[13] and more precise synchronizations are possible.

2. The pace of 5G communications deployments will continue to accelerate and the resulting increase in distributed communications capabilities will support massive increases in the sharing of data among the IoT sensing and actuating devices and their associated automated control systems.

The result of these two trends is to increase the ability of threats (from script kiddies to nation states) to exploit ongoing technical advances to achieve surprise at multiple echelons of command.

The implications of the recent malware attacks on critical infrastructures around the world and the demonstrated ability to compromise sensors at the lowest level have profound implications for future ISR systems as well as for future mission command decision support tools. One approach for abstracting the various processes for accumulating evidence for making decisions is the data-information-knowledge-wisdom (DIKW) triangle[11] (Figure 2). While formal logical analysis is preferred for achieving provably-correct results, the key challenge is that proving the absence of malware is an undecidable problem (like the halting problem). Thus, since formally proving that malware is not present in a working system is not a computable problem, most product-line solutions for complex systems (cars, aircraft, missile engagement) use algorithmic logic to achieve resilient control of distributed systems. The algorithmic logic includes both event-based algorithms and physics-based algorithms and the available solutions to the set of discrete and continuous constraints is not provably correct. Also, most humans-in-the-loop use intuitive logic based upon previous experiences to make decisions.

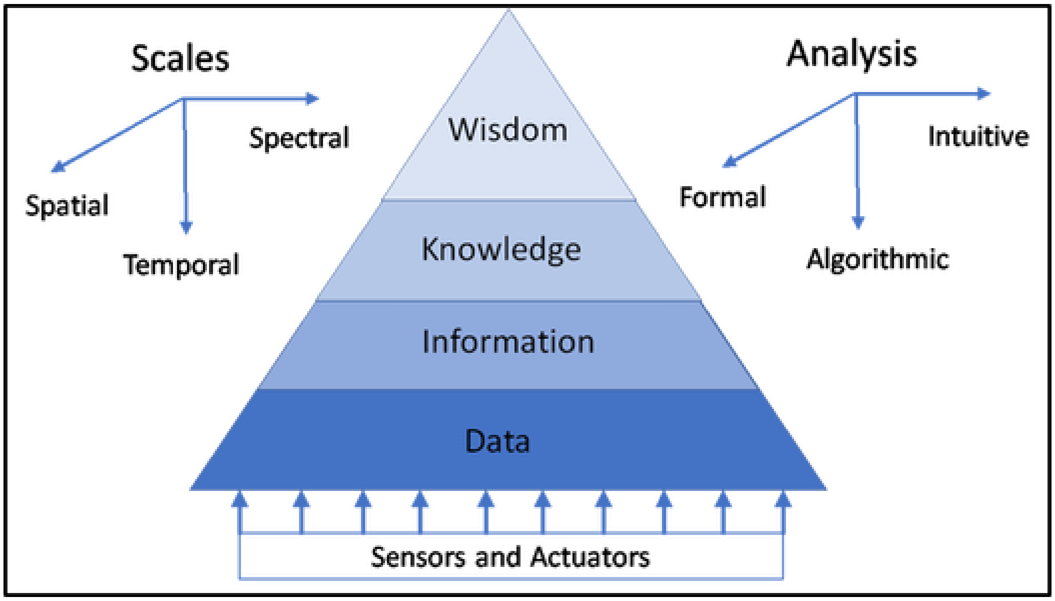


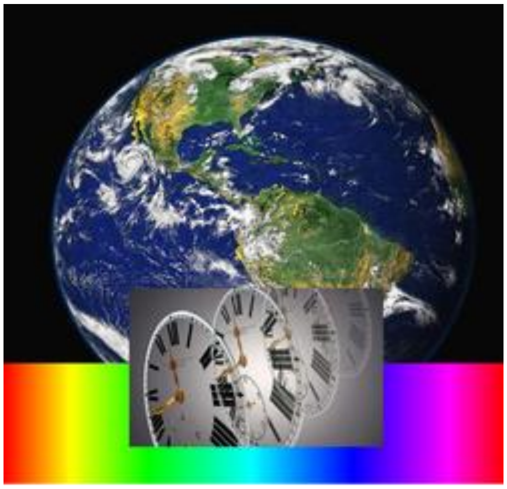
Figure 2. The data, information, knowledge, wisdom (DIKW) triangle.

In addition, achieving a common operational picture across echelons of mission command is a very difficult problem. Temporal, spatial, and spectral scales of interest span multiple orders of magnitude in their respective domains, making consistent visualizations of the situation very challenging.

Previously, commanders and staffs did not have to consider the possibility of opponents being able to capture hundreds of thousands of vulnerable sensors and actuators to perform deception / surprise operations. However, massive Distributed Denial of

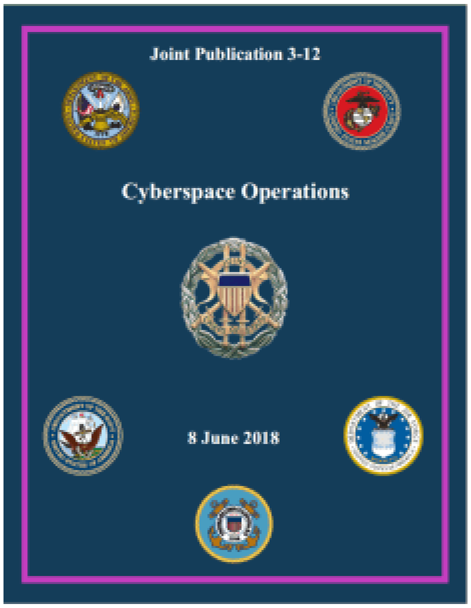
Service (DDoS) attacks have occurred through the capture and exploitation of hundreds of thousands of home local area network wireless routers and other devices.[10]

Such results demonstrate the ability to exploit vulnerable IoT devices, including capture of vulnerable sensors and actuators, to affect estimates over time scales of nanoseconds to years; over spatial scales of millimeters to thousands of kilometers; and over spectral scales that span the electromagnetic spectrum.



Moreover, deception / surprise has been demonstrated to be possible at the lowest possible level / echelon of man-machine interfaces.[9] Thus, a security service critical to avoiding surprise at every echelon of command will be a service to ensure non-repudiation of data being shared among nodes in the state estimation and control devices within each echelon and subsequently of data being shared between echelons. A recent cadet blockchain project [7],[8] demonstrated one approach for attaining non-repudiation of data shared among a whitelist of trusted partners to increase trust in shared data. Also, the man-in-the-middle attack of sensor data project[9] demonstrated that even non-repudiation is insufficient to prevent sharing of bad data if the data can be corrupted by changing data in the payload of packets between the sensor and higher-level applications. The corruption of data is possible even if the data packets are being sent in accordance with data transmission protocols over a trusted Ethernet network link. An idea which may be investigated in the future to address the data corruption result is to use redundant sensors to measure critical parameters, apply the blockchain result to share data among multiple sensors, and use a voting scheme to identify compromised/failed sensors.

A series of smart grid projects, including those discussed in these references,[7],[8],[9] have been coordinated over the past four years by **Dr. Aaron St. Leger** of the Department of Electrical Engineering and Computer Science at the United States Military Academy. For two years, a series of joint microgrid experiments involving Anomaly Detection of Cyber physical Systems (ADCPS) were supported by the Office of Naval Research (ONR).[14],[15],[16] Six microgrid emulators and/or simulators located at six institutions in five states (Idaho National Laboratory [INL], Army Research Laboratory [ARL], Iowa State University [ISU], United States Naval Academy [USNA], United States Air Force Academy [USAFA], and United States Military Academy [USMA]), were used to conduct experiments to improve technologies available for detecting, analyzing, and reacting to cyber and physical anomalies (failure modes) affecting distributed state estimation and control of the smart grid.



Joint Publication 3-12

Cyberspace Operations

8 June 2018

The ADCPS team in the past has applied machine learning (ML) approaches for identifying cyber and physical anomalies. Cyberspace has joined the land, sea, air and space domains of warfare as the fifth domain of warfare. The Department of Defense has recently issued the top-level operations document for conducting warfare in cyberspace.[17] It may be the case that future ML approaches may be useful in answering questions related to cyber key terrain. ML may be useful in answering questions such as:

1. How do we **detect** cyber-physical failures?

2. How do we **categorize** cyber-physical failures?

3. How do we **measure the impact** of cyber-physical failures?

4. How do we **measure the resilience** of cyber-physical systems subject to cyber-physical failures?

However, a growing problem in the application of ML systems is the possibility of adversarial activities affecting the usefulness of ML results.[12] Thus, another possible application of non-repudiation of shared information is the use of permissioned blockchain technology to improve the integrity of ML results. In addition, a barrier to wider use of ML results is the “black box” nature of recommended actions and the brittleness of the solutions for rare events. Thus, another line of possible investigations is to determine the possibility of use of ML technologies to incrementally improve the algorithmic models resulting from physics-based analysis.

In any event, recent cyber events affecting a broad range of critical infrastructures have verified the importance of improving available technologies for understanding the behaviors of distributed complex systems and especially in improving the capabilities for ensuring the non-repudiation of data received from the bottom of the data-information-knowledge-wisdom food chain, that level being the level of sensors and actuators. Since success in cyberspace operations will be critical for ensuring success in all combat domains, a key capability in future warfare will be recognizing the high ground of key terrain for cyberspace operations and ensuring that commanders have the confidence that they can recognize that cyberspace high ground, and can seize and exploit it.

Over 30 years ago the Directorate of Combat Developments of the U.S. Army Infantry Center developed a requirements document indicating the need to develop robotic systems to aid maneuver force commanders in conducting Reconnaissance, Selection, and Occupation of Position (RSOP) operations for maneuver forces. Today, this ISR capability is available with the emergence of a range of robotic vehicles, including swarms of quadcopters, which have demonstrated capabilities to improve the commander's estimate of the situation and reduce the attrition of forces in conducting RSOP of physical terrain.

Today and for the foreseeable future, commanders need a similar capability to identify elements of key terrain in cyberspace. Cyber operations are necessary for the execution of operations across the domains of warfare to meet the intent of the commander. This is true because the intent of the commander is mathematically the only stationary point in the evolution of the dynamics of the state space of measurements of variables across the temporal, spatial, and spectral scales of warfare. That is, in the American doctrine of warfare, everything is subject to change during a combat operation except the intent of the commander. Thus, commanders at each echelon are expected to understand the intent of the highest level of command and exercise "good military judgement" to adjust operations at their echelon to meet command intent.

CONCLUSION

This doctrine is consistent with Eisenhower's observation that "Plans are worthless, but planning is everything."[4],[5] Humans understand command intent through the planning process and apply intuitive logic to adjust operations to meet command intent. Unfortunately, technology is currently inadequate for machine "understanding" of intent to match human understanding of intent. The ongoing information systems revolution has transformed the way that humans interact with each other and how machines interact with humans. Thus, we are faced with a need to be continuously suspicious of what our machines are telling us because we know that we cannot prove that they have not been compromised by malware. Tools are needed to "trust but verify" that our machines are performing as expected. Like the capability available today to deploy robotic vehicles to reduce force attrition when conducting RSOP operations of physical terrain, commanders need similar tools for conducting RSOP operations of cyber terrain.

If you enjoyed this post, please also read:

Our companion piece to this blog post, **A New Era of Network Architecture**.

Takeaways Learned about the Future of the AI Battlefield, and our associated ***Crowdsourcing the Future of the AI Battlefield*** paper.

The Guy Behind the Guy: AI as the Indispensable Marshal, by Messrs. **Brady Moore** and **Chris Sauceda**.

The Human Targeting Solution: An AI Story, by **CW3 Jesse R. Crifasi**.

Influence at Machine Speed: The Coming of AI-Powered Propaganda, by **MAJ Chris Telley**.

Dr. John James *commanded three times at the company level (twice with ADA units in Germany and as a District Senior Advisor in Vietnam). His last active duty assignment was as Director of the TRADOC AI Center where he led development of over thirty small knowledge-based decision support systems, at least two of which were used for over 25 years. As a contractor with research engineers from the Lockheed Advanced Technology Laboratories (ATL), he investigated implementation of netted, distributed control of theater-level air defense fires for the Medium, Extended Air Defense System (MEADS). He has been teaching at USMA as a civilian faculty member since 2000.*

REFERENCES

[1] Stuxnet, https://en.wikipedia.org/wiki/Stuxnet accessed on 6 May 2019

[2] Aurora Generator Test, https://en.wikipedia.org/wiki/Aurora_Generator_Test accessed on 6 May 2019.

[3] P. Polityuk, O. Vukmanovic, and S. Jewkes, Ukraine's power outage was a cyber attack, Ukrenergo, Technology News, January 18, 2017, https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA accessed on 6 May 2019.

[4] W.M.Blair, President Draws Planning Moral, New York Times November 15 1957, https://www.nytimes.com/1957/11/15/archives/president-draws-planning-moral-recalls-army-days-to-show-value-of.html accessed on 6 May 2019.

[5] Quote Investigator, Plans Are Worthless, But Planning Is Everything, https://quoteinvestigator.com/2017/11/18/planning/ accessed on 6 May2019

[6] Morel, Thomas et al., Effects-Based Assessment Support System, OPERATIONS RESEARCH CENTER OF EXCELLENCE TECHNICAL REPORT DSE-TR-0539 DTIC #: ADA448132, 2006, https://apps.dtic.mil/dtic/tr/fulltext/u2/a448132.pdf accessed on 6 May 2019

[7] A. St. Leger, J. Spruce, T. Banwell, and M. Collins, Smart grid testbed for Wide-Area Monitoring and Control systems, 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), pp. 1-5, 2016.

[8] C. Banks, S. Kim, M. Neposchlan, N. Velez, K.J. Duncan, J. James, A. St. Leger, D. Hawthorne, Blockchain for Power Grids, Proceedings of the 2019 IEEE SoutheastCon, Huntsville, AL, April, 2019.

[9] J. J. Fritz, J. Sagisi, J. James, A. St. Leger, K. King, and K. J. Duncan, Simulation of Man in the Middle Attack on Smart Grid Testbed, Proceedings of the 2019 IEEE SoutheastCon, Huntsville, AL, April, 2019.

[10] The Guardian, DDoS attack that disrupted internet was largest of its kind in history, experts say, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet accessed on 7 May 2019

[11] D. Weinberger, The Problem with the Data-Information-Knowledge-Wisdom Hierarchy, Harvard Business Review, February 2010. https://hbr.org/2010/02/data-is-to-info-as-info-is-not accessed on 7 May 2019

[12] Wikipedia, Adversarial Machine Learning, https://en.wikipedia.org/wiki/Adversarial_machine_learning accessed on 7 May2019

[13] D. Arnold, What’s coming in the IEEE 1588 revision: Interdomain interactions, https://blog.meinbergglobal.com/2019/03/01/what-to-expect-in-the-ieee-1588-revision-interdomain-interactions/ accessed on 7 May 2019

[14] J. James, M. Lanham, F. Mabry, T. Cook, A. St. Leger, D. Opila, K. Kiriakides, J. Stevens, C. Rieger, K. Duncan, Anomaly Detection of Cyber Physical Systems (CPS), 85th Military Operations Research Society (MORS) Symposium, West Point, NY, 22 June 2017.

[15] M. Berman, G. Dudevoir, K. Duncan, M. Govindarasu, J. James, D. Opila, C. Rieger, A. St. Leger, E. Shaffer, V. Kumar-Singh, Anomaly Detection of Cyber Physical Systems (CPS) Overview, 86th Military Operations Research Society (MORS) Symposium, Monterey, CA, 20 June 2018.

[16] M. Berman, G. Dudevoir, K. Duncan, M. Govindarasu, J. James, D. Opila, C. Rieger, A. St. Leger, E. Shaffer, V. Kumar-Singh, Anomaly Detection of Cyber Physical Systems (CPS) Benchmark Problem, 86th Military Operations Research Society (MORS) Symposium, Monterey, CA, 20 June 2018.

[17] JCS Pub 3-12, Cyberspace Operations, 8 June 2018.