Winning Tactical Engagements in Contested Environments through C5ISRT Dominance

Andrew J. Newman, William A. Menner, Glenn E. Mitzel, and Mark D. LoPresto

ABSTRACT

The Johns Hopkins Applied Physics Laboratory (APL) Precision Strike Mission Area envisions a 2030 battlespace in which physical domains (e.g., land, maritime, air, and space) and the information domain are heavily contested and strongly coupled in terms of effects and outcomes. Creating a decisive advantage in this battlespace involves building command, control, communications, computing, cyber, intelligence, surveillance, reconnaissance, and targeting (C5ISRT) systems that provide a more complete, clear, accurate, current, assured, and accessible operating picture than an adversary's picture. To this end, this article proposes a new control and analytical framework that views a C5ISRT system as a cognitive dynamical system with a perception-action cycle that continually and collaboratively orchestrates its resources to optimize the situational awareness available for tactical decision-making. The article describes a vision for research and development in battlespace awareness control and anti-control to achieve continuous universal targeting with impunity. We refer to the resulting decisive advantage as C5ISRT dominance.

INTRODUCTION

The strength and credibility of the United States' national security strategy depends on our ability to globally project military power. However, our successful warfare history has prompted adversaries to develop anti-access, area-denial capabilities designed to track and target our forces at increasing ranges from their territories, complicating our operational deployments and challenging our freedom of maneuver in theaters of operation. This reshaping of the battlespace emphasizes information warfare, as evidenced by the US Army's recent creation of the 1st Information Operations Command, the US Navy's push toward dedicated information warfare cells within maritime operations centers, the US Air Force's recent stand-up of its first information warfare command in 16th Air Force, and the US Marine Corps' reorganization that created the Marine Expeditionary Force Information Groups. Without significant and strategic investment in the development of underlying technology enablers, the United States will not realize the benefits of information warfare, which is rapidly becoming a consequential, if not the dominant, domain of conflict with peer adversaries.

APL envisions disruptive technologies to win tactical engagements in contested environments through dominance of the information warfare functions that produce, transmit, interpret, and use information. These functions reside within the opposing command, control, communications, computing, cyber, intelligence, surveillance, reconnaissance, and targeting (C5ISRT) systems and inform the opposing battle management (BM) systems. We refer to the resulting decisive advantage as C5ISRT dominance.

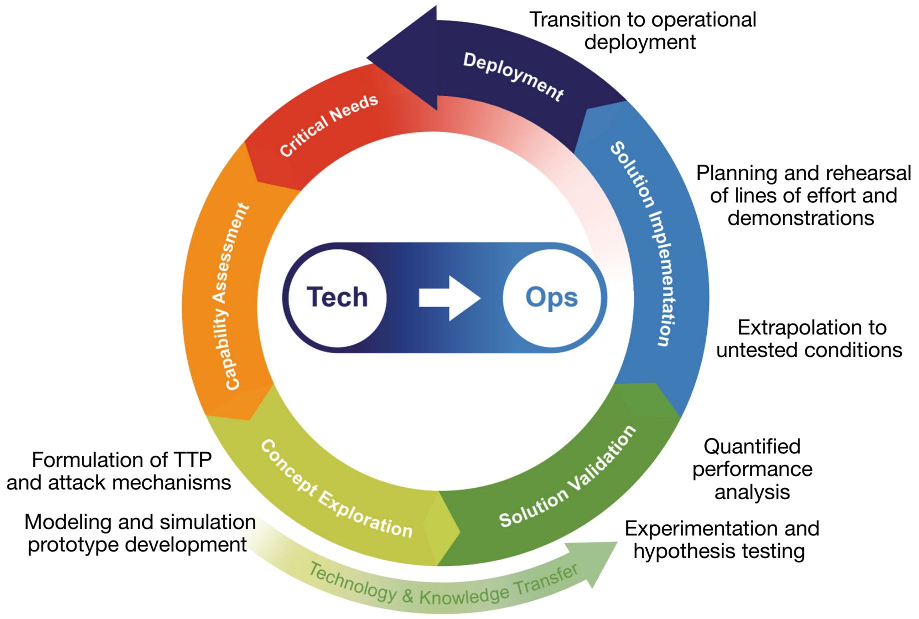
Transition to operational deployment
Deployment
Critical Needs
Solution Implementation
Planning and rehearsal of lines of effort and demonstrations
Capability Assessment
Tech
Ops
Extrapolation to untested conditions
Formulation of TTP and attack mechanisms
Concept Exploration
Solution Validation
Quantified performance analysis
Modeling and simulation prototype development
Experimentation and hypothesis testing
Technology & Knowledge Transfer

Figure 1. APL's end-to-end development and assessment cycle applied to C5ISRT dominance.

Near-peer adversaries currently enjoy advantages in executing and disrupting US kill chains in theaters of interest that are naturally derived through cost asymmetry and battlefield proximity ("home field advantage"). Achieving the vision of C5ISRT dominance would reshape the battlespace and reverse the advantage in the air dominance and force projection domains by enabling precise delivery of effects to disrupt the adversary's C5ISRT system while concurrently strengthening the US and coalition C5ISRT system against counterattacks and increasing its capacity to produce tactically relevant information.

Traditionally, shortfalls in targeting capability for tactical missions have been addressed through substantial investment in specialized and exquisite sensing assets. Conversely, vulnerabilities to adversary kill chains have been addressed by developing tactics, techniques, and procedures (TTP) that deny or deceive specific sensing systems. This naturally results in a perpetual cycle of alternating advantage where the utility of assets and TTP diminishes, and cost expands, over cycles of the competition. The vision described here, by contrast, is to combine technologies at varying readiness levels to achieve greater collective and holistic kill chain effects, which has the potential to break the cycle and provide an enduring advantage at an affordable cost.

We need a new control and analytical framework to understand, predict, and influence C5ISRT system response to a variety of attack mechanisms, both individually and collaboratively. This new framework views a C5ISRT system as a cognitive dynamical system (CDS) with a perception-action cycle (PAC), meaning that it continually redirects its resources to optimize the situational awareness available to support tactical decision-making. From this viewpoint, attack mechanisms are applied to create, modulate, and exploit information gaps that achieve a desired effect on the adversary's decision process. Conversely, our C5ISRT system can dynamically adapt its information flow to resist attempts at disruption and deception. We refer to this framework and approach as battlespace awareness control and anti-control.

APL is developing and using the new control and analytical framework, and a powerful set of modeling and simulation tools, to understand the interactions between competing highly automated and distributed C5ISRT systems. The framework enables combined effectiveness assessments of kinetic, electromagnetic, cyber, materiel, and maneuver TTP, and supports end-to-end development and quantitative assessment of C5ISRT and counter-C5ISRT capabilities and TTP.

APL's C5ISRT dominance vision takes advantage of a broad range of capabilities to provide an end-to-end approach for solving the problem (Figure 1), including formulation of TTP and attack mechanisms, modeling and simulation prototype development, experimentation and hypothesis testing, quantified performance analysis, extrapolation to untested conditions, planning and rehearsal of live experiments and demonstrations, and transition to operational deployment. These capabilities include mature modeling, simulation, and analysis environments, test beds, and test ranges—all informed by APL's deep connection with the strategic, operational, and tactical warfighting communities.

C5ISRT DOMINANCE 2030 VISION

APL envisions a 2030 battlespace in which physical domains (e.g., land, maritime, air, and space) and the information domain are heavily contested and strongly coupled in terms of effects and outcomes. A C5ISRT system that can provide the most complete, clear, accurate, current, assured, and accessible operating picture will provide a potentially decisive advantage. Achieving this advantage involves designing and controlling C5ISRT systems for resilience, such that they maximize mission-relevant awareness and minimize sensitivity to disturbances (e.g., environmental or warfare-related disturbances) and by applying countermeasures that exploit adversary C5ISRT sensitivities to degrade awareness.

APL is currently pioneering technologies directed toward providing the United States and its allies with the capability to disrupt adversary kill chains. A standard depiction of kill chain elements appears in Figure 2. Kill chains typically begin with finding targets and locating (or fixing) them in space and time. The target must then be surveilled to track its location at an accuracy sufficient for targeting and engagement, which is subsequently assessed to determine the possible need for reengagement. A task force studied 73 options for exploiting the vulnerabilities of adversary C5ISRT kill chains in anti-access, area-denial environments. These options were categorized as kinetic, electromagnetic warfare, or cyber operations. Some of these options and others were investigated in APL independent research and development (IRAD) projects in the 2012–2018 time frame. These investigations confirmed the potential of specific techniques for attacking adversary C5ISRT and led to a series of sponsor-funded tasks that are advancing the technology readiness of selected approaches.

The 2030 battle for C5ISRT dominance will include attack mechanisms that alter the environmental stimulus that is sensed (noninvasive attack) and disrupt the information flow within the C5ISRT system (invasive attack). Noninvasive attack or deception mechanisms fall into the general categories of materiel (e.g., decoys), maneuver, kinetic (i.e., physical alteration of the sensed battlespace), electromagnetic (e.g., radio frequency interference), and cyber (e.g., passive reporting of activity). Invasive attack mechanisms include kinetic (e.g., destruction of sensing, communication, and processing nodes), electromagnetic (e.g., jamming of sensing and communications nodes), and cyber (e.g., injection of false information into nodes and links).

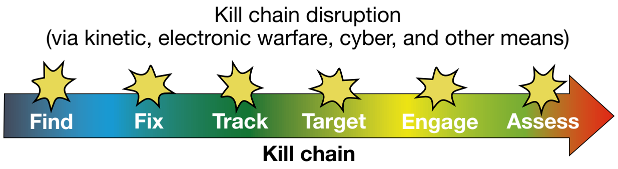

Figure 2. A standard depiction of kill chain elements. APL's vision is to attack the information production, transmission, and utilization functions within the kill chain.

Each such technique is typically intended to mitigate or defeat a particular element of the adversary C5ISRT capability. For this reason, they have largely been studied in isolation to assess effectiveness. However, in reality, a peer adversary's C5ISRT capability will be redundant, layered, distributed, and integrated to some degree. Therefore, it is necessary to understand the effects of technique combinations applied in concert. Coordinated attacks within and across categories will be highly advantageous; effects may be achieved through combinations of altering the stimulus presented to collection systems, directly injecting false information, overloading the capacity of key nodes and links, and directly reducing system capacity by destroying or degrading nodes and links. Stimuli may also be tailored to expose an adversary's vulnerabilities for exploitation. When these activities can be performed inside the adversary's kill chain timeline, the potential exists for inflicting tremendous confusion on the adversary's decision calculus, thereby weakening their situational awareness and potentially their resolve to fight.

Moreover, the competition between opposing C5ISRT systems, each of which will likely be distributed with many highly automated components, will necessarily involve system-versus-system interactions. Figure 3 shows competing C5ISRT systems—the United States (hereafter Blue) on the left and a representative significant adversary (hereafter Red) on the right. Both sides are separated into an intelligence, surveillance, reconnaissance, and targeting (ISRT) function (upper block) and a BM function (lower block) to reflect typical divisions of concern observed in nation-state organizations and ease the analysis and implementation of enablers in this realm. The ISRT function tasks sensors and collects the resulting data, processing it into tracks and other information that drive decision-making for the next cycle of sensor tasking. This PAC is often also called an observe, orient, decide, act (OODA) loop.[1] The BM function has its own OODA loop. Based on a common operational picture (COP) derived from the ISRT function, decisions are made regarding what types of actions (e.g., apply weapons or countermeasures) to take in the battlespace. Each action taken by either side (Blue or Red) may be perceived (sensed) by the opposing side as a stimulus that requires a response. Each response may also be perceived as an additional stimulus, spurring interactions to continue. Sensing and processing the effects caused by the actions of each side updates the COP, providing inputs for a next round of decisions.

Currently, the interactions depicted in Figure 3 are poorly understood and associated TTP do not exist, are uncoordinated, or have uncertain effectiveness. The 2030 vision for C5ISRT dominance is to attack adversary C5ISRT systems in a coordinated manner to achieve precision system-level effects. New approaches and technologies are needed to achieve this vision and enable the broader and more flexible analyses that are indicated.

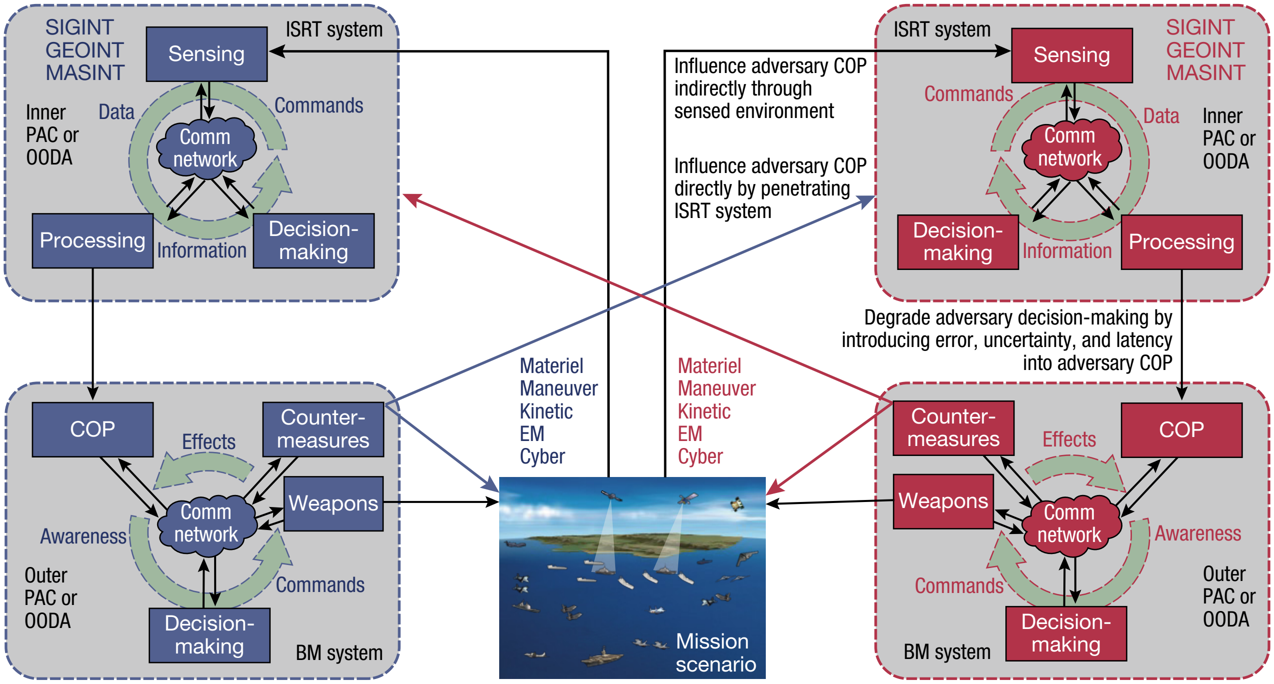

Figure 3. C5ISRT system-versus-system interactions. Left, The United States (Blue). Right, A representative significant adversary (Red). Both sides are represented as consisting of an ISRT function (upper block) and a BM function (lower block). EM, electromagnetic; GEOINT, geospatial intelligence; MASINT, measurement and signature intelligence; SIGINT, signals intelligence.

Battlespace Awareness Control and Anti-Control for C5ISRT System Conflict

It is useful to view a C5ISRT system as a CDS[2] that acquires and maintains situational awareness[3] about an environment, including specific entities within that environment (i.e., for targeting). In this context, a system is "cognitive" only if it has a memory for recalling its prior actions when encountering similar stimuli.[4] This does not mean that the system will take the same prior actions; it means that the system is informed and "smarter" from having encountered similar stimuli. A CDS must adapt to circumstances that are likely to change as conflicts escalate. This is an important property for a C5ISRT CDS that informs a BM decision system (including the human decision-makers) responsible for creating desired effects that realize the mission commander's intent. The ISRT system operates as a feedback system with a PAC that continually redirects sensing, transmission, and processing resources and governs the information flow to regulate the resulting situational awareness. Moreover, the combined ISRT-BM system operates as an outer feedback system with a PAC that continually redirects weapons and countermeasures to regulate battlespace effects.

The capacity of an aggregated suite of C5ISRT systems to adapt its tasking, collection, processing, communication, and targeting capabilities in response to external stimuli is an under-studied problem. Moreover, little is known about how to control such systems to achieve desired performance and robustness objectives. Research is needed to understand the properties and behaviors of C5ISRT systems (in particular within the CDS framework) and how to control (and conversely disrupt) them.

In engineering disciplines, control systems are usually designed based on a trade-off between optimality (performance) and robustness (disturbance rejection). A control law typically seeks to guarantee performance or behavior within certain limits on the uncontrolled exogenous inputs. In a cognitive system, such as a combined ISRT-BM system (ours or the adversary's), the flow of information is of critical importance to performance and robustness. We apply the emerging field of cognitive control theory[4] to understand how to predict the response of an ISRT-BM system to stimuli, how to use the stimuli at our disposal to achieve desired effects, and how to reject or otherwise mitigate such attempts against us.

The available information in a CDS is extracted from noisy measurements (e.g., from sensors). The available information can be partitioned into relevant and redundant information, where the partition depends on what information is needed to perform the task at hand (relevant is needed; redundant is not needed). Therefore, the relevant information is the difference between the available information and the redundant information. As a hypothetical, illustrative example, to estimate the position of a slowly moving target to a precision required for acquisition by a modern weapon seeker, a tracking filter might need a sensor measurement only once per minute (available information); and any additional measurements might be ignored (redundant information). The sufficient information in a CDS is defined as the information needed to perform the task at a desired level of risk or quality. For the previous example, the sufficient information would be the precision of the track on the target that is required for the weapon to strike it with probability above a desired threshold. The information gap in a CDS is defined as the difference between the relevant information and sufficient information (Figure 4, Ref. 4). For the previous example, there might be an information gap if the sensor measurements were not precise enough or received frequently enough (e.g., at least once per minute) to enable weapon engagement.

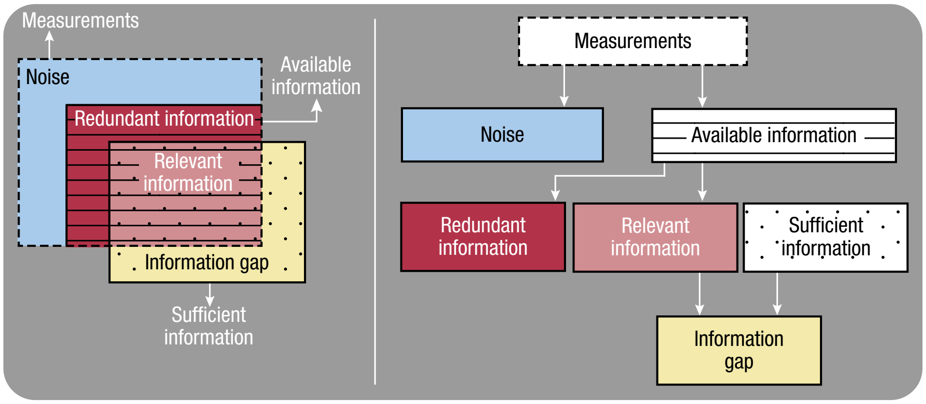

Figure 4. Illustration of the information gap. The information gap is defined as the difference between the relevant information (pink) and the sufficient information (dotted). The relevant information is the difference between the available information (striped) and the redundant information (red). The available information is extracted from noisy measurements. (© 2012 IEEE. Adapted, with permission, from Haykin et al.[4])

The function of cognitive control is to reduce the information gap in a CDS by adapting the directed flow of information from the perceptual part of the system to its executive part.[4] The information must be sufficient for holding a target at risk. The feedback signal in a cognitive control system is the entropic state, which quantifies the information gap and depends on exogenous disturbances, sensing and processing imperfections, and sufficient statistics of the problem. It is clear that the concepts of available, relevant, redundant, and sufficient information, and consequently information gap, are situationally applied to each specific mission or task. Moreover, a CDS could be managing multiple tasks concurrently; and the set of tasks and their respective sufficient information requirements could be evolving situationally.

We refer to *battlespace awareness control* as the application of cognitive control concepts to a C5ISRT system informing a BM system for strike missions. In this case, the information gap would be quantified through a risk function related to the mission gain derived from correct strike decisions and, conversely, the mission loss from incorrect strike decisions. The battlespace awareness controller must dynamically manage sensing, transmission, and processing resources to minimize mission risk (or maximize "awareness" modulated by mission concerns). It should also be designed to minimize sensitivity to disturbances (intentional or environmental).

Conversely, the counter-C5ISRT strategy must include modulation of the adversary's information gap by introducing noise, decreasing available information, and decreasing the ratio of relevant to redundant information. For example (Figure 5), attacks can be made across Red's ISRT system to disrupt its sensing, communications, processing, and decision-making, resulting in a COP that either does not represent reality or represents a perception advantageous to Blue. Modulating, rather than necessarily maximizing, the adversary's information gap allows us to control the adversary's ability to detect and respond to the disruptions. In other words, even if maximum disruption of an adversary is achievable, it is most often more advantageous to tailor actions for only accomplishing desired effects. We refer to this approach as *battlespace awareness anti-control*. Research is needed to understand how to apply battlespace awareness control and anti-control and the impact of different techniques on performance and robustness.

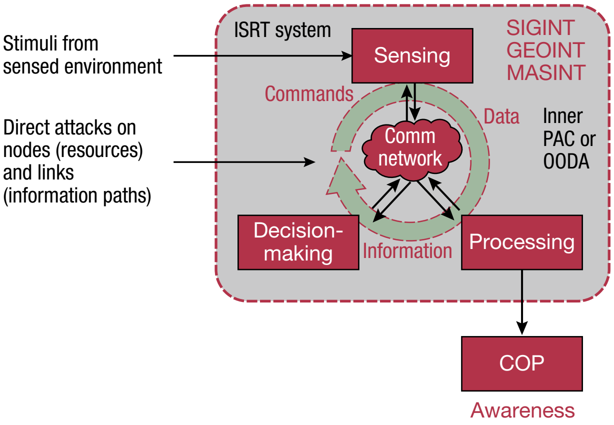

Figure 5. C5ISRT attack mechanisms. Attacks can be made across Red's ISRT system to disrupt its sensing, communications, processing, and decision-making, resulting in a COP that either does not represent reality or represents a perception advantageous to Blue. GEOINT, geospatial intelligence; MASINT, measurement and signature intelligence; SIGINT, signals intelligence.

PROGRESS

APL is making significant progress toward the goals described in this article. The series of IRAD efforts mentioned earlier attracted government funding, with APL playing prominent roles. In one program, algorithms are being developed to coordinate and orchestrate countermeasures. This work relies on models, being developed through APL's strong relationship with the US Intelligence Community, that parameterize and characterize a comprehensive set of adversary threats and own-force signatures.[5] Additional programs are developing individual, one-on-one countermeasures for disrupting an adversary's ability to sense US force activity. These countermeasures have demonstrated initial and positive testing in live exercise environments. Along the way, APL's work on C5ISRT dominance captured interest from deployed units, resulting in a program where APL scientists deployed to warfighter locations to develop algorithm-based systems from the perspective of the warfighters who will use them.

Most recently, attention has been on joint deception strategies with goals beyond minimizing exposure to adversary ISRT. Here we wish to plan for intentional deception and detect the same from our opponents while determining their real intent. To be believable, deception must account for the behavior and ideology of our adversaries. Effective deception, upon discovery, causes an adversary to lose confidence in their perception of reality and hesitate in the face of subsequent truth.

Current IRAD efforts focusing on controlling Red perception (see the article by Ward et al., in this issue) and continuous universal targeting are investigating techniques for deception and counter-deception. For example, Jonathan DeSena's IRAD project on skeptical fusion and sensemaking showed that a fusion approach that is skeptical of the input data, and therefore incorporating the possibility of deception, can recognize an adversary's attempt to manipulate the Blue tactical picture. However, this work did not develop a method to compensate for the recognized deception. DeSena built on these ideas in his subsequent IRAD project on active counter-deception, which showed that coordinated ISR retasking and active probing can result in eliciting targeted observables that enable more efficient evaluation and identification of deception hypotheses and can mitigate deception with some robustness to modeling errors. As another example, Zachary Akilan's IRAD project titled Training Reinforcement Learning with the Objective of Learning to Lie (TROLL) investigated the use of reinforcement learning to construct representative sets of deception strategies and supervised learning to recognize them.

Techniques derived from or inspired by these and other IRAD efforts would ultimately be combined into a comprehensive and cohesive warfighting capability, which we call Continuous Universal Targeting with Impunity (CUTI). As shown in Figure 6, CUTI allows Blue to control perception of the battlespace, such that Blue has targeting-quality awareness of every consequential Red asset at all times (continuous universal targeting), whereas Red lacks target-quality awareness of any consequential Blue entity at any time (operating with impunity). To achieve CUTI, we must achieve a capability to systematically (with purpose), consistently (across domains), and synchronously (in plausible sequence and time) cause Red to perceive the battlespace to the strategic, operational, and tactical benefit of Blue.

Figure 6 shows four intertwined processes or loops within the CUTI concept. Blue forces attempt to maintain a comprehensive view of the battlespace, despite adversary denial and deception and despite error induced by partial observability and imperfect sensors and models (upper right loop). Blue must also be aware of and prevail against Red attempts to directly attack Blue cognition or sense-making through, for example, cyberattack (lower right loop). A significant advancement envisioned in CUTI is to use Blue's awareness and understanding of the battlespace to create a calculated fiction that Blue desires to impose on Red. To impose this believable (to Red) fiction, Blue must plan and execute a series of stimuli that feed into the battlespace under the assumption they will be observed by Red (upper left loop). Although the stimuli and desired responses are specifically tailored to influence Red's understanding of the battlespace, they could have the additional benefit that it may drive Red responses that, when observed by Blue, not only inform Blue of Red's understanding but also reduce the ambiguity and uncertainty in Blue's view of the battlespace. Blue stimuli may also be inserted to directly influence the ability of the Red side to perceive the battlespace (lower left loop). Clearly this is a completely symmetric proposition; Blue must assume that Red will attempt to influence and control Blue's view of the battlespace—and so Blue cognition must account for Red's attempts to slant Blue's view toward an advantageous outcome for Red.

CONCLUSIONS

This article describes a vision for research and development in battlespace awareness control and anticontrol leading to a realization of the CUTI concept and C5ISRT dominance. It describes a new control and analytical framework to understand the interactions between competing (Blue versus Red) highly automated and distributed C5ISRT systems and to predict and influence C5ISRT system response to a variety of attack mechanisms, both individually and collaboratively. This framework views a C5ISRT system as a CDS with a PAC that continually redirects its resources to optimize the situational awareness available to support tactical decision-making. From this viewpoint, attack

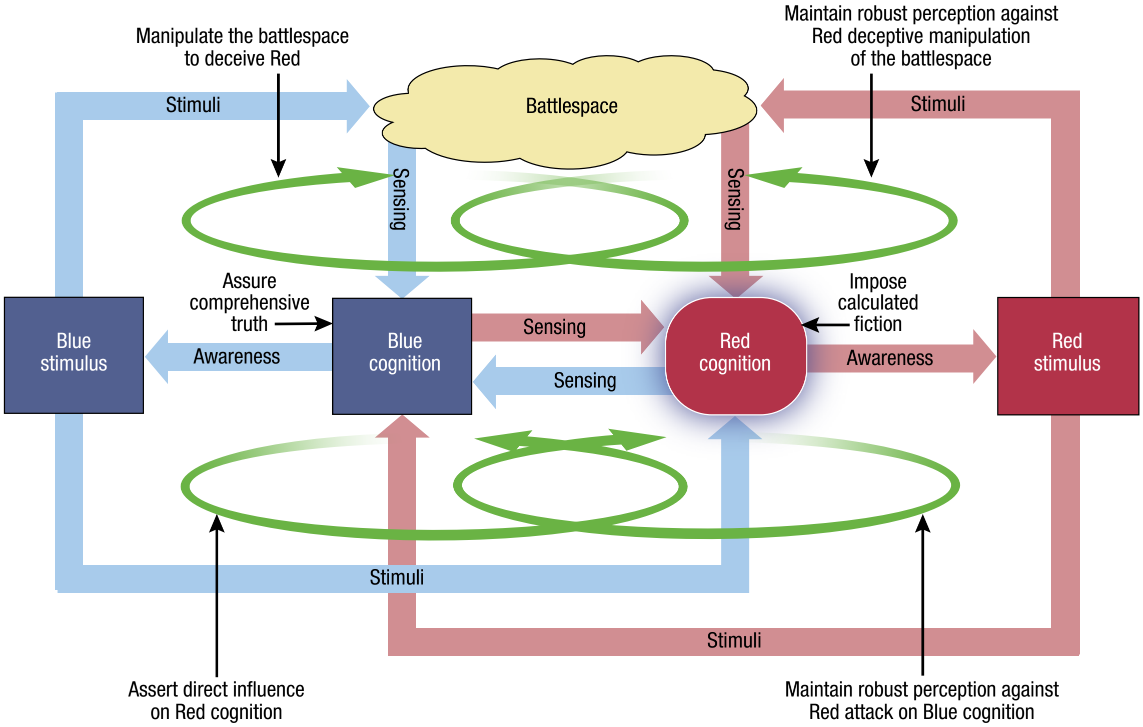
Manipulate the battlespace to deceive Red
Maintain robust perception against Red deceptive manipulation of the battlespace
Stimuli
Battlespace
Stimuli
Sensing
Sensing
Assure comprehensive truth
Impose calculated fiction
Blue stimulus
Awareness
Blue cognition
Sensing
Sensing
Red cognition
Awareness
Red stimulus
Stimuli
Stimuli
Assert direct influence on Red cognition
Maintain robust perception against Red attack on Blue cognition

Figure 6. The CUTI concept. Shown are the four intertwined processes, or loops, within the concept. The right side reflects Blue forces' attempt to maintain a comprehensive view of the battlespace and remain aware of and prevail against Red attempts to directly attack Blue cognition or sense-making. The left side reflects Blue's attempts to control Red's perception.

mechanisms are applied to create, modulate, and exploit information gaps that achieve a desired effect on the adversary's decision process. Conversely, our C5ISRT system can dynamically adapt its information flow to resist attempts at disruption and deception.

Success of future air dominance and force projection against adversaries with anti-access, area-denial capabilities will depend on the relative strengths of the opposing C5ISRT capabilities. The 2030 vision for C5ISRT dominance is to attack adversary C5ISRT systems in a coordinated manner to achieve precision system-level effects. The effects of invasive and noninvasive attacks and the deception options for disrupting the adversary's C5ISRT must be understood and applied in concert. This enables combined effectiveness assessments of kinetic, electromagnetic, cyber, materiel, and maneuver TTP, and supports end-to-end development and quantitative assessment of C5ISRT and counter-C5ISRT capabilities and TTP.

Although US forces are making progress toward these goals, adversary forces continue to rapidly evolve their capabilities. Increased and sustained US investment in C5ISRT dominance is imperative to stay ahead of adversary advancements and ensure our ability to globally project military power. Indeed, these investments must be coordinated with complementary investments in continuous universal targeting and controlling Red perception (see the article by Ward et al., in this issue) so that the vision of CUTI is fully realized. Such a grand challenge can best be executed through a government-led initiative coordinating the work of academia and industry to develop and execute a research and development campaign, and the transition of promising technology into operational capabilities that ensure the nation's security in the highly contested environments that have so recently reemerged and that will characterize the global security environment for years to come.

REFERENCES

[1] J. R. Boyd, "Destruction and creation," US Army Command and General Staff College, Fort Leavenworth, KS, Sep. 3, 1976.

[2] S. Haykin, "Cognitive dynamic systems," *Proc. IEEE*, vol. 94, no. 11, pp. 1910–1911, Nov. 2006, https://doi.org/10.1109/JPROC.2006.886014.y.

[3] M. Endsley, "Toward a theory of situational awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995, https://doi.org/10.1518/001872095779049543.

[4] S. Haykin, M. Fatemi, P. Setoodeh, and Y. Xue, "Cognitive control," *Proc. IEEE*, vol. 100, no. 12, pp. 3156–3169, Dec. 2012, https://doi.org/10.1109/JPROC.2012.2215773.

[5] W. Menner et al., "Counter-ISR decision aids in anti-access area denial environments," in *Military Sensing Symp., Nat. Symp. on Sensors and Data Fusion*, Oct. 25, 2018.

Andrew J. Newman, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Andrew J. Newman is supervisor of the ISRT and Sensors Group in APL's Force Projection Sector. He has a BS in systems engineering from the University of Pennsylvania, an MS in electrical engineering from the University of Virginia, and a PhD in electrical and computer engineering from the University of Maryland. He has extensive experience in analysis, planning, control, and data fusion for military command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems. Since joining APL in 2003, he has led or been a major contributor to a wide variety of projects in ISR systems, sensor and data fusion, target tracking, and dynamic ISR resource management applied to missions in the ground, maritime, air, and space domains. Andrew won the APL Hart Prize in 2006 and 2012 for excellence in independent research and development in the development category. His email is andrew.newman@jhuapl.edu.

William A. Menner, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

William A. Menner is a chief engineer in the ISRT and Sensors Group in APL's Force Projection Sector. He has a BS in mathematics from Michigan Technological University and an MS in applied mathematics from Rensselaer Polytechnic Institute. Will led a modeling and simulation team to create a capability for exploring the effectiveness of command, control, communications, computers, intelligence, surveillance, reconnaissance, and targeting (C4ISRT) and countermeasures. His Intelligence Community outreach on C4ISRT issues resulted in APL's position on working groups, a key program, and strong relationships with key elements of the IC. For APL's innovation initiative known as Agile Central, he leads the Education Team, which produces Agile workshops for APL staff. He also successfully led technical efforts in the Naval Strike Warfare Planning Center and Cooperative Engagement Capability programs. His email is will.menner@jhuapl.edu.

Glenn E. Mitzel, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Glenn E. Mitzel is a chief scientist in the Precision Strike Mission Area in APL's Force Projection Sector. He has a BE, an MS, and a PhD in electrical engineering, all from Johns Hopkins University. Glenn is a recognized authority in military surveillance, targeting, and upstream data fusion and its applications, and he has strong expertise in optimal estimation and control, remote sensing, and rapid prototyping. In addition, he is a demonstrated leader of large multidisciplinary technical teams attacking and solving complex technical problems in these fields. His email is glenn.mitzel@jhuapl.edu.

Mark D. LoPresto, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Mark D. LoPresto is a principal engineer in the ISRT and Sensors Group in APL's Force Projection Sector. He has BS in systems engineering from the US Naval Academy and an MS in electrical engineering from Johns Hopkins University, and is pursuing a PhD in electrical engineering from the University of Maryland, Baltimore County. He served in the US Navy as a surface warfare officer and has over 30 years of experience in command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR); systems engineering; and program management, and he has extensive background in all elements of the offensive kill chain. His email is mark.lopresto@jhuapl.edu.