Title: Combining Cyber, EW and Kinetic Maneuvers in MDO

Author: Patrick D. Allen, Johns Hopkins University Applied Physics Laboratory

Abstract:

Recent literature has discussed the use of offensive and defensive cyber maneuvers (CMs) and schemes of maneuver in cyberspace.[1,2] Because CM is a contributor to Multi-Domain Operations (MDO), a next logical step is to describe a more encompassing campaign that incorporates CMs, Electronic Warfare (EW) and kinetic maneuvers into a synergistic set of effects. This presentation focuses primarily on the desire to *manipulate the cognitive views and decisions* of the adversary facing threats and disadvantageous outcomes across a range of dimensions. The goal is for the adversary to face a rapidly increasing sequence of bad results that eventually exceeds their ability to cope. Placing the adversary on the "horns of a dilemma" means that any decision results in a poor outcome for the adversary.[3] Placing the adversary in succeeding dilemmas at an increasing rate can demoralize and paralyze an adversary. The paper highlights some of the requirements for the information necessary to synchronize the cyber, EW and kinetic capabilities. This will require substantial fusion of information across a wide range of existing and emerging data sources and command and control systems necessary to plan, maneuver, execute, and achieve the desired synergy of actions across MDO, as well as measuring their effects. For purposes of measuring effects, we examined the Joint Director of Labs (JDL) Data Fusion Information Group (DFIG) levels 4, 5 and 6, and concluded that a reduction in the latency of the Processing, Exploitation and Dissemination (PED) process and its supporting approval process will be essential to achieving these goals.

Purpose

The purpose of this paper is to describe the fusion requirements for an approach to Multi-Domain Operations that focuses primarily on achieving significant cognitive effects on our adversaries using synchronized cyber maneuvers, electronic warfare (EW) and kinetic actions.

Introduction

All conflict is a battle of wits: Our minds against the minds of our adversaries.

---

[1] Allen, P. (2020). Cyber Maneuver and Schemes of Maneuver. *Cyber Defense Review*, *5*(6). https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2006_Allen.pdf?ver=SGIrAHDc1d3ZOrQihG_XFg%3D%3D

[2] Applegate, S. D. (2013). The Dawn of Kinetic Cyber. *NATO CCD COE Publications*. https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf

[3] The phrase "horns of a dilemma" describes placing the adversary in a position of two options, where both options cause the adversary to lose something significant. B.H. Liddell Hart, *Strategy*, Praeger, New York, 1954, p. 152.

Because cyber and electronic warfare (EW) tend to be very technical, it is easy to lose sight of our real target—the minds of the adversaries. Moreover, the technical nature also makes it difficult to aggregate situational awareness and decision-supporting information to our leaders. Most military leaders are well-versed in kinetic operations, but have limited exposure to cyber maneuvers or electronic warfare.

What is needed is a more top-down approach to why we are fusing information and capabilities in the first place: to achieve desired effects on the minds of our adversaries, and to support our non-technical decision makers in making better-informed decisions.

Describing Cyber Maneuver

We will introduce the concept of cyber maneuver first since that is relatively new compared to EW and kinetic operations. The following definition of Cyber Maneuver is adapted from the Fall 2020 issue of Cyber Defense Review:[4]

> Cyber maneuvers are actions taken in and through cyberspace to achieve positional and temporal advantages over an adversary in the physical, technical and cognitive domains. These advantages are typically achieved by rapidly implementing multiple maneuvers in sequence or in parallel, but can also be achieved by single, significant maneuvers.

- Cognitive advantages include having better information about a situation; surprise, deception, apparent invincibility; the ability to manipulate adversary thoughts & actions, and *undermining adversary confidence*
- Cognitive *positional* advantages include gaining dominance over the minds of the adversary with respect to their views of their options, chances for success, confidence in their situation, and will to continue the conflict
- Physical and Technical *positional* advantages include having access where and when desired, thus allowing for unhindered use of cyberspace to achieve objectives against the adversary
- Temporal advantages include being able to choose not only when desired effects actually occur, but also choosing when the adversary is made aware of the threats or results of those actions

The article cited above lists 21 different categories of cyber maneuvers, within which are included various types of cyber actions. More categories will likely be added in the future, but this is a useful starting point. Some of the cyber maneuvers are similar to traditional psychological operations principles, others are similar to common hacking principles, and some are similar to the traditional kinetic principles. Each maneuver category below is marked as being either an offensive cyber operation (OCO) or a defensive cyber operation (DCO) or both. The four underlined categories are the ones that will be used as examples in this article. For details on the remaining cyber maneuvers, please see the Fall 2020 issue of Cyber Defense Review.

[4] Allen, Ibid.

Cyber Maneuver Principles Similar to Kinetic Principles

- Ambush: Attract an adversary into a hidden "kill zone" (OCO, DCO)
- Herd: Push or Turn an adversary into a hidden "kill zone" (OCO, DCO)
- Stimulate a Response (DCO)
- Probe Adversary (OCO)
- Distract (OCO, DCO)
- Delay Adversary (OCO, DCO)
- Launch Spoiling Attack (OCO, DCO)
- Launch Supporting Attack (OCO)
- Counterattack (OCO, DCO)
- Counter Asymmetric Advantage (OCO, DCO)
- Leverage Deception (OCO, DCO)

Cyber Maneuver Principles Similar to Psychological Operations (PSYOP) Principles

- Undermine Adversary Confidence (OCO, DCO)
- Create False Sense of Security (OCO)
- Appear Invincible (OCO, DCO)
- Leverage Shifting Allegiances (OCO, DCO)
- Employ Influence Messaging (OCO, DCO)

Common Cyber Hacking and Counter-Hacking Principles

- Change the Terrain (or Manipulate the Network) (OCO, DCO)
- Ensure Persistence (OCO)
- Leverage Perishability
- Vary Launch Points (OCO)
- Apply Social Engineering (OCO)

The purpose for offensive cyber maneuvers is not only to find vulnerabilities, but to create them! We will provide an example of the ambush cyber maneuver to elaborate on this point, as shown in Figure 1.

In Figure 1, the U.S. is the attacker (on the left hand side). Steps 1 and 2 are to infect a leaf (alpha) node and upstream (beta) node on adversary network. The infected alpha node then lets the defender know it has been infected. In steps 3, 4, and 5, the adversary reacts to the information that the alpha node has been infected and remotely logs in to "clean it up" using their standard toolkit. While the defending adversary is in the midst of the clean-up process, the U.S. attacker performs a man-in-the-middle attack on the tools in the defender's toolkit from the infected beta node.

Later, the defender uses the infected toolkit to repair other assets. The infected toolkit has U.S. malware that randomizes the types of subsequent infections and timing of the launch of the infection to make it difficult for the defender to figure out the real source. Whether and how long this ambush maneuver will work against an adversary depends on how good the defender's cyber hygiene is with respect to their toolkit.

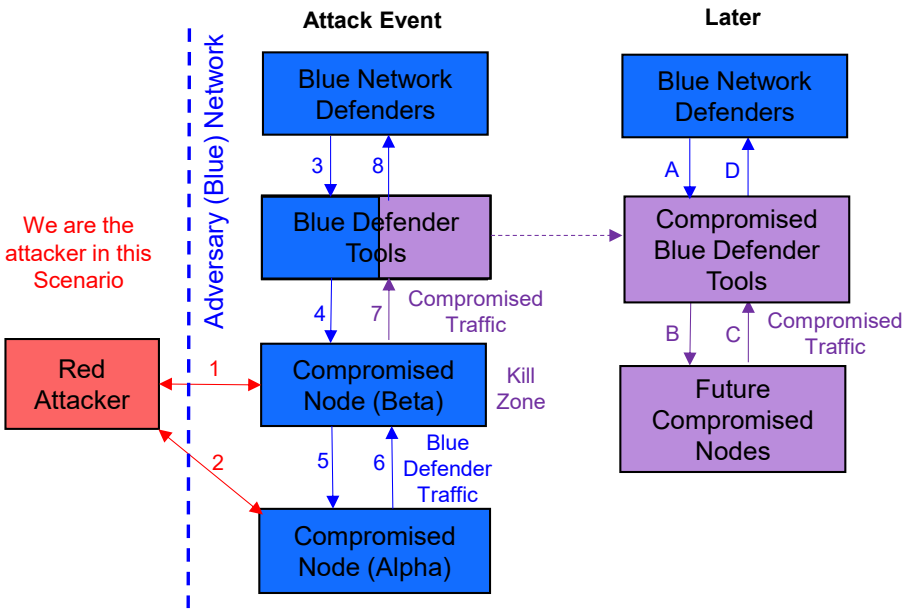

Figure 1: Ambush Example of Cyber Maneuver: Creating Vulnerabilities

However, even after the adversary knows about such ambushes, this maneuver action can act as a distraction for other cyber actions being performed elsewhere on the network. The use of the ambush maneuver can make the adversary "gun-shy" to fix problems immediately, which could achieve the delay in an adversary response that was the actual desired effect. As long as we can keep the adversary defender delayed through paralysis (not knowing whether it is a trap), we can accomplish a lot of actions while they think it over. Increasing the adversary's uncertainty and decreasing the adversary confidence in their networks are key objectives. The more often we place the adversary on the "horns of a dilemma," the more demoralizing the effect of always having to select from a set of only bad outcomes.[5]

More Cyber Maneuvers

The remaining three cyber maneuvers we will use as examples are described in this section, while the next section describes how cyber maneuvers are tied together in a scheme of maneuver.

- Undermine Adversary Confidence
- Create False Sense of Security
- Appear Invincible

Undermining adversary confidence shakes the adversary's confidence in its resources**.** During the First Gulf War, Coalition forces would come up on the Iraqi military radio nets and announce coalition

[5] Hart, Ibid.

presence, thereby proving they were literally operating within the Iraqi communications space.[6] These on-net announcements had a devastating effect on Iraqi morale, with lost confidence in the confidentiality, integrity, and even availability of working communications. A similar set of cyber maneuvers can be performed, for example, by leaving messages on adversary computer screens, confirming U.S. access to their network. Such messages will cause the adversary to lose confidence in the confidentiality, integrity, and even future availability of their cyber networks.

Of course, the adversary will attempt to block these messages and take actions to do so. At some point, the U.S. attacker should pretend that the actions taken succeeded in stopping the U.S. access to their networks. This creates a **false sense of security** for the adversary that is unfounded. The adversary mistakenly believes its actions are what stopped our messages. Note that the use of maneuvers to cause the adversary to lose confidence in its resources, followed by a false sense of security maneuver, is a good combination to employ as a pair within a scheme of maneuver, as described below. At some time in the future, the U.S. attacker restarts the messages to further undermine the confidence of the adversary in their network, as they were sure they had blocked the original attack vector.

This leads to the next maneuver, projecting the **appearance of invincibility**, which can also seriously degrade the adversary's morale. In some cases, the adversary is truly helpless, such as when the Operation Desert Storm (ODS) Coalition had air superiority over Iraqi ground forces and could bomb them at will.[7]

In other cases, the invincibility may merely be an illusion. The following cyberspace example dates from when "Anonymous," in its heyday, would announce that on a certain date on the following week, nothing could be done to stop the hacking of a given target. The author is not sure if the following is what Anonymous did, but it is likely that Anonymous would have already hacked the target and planted several back doors. They could also have already downloaded materials unique to the target to prove the target was hacked, even if the target disconnected from the Internet. Sure enough, whenever Anonymous declared a target would be hacked, it was. Whether Anonymous really could hack any target or had already hacked the target was irrelevant, as either way, *it gave the impression of invincibility*. The appearance of invincibility directly strikes against the cognitive status of the adversary and can significantly degrade the adversary's will to continue the conflict.

Scheme of Maneuver for Preceding Scenario

Individual CMs can be useful, but a set of parallel or sequential CMs can be combined into a Scheme of Maneuver as part of the commander defining his or her intent.

---

[6] Al Zdon, "Persian Gulf War Ten Years Later: Winning the war by convincing the enemy to go home," http://www.iwar.org.uk/psyops/resources/gulf-war/13th_psyops.htm.
[7] Zdon, Ibid.

Assume that the U.S. commander has been assigned the mission to deter the country of Badistan from invading a U.S. ally Guderland using non-kinetic means. The scheme of maneuver for this sample scenario is:

> Employ cyber *probing*, *ambushes* and *herding* to *ensure persistent access* to the adversary network. By [specified date], launch actions with the intent to *undermine adversary confidence* in their network resources, followed by *manipulate adversary network* to preclude network connectivity until [specified date and time]. If by this [specified date and time] the adversary has been deterred from invading the neighboring country, execute *create a false sense of security* on their network. If the adversary starts preparing again to invade their neighbor, resume *undermining adversary confidence* and *manipulating adversary network* while executing *appearance of invincibility* maneuvers to deter their resumption of preparations.

Note that the focus is on affecting the adversary minds—their confidence in their networks, and their morale. To support MDO, the scheme of maneuver should also include the EW and kinetic effects, as well as broader branches and sequels, as part of an overall campaign plan.

In addition, the commander does not have to have the technical knowledge of the cyber capabilities in order to include the categories of cyber maneuvers in the scheme of maneuver. The categories of maneuver are sufficiently aggregated that the commander can specify the desired effect and have the staff determine whether and how the achievement of the desired categories of maneuver can be accomplished.

Cyber Maneuver: From Mission to Actions

As shown in Figure 2, the starting point is the mission or objective, such as described in the previous example. The commander develops the "commander's intent" which can be represented by the scheme of maneuver. The scheme of maneuver includes one or more of the maneuver categories. The staff takes the commander's intent (the scheme of maneuver), and selects specific maneuver actions and fires to accomplish the categories of maneuvers.[8]

There are multiple feedback loops in this process. The longest, on the right, includes experimentation and training. The medium feedback loop on the left is based on situational awareness and intelligence based on the likely or actual results of the actions. The shortest feedback loop is in the interior, where immediate feedback from the actions can trigger branches and sequels within the scheme of maneuver or provide some measure of the achievement of the mission or objective.

[8]Allen, Ibid.

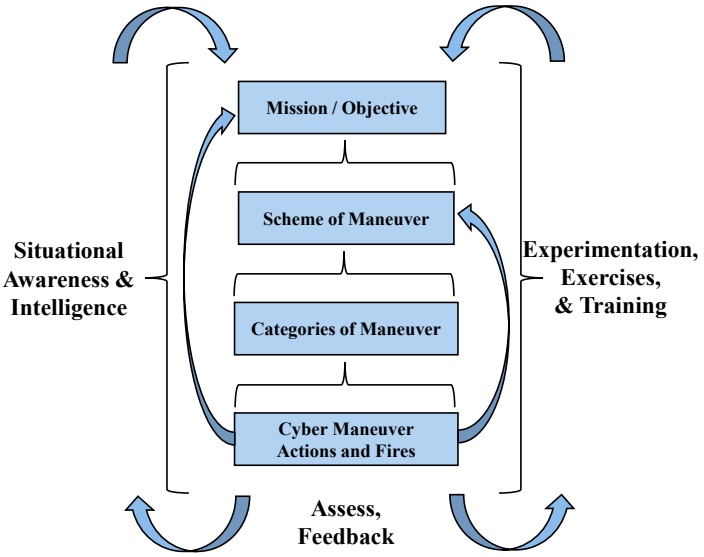

Figure 2: From Mission to Cyber Actions and Fires

Supporting Multi-Domain Operations (MDOs)

Here is a short summary of MDO:

> Our adversaries are *competing* with the US short of conflict, using political, military, and economic means to separate the US from its partners. "The **central idea** in solving this problem is the ***rapid and continuous integration of all domains of warfare*** to deter and prevail as we ***compete*** short of armed conflict." During conflict, our adversaries "will employ ***multiple layers of stand-off*** [attacks] in ***all domains—land, sea, air, space and cyberspace***—to separate U.S. forces and our allies in time, space and function in order to defeat us… ***The U.S. Army in Multi-Domain Operations 2028*** concept proposes a series of solutions to solve the problem of ***layered standoff.*** *"* ***"Multi-domain formations*** possess the capacity, endurance and capability to access and employ capabilities across all domains to pose multiple and compounding dilemmas on the adversary." [Text as highlighted in the original; cyberspace defined in JP 3-12.][9]

Cyber maneuvers are one component of MDO, and focus on the warfighting function of maneuver within and through cyberspace. Offensive and defensive CMs support MDOs outside of cyber, and vice versa, as part of MDO doctrine integrating the warfighting functions during both competition and conflict. Work by Nichols and the Congressional Research Service has previously described approaches

[9] TRADOC PAM 525-3-1 "The U.S. Army in Multi-Domain Operations 2028," December 6, 2018, Preface.

to bringing diverse elements together.[10,11] The following sections provide examples of how cyber, EW and kinetic maneuvers, actions and fires can combine to achieve combined desired effects.

IADS Scenario Combining CMs, EW, and Kinetic

The mission for this scenario is to take down an adversary's integrated Air Defense System (IADS). As shown in Figure 3, supply chain compromises (shown on far left) may have been accomplished prior to the counter IADS mission, which could assist the cyber maneuvers and possibly EW capabilities as well.

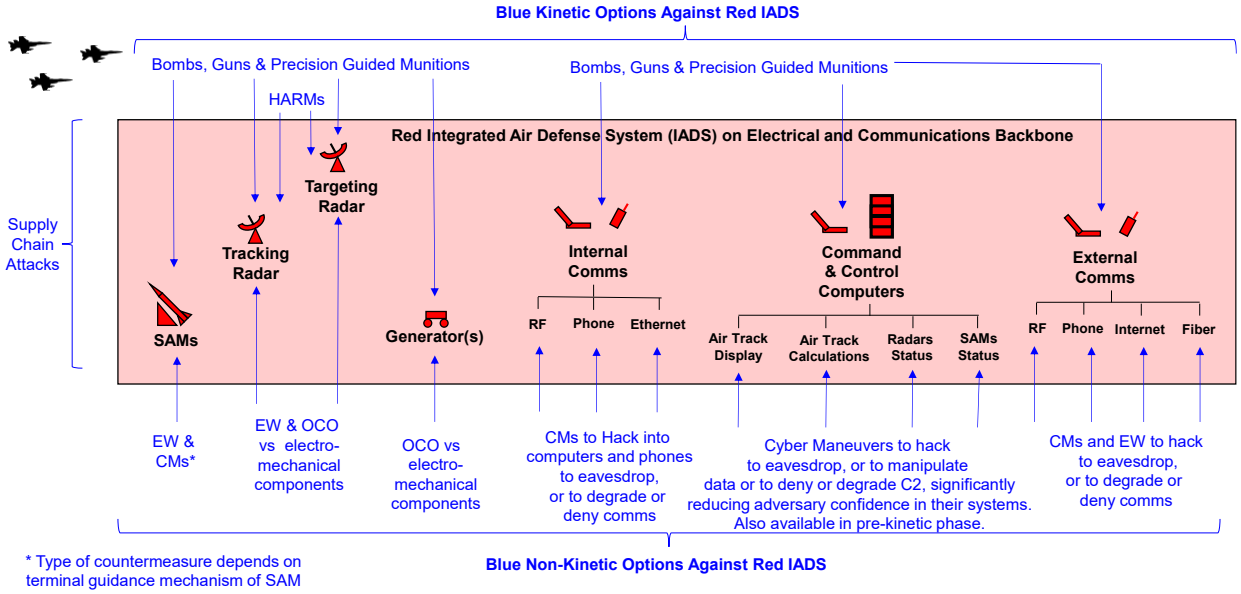

Figure 3: IADS Scenario for Combining Effects CM, EW, and Kinetic Effects

The top row of the figure shows the types of kinetic capabilities that could be brought to bear against the various elements of the adversary's IADS. The SAMs, tracking and targeting radars, generators, internal and external communication and their command and control computers could all be attacked via kinetic means, assuming the locations of the targets are known and accessible.

The bottom row of the figure shows the opportunities for the use of EW and Cyber Maneuvers and actions to affect these same target categories. EW can be used against the SAMs and radars, and jamming can be accomplished at least against the external long-haul communications. CMs can be used against all of the target categories listed above due to the increasing reliance on cyber hardware and software across the IADS. Depending on access availability, cyber effects could include disrupting the

[10] Nichols, R. K. (2020). Chapter 9: Non- Kinetic: Military Avionics, EW, CW, DE, SCADA Defenses. In *Counter Unmanned Aircraft Systems Technologies and Operations*. Pressbook. https://kstatelibraries.pressbooks.pub/counterunmannedaircraft/chapter/chapter-9-non-kinetic-military-avionics-acoustic-defenses-iff-library-nichols/

[11] Convergence of Cyberspace Operations and Electronic Warfare. (2019). *Congressional Research Service*. https://fas.org/sgp/crs/natsec/IF11292.pdf.

electromechanical components of the SAMs or radars, as well as the generators. All of the internal and external communications channels, and especially the command and control computers, are subject to cyber attacks.

Note that while this example shows mutually supporting effects during a kinetic operation, the cyber maneuvers could also be used during the pre-kinetic phase of operations, performing the sample scheme of maneuver described previously. Causing the adversary to lose confidence in their C2 systems prior to the start of kinetic operations, and then giving the adversary a false sense of security, are excellent set-up conditions for the kinetic and EW operations and resumption of CMs. This could lead to a successful maneuver providing the appearance of invincibility of our capabilities. The cognitive effects on the confidence and morale of the adversaries are the focus of these CMs.

Information Fusion Requirements for Combining CMs, EW, and Kinetic

Figure 4 presents some sample information and fusion requirements for achieving the combined CM, EW and kinetic effects described above.

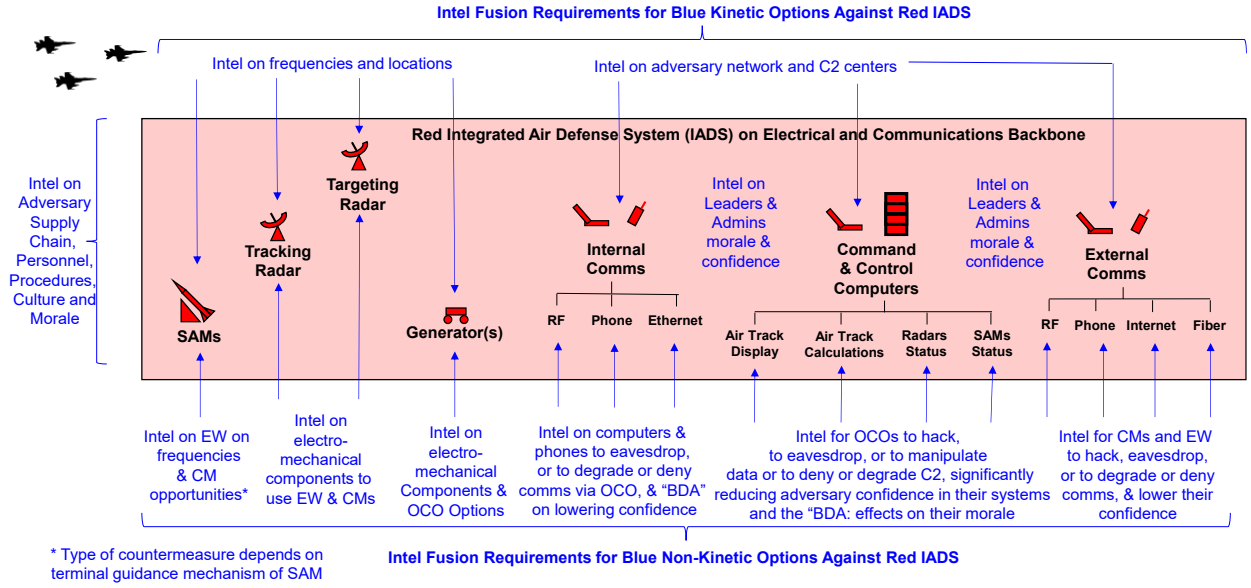

Figure 4: IADS Scenario for Information Fusion Requirements for CM, EW, and Kinetic Effects

Starting on the left hand side, information would be required not only about the supply chain, but also about the adversary's personnel, procedures, culture and overall morale. These latter aspects will be useful in determining the type and timing of the cognitive effects planned against the adversary. The top row lists the usual intelligence requirements for the preparation of a kinetic attack, while the expanded bottom row includes intelligence requirements for the EW and cyber maneuvers to achieve cognitive effects. The new middle row includes intelligence requirements and fusion of information about the adversary's leaders, system administrators, and other key personnel.

These intelligence requirements are needed for pre-kinetic, kinetic, and post-kinetic operations, as well as the assessment of effects in each of these three phases. For example, did the cyber maneuvers cause a lack of confidence in the adversary's command and control and communications systems? Does the adversary think they have that situation under control prior to the launch of the combined CM, EW and kinetic operation? What are the effects on the adversary's morale during and after the kinetic phase of the operation? Is their confidence undermined, and what is their level of will within the targeted units to continue the conflict?

Overall, MDO campaign planning, execution and battle damage assessment (BDA) will require both traditional and emerging sensors, focusing heavily on the measures of cognitive status of our adversaries. The U.S. and our allies will need to assess results at each stage of the campaign. Fusion is required on the planning, execution and BDA, not just for kinetic and EW effects, but also on the cognitive effects on the adversary. This supports the Joint Director of the Labs (*JDL*)/Data Fusion Information Group (DFIG) model Levels 4, 5, & 6. (Level 4 is Process Refinement, Level 5 is Cognitive Refinement, and Level 6 is Mission Refinement.)[12] Note that the timing of the actions and the timing of the desired effects may not be identical, especially for cyber maneuvers. In contrast, the timing of the effects for kinetic and EW tend to coincide with the actions.

Current MDO Fusion Limitations and Opportunities

Collecting, sharing and fusing such a wide range of information for cyber, EW and kinetic will require new processes or the modification of existing processes to focus more heavily on synchronizing the cognitive effects on the adversary. For example, there is a need to consider and synchronize (or even develop) a much broader range of intelligence sources and fusion than in the past to synchronize these many CM, EW, and kinetic elements to achieve the desired cognitive effects on the adversary.

Current sensors are not synchronized for BDA of cognitive effects and status of the adversary. However, due to the explosion of information in the commercial world, planners may be able to leverage more OSINT sources than were previously available. In addition, the continued advances in Machine Learning and Artificial Intelligence may help speed the collection, sharing and fusion processes.

The Processing, Exploitation and Dissemination (PED) system, however, will need to run on a faster cycle to better incorporate cyber and EW effectively with kinetic. The reason is that the speed of cyber and EW actions are much faster than the kinetic cycle. For example, the Joint Targeting "Chicklet Chart" is very manual and may not be sufficiently rapid to support the necessary speed of approving combined targets in its current form. Preapproved cyber actions will likely be required to meet the pace of conflict at the speed of cyber.

In addition, policies on cyber actions may need to provide expanded freedom of action to achieve the desired, synchronized cognitive effects.

[12] Data Fusion and JDL, Wikipedia, downloaded 25 Oct 2021.

Closing Observation

- Where we are: MDO is a great way forward to drive the combination of cyber, EW and kinetic effects.
- Where we want to be: Need to focus primarily on achieving the cognitive effects against the adversary, not just technical effects. For example, messaging by action can include undermining their confidence, giving them a false sense of security, then hitting them again with an appearance of invincibility
- What we need to do to get there: Determine the necessary data sources, exploit them, combine them focusing on mainly achieving the cognitive effects, supported by the current technical effects

Summary of Key Points

MDO is a promising way forward. To achieve the best results from MDO, we need to focus primarily on achieving the desired cognitive effects on the adversary, though it is the technical capabilities that implement the effects.

There is a need for more information to support achieving, and measuring the achievement of, these cognitive effects. This will require greater exploitation of additional or as-yet unsynchronized data sources. Leveraging new sources of OSINT, and applying machine learning and artificial intelligence, provides new opportunities to achieve the desired cognitive effects by understanding adversary mindsets under various types of stressors.

Cyber maneuvers, EW, and kinetic can together provide the synchronized effects that constantly place adversary on horns of a dilemma, limiting the adversary to selection from a set of bad outcomes.

References

- Allen, Patrick D., "Cyber Maneuver and Schemes of Maneuver: Preliminary Concepts, Definitions and Examples," *Cyber Defense Review*, Vol 5 No.3, Fall 2020. https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2006_Allen.pdf?ver=SGIrAHDc1d3ZOrQihG_XFg%3D%3D
- Applegate, S. D. (2013). The Dawn of Kinetic Cyber. *NATO CCD COE Publications*. https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf
- Convergence of Cyberspace Operations and Electronic Warfare. (2019). *Congressional Research Service*. https://fas.org/sgp/crs/natsec/IF11292.pdf.
- Hart, B.H. Liddell, *Strategy*, Praeger, New York, 1954.
- Nichols, R. K. (2020). Chapter 9: Non- Kinetic: Military Avionics, EW, CW, DE, SCADA Defenses. In *Counter Unmanned Aircraft Systems Technologies and Operations*. Pressbook. https://kstatelibraries.pressbooks.pub/counterunmannedaircraft/chapter/chapter-9-non-kinetic-military-avionics-acoustic-defenses-iff-library-nichols/

- TRADOC PAM 525-3-1 “The U.S. Army in Multi-Domain Operations 2028,” December 6, 2018.
- Wikipedia, JDL and Data Fusion, downloaded 25 Oct 2021.
- Zdon, Al, “Persian Gulf War Ten Years Later: Winning the war by convincing the enemy to go home,” http://www.iwar.org.uk/psyops/resources/gulf-war/13th_psyops.htm