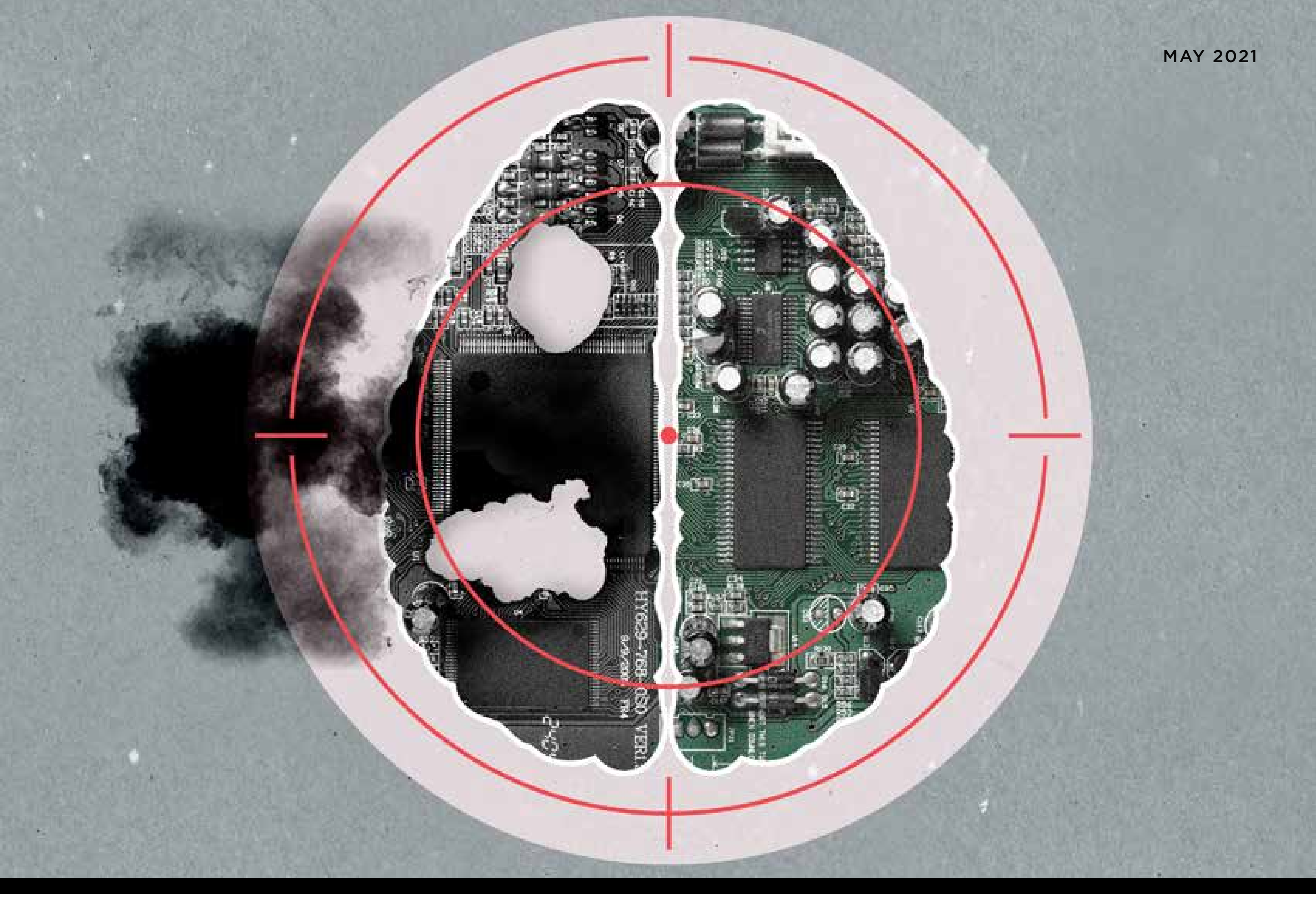
MAY 2021



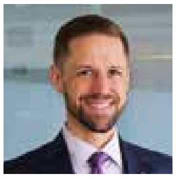
More than Half the Battle

Information and Command in a New American Way of War

Chris Dougherty

CNAS

About the Author



Chris Dougherty is a Senior Fellow in the Defense Program at the Center for a New American Security (CNAS). His research areas include defense strategy, strategic assessments, force planning, and wargaming.

Prior to joining CNAS, Mr. Dougherty served as Senior Advisor to the Deputy Assistant Secretary of Defense for Strategy and Force Development at the Department of Defense (DoD). During this time, he led a handful of major initiatives including the development and writing of major sections of the 2018 *National Defense Strategy.*

About the Defense Program

Over the past 10 years, CNAS has defined the future of U.S. defense strategy. Building on this legacy, the CNAS Defense team continues to develop high-level concepts and concrete recommendations to ensure U.S. military preeminence into the future and to reverse the erosion of U.S. military advantages vis-a-vis China, and to a lesser extent Russia. Specific areas of study include concentrating on great-power competition, developing a force structure and innovative operational concepts adapted for this more challenging era, and making hard choices to effect necessary change.

Acknowledgments

I'd like to thank Will Mackenzie, Ed McGrady, and Becca Wasser for being my partners in wargaming, providing support to this project, and helping to review this paper. I'd like to thank Molly Parrish for her tireless support of the defense program. I'd like to thank the CNAS interns who have helped put on our wargames and served as note-takers. In particular, I'd like to thank Jessie Dietz and Ripley Hunter for their research assistance. I'd like to thank Alec Barker, Peter Revay, and Group W for their modeling and simulation support. I'd like to thank Loren Schulman, Maura McCarthy, and Usha Sahay for providing much-needed feedback on the structure of the paper. I'd like to thank the following folks for reviewing the paper and providing their thoughts, feedback, and edits: Elbridge Colby, Jon Solomon, Frank Hoffman, COL Buzz Phillips, Col Brian "Brutus" Stahl, Maj Kevin "Klinger" Mendel, Jennifer McArdle, Tim Walton, Andrew Metrick, Jacob Cohn, Will Schlickenmaier, CAPT Greg Malandrino, Adam Comfort, Scott Kendricks, Iskander Rehman, CAPT Mike Martinez, MAJ Sarah P. White, Tom Shugart, and Shawn Steene. I'd also like to thank many of our wargaming "regulars" without whom this project would not have been possible: Eric Coulter, Derreck Holian, Mark Goolsbay, Col Dan Skuce, COL Sarah Albrycht, Scott Boston, Eric Heginbotham, Cristina Garafola, Mark Seip, Greg Grant, Chris Rielage, Nina Kollars, Caitlyn Leong, Col Steven Sutey, Col Kaveri Crum, Col Paul Calhoun, Shane Bilsborough, Maj Jason Buell, Ryan Boone, Michael Kofman, et al. My sincerest apologies if I left anyone off of this list—the next post-wargame round is on me. Finally, I'd like to thank Jennie Matuschak for helping me get this over the line, and most of all Susanna Blume for her patience, direction, and leadership.

Dedication

To Bernie, Susan, and Mary Jo: You always believed in me and you were always there for me. I miss you all dearly.

TABLE OF CONTENTS

Executive Summary

China's rise and Russia's reemergence as serious military competitors to the United States during the last decade have changed the character of warfare as profoundly as the U.S. victory in the Gulf War. Precision-guided munitions and other advanced weapons systems likely will play an important role in this new era of warfare. However, to confer an advantage, these systems will require the ability to gather, transmit, process, understand, and act on information faster and with greater accuracy than an opponent. Advantage in peace and victory in war will demand a mixture of technical information systems and cognitive functions such as command decision-making. Every effort should be expended to attain an advantage by degrading adversary systems and protecting friendly systems while disrupting the enemy's cognitive command processes and sustaining one's own. These imperatives create a "techno-cognitive confrontation" that is continual and widespread, crossing delineations between peace and war. Within this context, great-power warfare would be far more chaotic, lethal, and contested than the conflicts of the post–Cold War period.

China and Russia have developed distinct but similar theories of victory in this new type of warfare focused on prevailing in the techno-cognitive confrontation. While their military strategies and concepts are complex and diverse, they share four critical attributes. First, they aim to keep conflicts local, limited, and therefore relatively manageable, while obviating U.S. global military preponderance. Second, they use "peacetime" information operations to (ideally) achieve their objectives without fighting or to create favorable conditions if conflict occurs. Third, they attack critical systems in space, cyberspace, and the electromagnetic spectrum, as well as physical network nodes, to achieve information degradation and command disruption, or ID/CD, against adversary systems and the cognitive processes they enable.[1] Fourth, they increasingly are centralizing, automating, and "intelligentizing" their command and control to enable rapid, coordinated actions across multiple domains in the critical opening days of a potential conflict.

The Department of Defense 's (DoD) belated response to emerging Chinese and Russian concepts has been overly technological and fixated on regaining the kind of information dominance that U.S. armed forces enjoyed from 1990 until very recently. The DoD certainly needs to develop new systems to replace its current information and command architecture, much of which dates back to the 1970s and '80s. Still, a myopic focus on technology misses the critical cognitive and organizational aspects of the confrontation with China and Russia. The obsession with regaining information dominance is perhaps even more deleterious. Barring some wholly unforeseen event, the DoD is unlikely to regain its post–Cold War techno-cognitive dominance against China or Russia. They are too capable and too competent to allow this to happen, and the chaotic character of modern warfare vitiates against the kind of lopsided information advantage U.S. forces enjoyed against Iraq in the Gulf War.

The DoD needs to embrace, rather than fight against, the changes in the character of warfare and learn to thrive within its chaos in ways that China and Russia may be unable to match given their highly centralized and directive command-and-control structures. Instead of striving for information dominance, the DoD should seek "degradation dominance" as a way of achieving an advantage in the techno-cognitive confrontation with China and Russia. This notion attacks their theory of victory by demonstrating the ability to operate *effectively enough* with degraded systems in contested environments, while imposing proportional degradation on Chinese and Russian systems, thereby causing them to lose confidence in their ability to gain an insuperable advantage in the techno-cognitive confrontation.

Achieving degradation dominance against China and Russia comprises four mutually reinforcing lines of effort:

1. Force them into dilemmas about expanding or escalating a conflict by exploiting tensions between their limited-war strategies and their operational imperative to attack information and command systems aggressively at the outset of a conflict by:
   - Focusing concept and capability development on limiting the effectiveness of reversible and non-kinetic attacks, particularly in space;
   - Adopting a more dispersed posture for information and command systems;
   - Working with allies and partners to increase multilateral cooperation in key information and command mission areas that would be high priority targets for China and Russia; and
   - Forcing China or Russia into dilemmas about attacking the U.S. homeland.
2. Level the playing field in the "peacetime" information environment by:
   - Gaining proper authorities for information operations in key theaters and deconflicting with other government agencies;

- Training, educating, and exercising the joint force to deal with Chinese and Russian information confrontation;
- Serving as a "systems integrator" to leverage allied and partner expertise with Chinese and Russian information operations;
- Aligning information operations with military operations to increase trust with allies, partners, and key audiences abroad; and
- Avoiding civilian casualties to stymie Chinese and Russian information operations aimed at degrading coalition cohesion.

3. Achieve degradation dominance in the techno-cognitive confrontation in space, cyberspace, and the electromagnetic spectrum by:
   - Enabling people and building trust across command echelons and organizations, as well as with critical systems;
   - Adopting policies and demonstrating capabilities to proportionally attack sensitive Chinese and Russian information and command systems;
   - Training to fight with degraded information and disrupted command;
   - Developing the ability to operate with "loose" decentralized peer-to-peer command, control, and communications structures in degraded, disrupted, or contested environments;
   - Developing and deploying a "Rosetta Stone" communications architecture that enables resilient multi-path networks through translation, rather than interoperability;
   - Employing mission command and other forms of decentralized and delegated command philosophies, particularly when command systems are disrupted;
   - Accepting "good enough" targeting against low-value targets in contested environments;
   - Adopting rapid targeting processes for high-tempo, degraded operations in contested environments;
   - Leveraging artificial intelligence, sophisticated automation, and bounded autonomy to reduce cognitive loads and accelerate decision-making; and
   - Using military deception to foil adversary planning and targeting, particularly automated, artificially intelligent, or other algorithmically enhanced systems.

4. Organize and train for degraded and disrupted multi-domain operations:
   - Put the "combat" back in the Geographic Combatant Commands by refocusing them on warfighting vice military diplomacy;
   - Create standing, multi-domain units across multiple echelons of command down to the tactical level;
   - Increase regular joint and multi-domain training and Combatant Commanders Exercise Engagement and Training Transformation (CE2T2) funds; and
   - Use live, virtual, and synthetic training to train realistically in all domains.

Enacting these recommendations would mark a major change in the DoD's mindset about the future of warfare and the role of information and command in competition and conflict. Letting go of notions of dominance to strive instead for operating effectively enough while degraded is a difficult, but needed, paradigm shift given the challenges posed by China and Russia and the changing character of modern warfare. The alternative likely would be a ruinously expensive and fruitless search for symmetrical "overmatch."

Though daunting, the DoD has successfully embarked on similar paradigm-shifting reform efforts in the past. The most relevant was the post-Vietnam initiative to address the persistent weakness of U.S. night-fighting capabilities. By becoming, arguably, the world's most effective night-fighting force, the DoD presented adversaries with a vexing dilemma: fight during the day and face the wrath of U.S. airpower and firepower, or fight at night at perhaps an even worse disadvantage.

Achieving degradation dominance through these lines of effort would pose a similar dilemma to Chinese and Russian forces in the event of a crisis or conflict. They would have to consider attacking U.S. information and command capabilities, albeit with diminishing confidence that such attacks would render U.S. forces incapable of responding. At the same time, their aggression would risk escalating or expanding a conflict and open up their own information and command systems to proportional U.S. responses. Alternatively, they could opt not to attack, or limit their attacks to reduce the risk of escalation, but these approaches would leave U.S. information and command systems relatively unscathed. Either option would leave them with a less than satisfactory outcome, and maintaining that pessimistic assessment is key to deterring aggression; defending U.S. allies, partners, and vital interests; and upholding a free and open international order in East Asia and eastern Europe.

Introduction

After roughly 40 years of advantage, if not outright dominance, in the ability to use information to gain greater situational awareness and command forces more effectively than its adversaries, the DoD is facing competitors that have developed the means and methods to level this playing field or shift it to their advantage. The emergence of China and reemergence of Russia as advanced military competitors—and particularly their development of precision-strike weapons and advanced information systems—have changed the character of warfare. Some, such as the late Andrew Marshall, Barry Watts, and Andrew Krepinevich, have referred to this new era of warfare as a "mature precision-strike regime," in which multiple advanced militaries possess the requisite sensors, networks, and precision-guided munitions to conduct precise long-range attacks at scale.[2] The character of modern warfare incorporates this regime, but also includes other related aspects such as the increasing salience of space and cyberspace as combat domains and the growing importance of sub-conflict competition or "confrontation" in the information environment.

The end result of these developments is that warfare between modern great powers is likely to be fast-paced, chaotic, highly lethal, and contested at long ranges in every environment from under the sea to the far reaches of geosynchronous earth orbit (GEO).[3] Large-scale industrial platforms and processes will remain relevant, but inter-state military competition and conflict increasingly will center around "techno-cognitive confrontation" between opposing information systems and cognitive command processes.

To prevail in this new kind of warfare, China and Russia have developed similar, albeit distinct, theories of victory that align their concepts, force structure, operations, and command philosophies. They are pursuing concepts and capabilities to degrade the ability of U.S., allied, and partner forces to maintain situational awareness, trust their information, and communicate, and to disrupt their ability to exercise command and control. This shared "information degradation/command disruption" or ID/CD approach, is designed to turn longstanding U.S. advantages in information and command into critical vulnerabilities.

To execute these concepts, they have developed their own ways of using information and commanding their forces. They increasingly have centralized, automated, and routinized their information and command processes to exert greater direct control and better synchronize their operations. These methods are designed to operate effectively across "peacetime" geopolitical confrontation and military conflicts. More worryingly, they are investing in new technologies like artificial intelligence to leapfrog remaining U.S. technical and cognitive advantages.

The DoD's response to this challenge has been slow and hobbled by different understandings of the problem and therefore divergent visions as to the solution. While the DoD belatedly has begun to show progress in areas such as the Joint All-Domain Command and Control (JADC2) concept, these solutions are technical, when many of the challenges China and Russia pose are cognitive, psychological, and organizational.[4] Moreover, there is a pernicious thread running through many DoD initiatives regarding information and command and control. Namely that smart investments in the right system, "system-of-systems," or "architecture" can enable the DoD to return to the level of information and command dominance or "overmatch" that U.S. armed forces have enjoyed over the last several decades.[5]

> **Warfare between modern great powers is likely to be fast-paced, chaotic, highly lethal, and contested at long ranges in every environment from under the sea to the far reaches of geosynchronous earth orbit.**

While investments in information and command-and-control systems are critical and should remain one of the DoD's top modernization priorities, the desire for dominance underestimates the scale of the challenges posed by China and Russia, and misunderstands the character of modern great-power warfare. For the foreseeable future, there is no going back to the level of information and command superiority to which the U.S. joint force has become accustomed. China and Russia are simply too sophisticated and too capable for that to be a feasible objective in the scenarios that most worry U.S. defense planners. Furthermore, the character of future conflict with China or Russia would vitiate the relative advantages in situational awareness and rapid decision-making that have been the hallmark of the American way of war since at least 1990.

To explore the challenges of using information and commanding forces in modern great-power conflict, the Defense Team at CNAS, during the last 18 months, conducted more than 10 wargames set in the 2030 time frame. Specifically, these games explored future interactions between U.S., Chinese, and Russian information and command concepts in competition and conflict. Three observations from these games were salient across a variety of scenarios and assumptions.

First, conflict between great powers using modern weaponry is shockingly fast and disturbingly destructive. For example, in more than eight wargames set in the Indo-Pacific theater, covering campaigns lasting from several days to several weeks, typical attrition exceeded the estimated combined U.S. and Japanese ship and aircraft losses from the Battle of the Coral Sea and the Battle of Midway—two of the costliest air and naval battles in World War II. The combat is also disorientingly chaotic, regardless of whether information and command systems worked (in which case, long-range precision fires resulted in catastrophic attrition and destruction) or not (in which case, both sides scrambled to understand what was happening, make decisions, and communicate these decisions across their forces).

Second, the side that could rapidly impose chaos on its opponent while maintaining sufficient understanding and order to command its own forces gained an enormous advantage. This advantage accrued to the Chinese and Russian teams in nearly every scenario in which U.S. teams used current concepts. Most Chinese and Russian red teams had a relatively consistent "script" of attacks that they would use to systematically conduct ID/CD against U.S. forces. This script rapidly gave them an advantage in key aspects of the techno-cognitive confrontation, such as the ability to target ships at long range and coordinate attacks from multiple domains.

Third, once gained (or lost), this advantage had cascading effects that put the weaker side—usually the U.S. team—into untenable dilemmas or, worse, seemingly unrecoverable positions. These games suggested that, without urgent changes to how the DoD is conceptualizing and engaging in techno-cognitive confrontation, U.S. forces face a real risk of losing their situational awareness, capacity to make decisions, ability to communicate reliably, and the initiative in plausible conflict scenarios. Once the fight for information and command is lost, U.S. forces may not be able to recover, and military defeat becomes likely.

Despite these dispiriting outcomes, the lessons learned from these games and from computer modeling and simulation suggest that the DoD has a feasible path toward an advantage in the techno-cognitive confrontation, provided it lets go of the idea of regaining information dominance and possessing an unassailable advantage in the ability to command forces. Rather than bringing order to the chaos of modern conflict, the DoD needs to accept that chaos is endemic and learn to operate within it while forcing China and Russia to do the same in ways that they may be structurally unable or disinclined to do. Instead of striving for information dominance or "overmatch," the DoD and the armed services should focus on operating with degraded information and disrupted command systems while demonstrating the ability to proportionally degrade adversary systems, to achieve what this paper calls "degradation dominance." The fundamental idea is to demonstrate the ability to operate effectively enough with degraded systems in contested environments—while imposing sufficient degradation on Chinese and Russian systems—that they lose confidence in their ability to gain a decisive advantage in this confrontation through rapid or preemptive attacks.

The first aspect of degradation dominance thwarts revisionist, antagonistic, and aggressive Chinese and Russian policies by undermining and attacking Chinese and Russian limited war and "active defense" strategies while making U.S. and coalition responses more credible. Chinese and Russian approaches to fighting U.S.-led coalitions have inherent tensions between their strategic aim of limiting and controlling conflicts and the operational imperative toward aggressively seizing the initiative inherent in any effort to deter or defeat a U.S.-led coalition response launched from a global posture. Attacking information and command systems at the outset of a conflict—or even preemptively—is at the core of Chinese and Russian military approach to deterring, delaying, or defeating U.S. military operations. At the same time, China and Russia would prefer to limit and tailor these attacks to avoid provoking a strong counter-coalition or a broader global war with all the potential risks it would entail. U.S. information and command systems therefore should be designed, postured, and operated in such a way that attacking them risks escalating or expanding a conflict while simultaneously making attacks on Chinese and Russian systems more credible. This puts China and Russia into a dilemma: act aggressively and risk escalation, expansion, and more aggressive counterattacks on their systems, or restrain their actions and incur operational risks by allowing key U.S. information and command systems to remain functional.

The second aspect is to level or advantageously tilt the information playing field in key regions by acting as an enabler and "systems integrator" for allied and partner efforts to push back on Chinese and Russian information warfare. Given the breadth of Chinese and Russian information operations, the DoD should focus its efforts on maintaining alliance and coalition cohesion, improving local situational awareness, and gaining a public opinion advantage versus China and Russia in key locations. This persistent competition—which China and Russia call confrontation or struggle—is foundational. Unless the United States pushes back on Chinese and Russian operations, it could lose the techno-cognitive confrontation without a fight, or it could begin any conflict in such a deficit that victory becomes extremely unlikely.

The third aspect is to achieve degradation dominance in the techno-cognitive confrontation centered on space, cyberspace, and the electromagnetic spectrum. Gaining an advantage in these domains, in large part by preemptively or rapidly deceiving, exploiting, degrading, or destroying adversary systems and the cognitive processes that rely on them, is central to Chinese and Russian approaches to confronting or fighting the United States. Demonstrating the ability to operate *effectively enough* in the face of their efforts to contest these domains and degrade U.S. information and command systems, coupled with a credible ability to deceive, exploit, and degrade their information and command systems, could profoundly impact Chinese and Russian calculations of the correlation of forces in key theaters. The key to this is developing more flexible and resilient “loose” information and command structures, in contrast to the rigid, stovepiped, hierarchical structures that predominate today.

The fourth aspect of this concept is to change how the DoD and the armed services organize and train forces for combat to operate more flexibly under ID/CD attacks. If the DoD believes that increasing joint integration or multi-domain operations are critical to success, it must change organizational structures to enable, rather than impede this shift by creating standing forces—vice ad hoc task forces—in key theaters, built around critical capabilities and sized on spans of control that are feasible using degraded systems in contested environments. Unit and personnel rotation policies should emphasize familiarity and the shared understanding that is vital in chaotic and contested combat operations when communications systems break down, rather than flexibility for personnel managers. Training should continually emphasize joint or multi-domain operations in contested environments using degraded systems, leveraging live, virtual, and constructive or synthetic training where needed. Given the reality that U.S. armed forces will almost always fight as part of a multinational coalition, these reforms cannot be limited to U.S. forces and operations, but must incorporate key allies and partners from the outset.

The idea of eschewing information dominance and accepting degradation represents a massive shift for the DoD and the armed services, but it is not without precedent. Following Vietnam, the DoD made a conscious decision that, after decades of poor performance in nighttime operations, it would invest heavily in night-fighting capabilities, such as night vision, along with intensive training in order to “own the night.” This decision brought about a profound shift in U.S. and adversary military operations. After decades in which opponents sought to negate U.S. advantages in firepower by fighting at night, they now faced an unpleasant dilemma: fight during the day and expose themselves to U.S. firepower, or fight at night at an arguably greater disadvantage against U.S. night-fighting abilities.

If the United States and its key allies and partners can demonstrate the ability to operate effectively with degraded systems and to degrade adversary systems, they can pose a similar dilemma to China and Russia. They can choose to attack information and command systems and risk initiating a larger, more aggressive conflict while opening up their own systems to attack and creating a degraded and contested information environment in which U.S., allied, and partner forces are comfortable operating. Or they could exercise restraint and allow U.S., allied, and partner forces to leverage their full complement of information and command systems. Either choice would leave them with a less than satisfactory outcome and therefore a pessimistic assessment of their ability to rapidly establish an advantageous correlation of forces in the critical opening moments of a conflict. Maintaining that pessimistic assessment through degradation dominance is a key component to deterring aggression; defending U.S. allies, partners, and vital interests; and upholding a free and open international order in East Asia and eastern Europe.

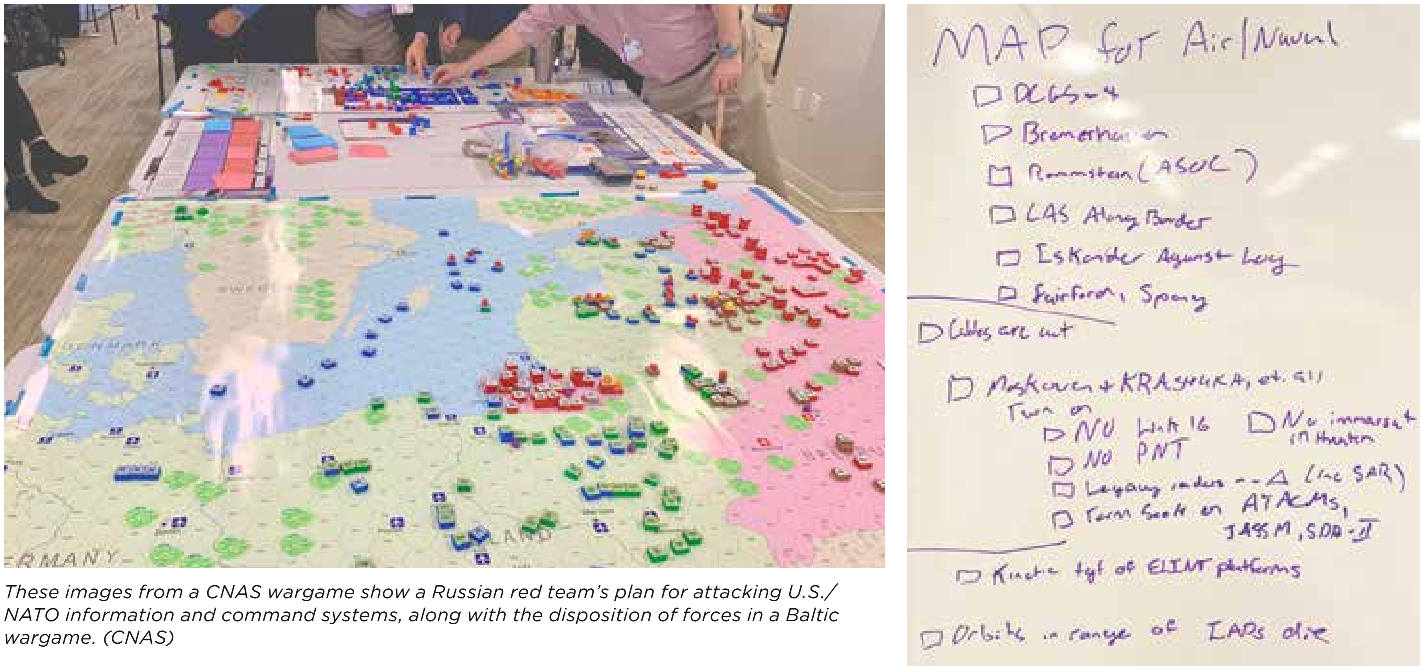
The body of this paper is organized into six parts. The first section explains the methodology used to research the topic, and the following section summarizes how that methodology led to a more holistic focus on “information and command,” vice the more typical focus on command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The second section briefly describes Chinese and Russian military strategies and concepts for confronting and combating the United States, and presents a short fictional vignette explaining how Russian concepts might play out in a scenario involving heightened military confrontation during a crisis in the Baltic region. The paper then lays out the full joint concept for achieving degradation dominance and makes some additional domain- and service-specific recommendations. Next, the paper revisits the fictional Baltic vignette to demonstrate the concept in action before concluding.

This project draws on more than a year's worth of unclassified research on conflict between the United States and China or Russia. It is informed by more than 10 adjudicated wargames covering a variety of conflict scenarios, although mostly focused on conflict over Taiwan in Asia and the Baltic region in Europe. These games used a variety of methods to represent the challenges of information and command. Moving to a virtual format because of COVID-19 allowed the research team to discretely control the information and communication capabilities of the teams.

The wargames fed directly into computer modeling and simulation of critical aspects of a Russia-Baltic scenario. In particular, the analysis focused on the ability of joint or "multi-domain" forces to cooperatively find and target adversary ground forces in a highly contested environment with degraded command, control, and communications capabilities. Conducting thousands of "runs" of an agent-based, stochastic model allowed the research team to add to the wargaming in two key ways. First, it examined the insights and concepts from the game to determine whether key outcomes were outliers, or sufficiently robust to merit further consideration by the DoD. Second, it allowed the research team to examine alternative concepts, control models, and communications architectures that could not be explored adequately during a relatively limited number of games.

This project began as an attempt to develop new concepts in C4ISR—i.e., command, control, communications, computers, intelligence, surveillance, and reconnaissance—as part of a broader effort to develop a new American way of war for 21st-century competition and conflict with China and Russia. The focus on C4ISR derived in part from the 2018 *National Defense Strategy* (NDS), which emphasizes the need to build a more resilient C4ISR architecture.[6] At their core, however, both the NDS and this project are dealing with the same issue, which will persist into the next *National Defense Strategy* and beyond: The current American way of war relies on a suite of C4ISR systems and practices that are obsolescing rapidly in the face of technological change and, more importantly, concerted Chinese and Russian efforts to exploit, disrupt, degrade, deny, or destroy them.

The wargames and modeling that informed this project made clear that changes to C4ISR systems would be necessary, but insufficient to maintain U.S. military advantages versus China and Russia in key theaters. In addition to making U.S. C4ISR systems more resilient and making greater investments in electronic warfare, cyber, and deception to better counter adversaries' command-and-information systems, the DoD and the armed services must change the way they think about information and command; how they operate; and how they train, organize, and equip U.S. forces. Put another way, when it comes to developing more resilient joint information and command functions, the cognitive, conceptual, and organizational challenges facing the DoD



MAP for Air/Naval

□ DCGS-A

□ Bremerhaven

□ Ramstein (ASOC)

□ CAS Along Border

□ Iskander Against Log

□ Fairford, Spang

□ Cables are cut

□ Moskovia + KRASUKHA, et. al
Turn on

□ NO Link 16 □ No immersant in theater

□ NO PNT

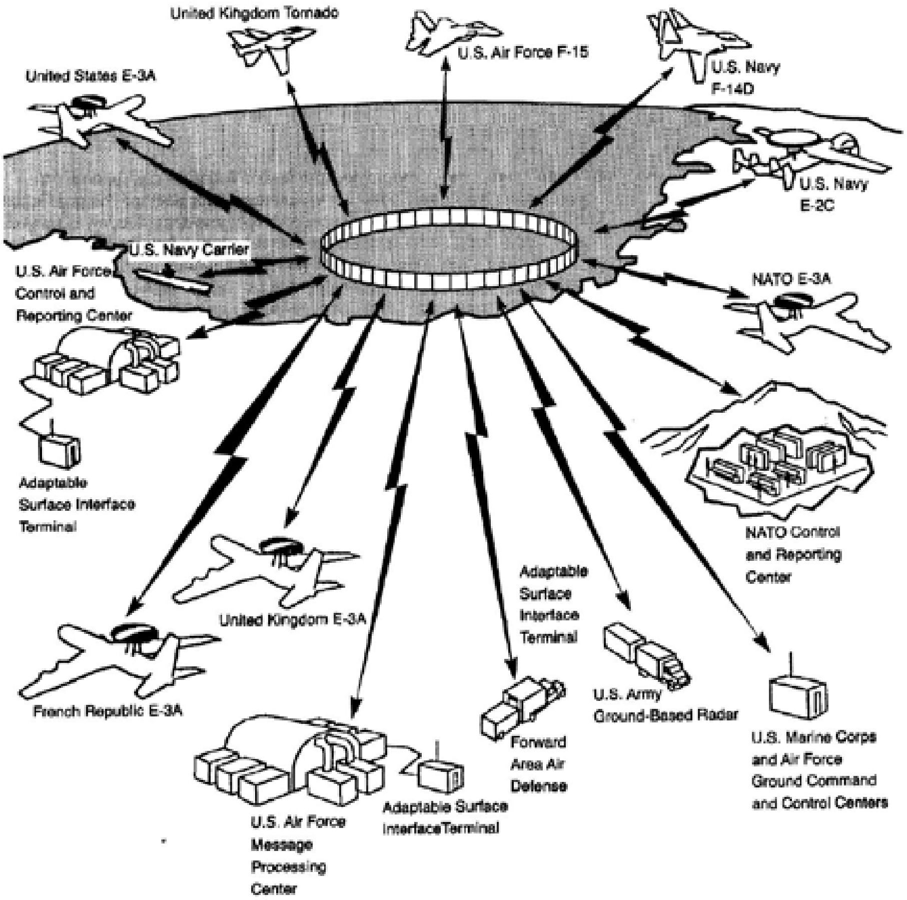
□ Legacy radars -- Δ (inc SAR)

□ Form Seek on ATACMS, JASSM, SDB-II

□ Kinetic tgt of ELINT platforms

□ Orbits in range of IADs die

These images from a CNAS wargame show a Russian red team's plan for attacking U.S./NATO information and command systems, along with the disposition of forces in a Baltic wargame. (CNAS)


United Kingdom Tornado
U.S. Air Force F-15
U.S. Navy F-14D
United States E-3A
U.S. Navy E-2C
U.S. Navy Carrier
U.S. Air Force Control and Reporting Center
NATO E-3A
Adaptable Surface Interface Terminal
NATO Control and Reporting Center
United Kingdom E-3A
Adaptable Surface Interface Terminal
U.S. Army Ground-Based Radar
French Republic E-3A
Forward Area Air Defense
U.S. Marine Corps and Air Force Ground Command and Control Centers
Adaptable Surface InterfaceTerminal
U.S. Air Force Message Processing Center

The Joint Tactical Information Distribution System (JTIDS) datalink system served U.S. and allied forces well for decades, but badly needs modernization. (Wikimedia Commons/DoD)

are greater than the engineering hurdles. Additionally, while this is ultimately a concept for combat operations, it is impossible to ignore China and Russia's use of information to achieve their objectives without fighting or to set advantageous conditions for combat.

Sometimes nomenclature and terminology matter, as they can alter—even if subtly and implicitly—thinking about a subject. Such is the case with the term C4ISR. By combining functions whose only major connection is their linkage through networks, C4ISR tends to focus discussions on the system of systems that comprises C4ISR, and elides the non-technical aspects of the underlying functions, such as the cognitive exercise of command and control, new organizational constructs, or non-technical methods for gathering and processing information. This is not to say that all uses of the term are flawed, or that efforts to improve the resilience of the DoD C4ISR architecture are misplaced. However, the casual use of the term as shorthand for the military process of gathering, processing, deciding, and acting on information should be reconsidered. It tends to pigeonhole thinking about information and command—which should be central to concept development and force design—into discussions about widgets, rather than missions, doctrine, organizational constructs, and training.

Instead, this paper focuses on information and command because more circumscribed frameworks like C4ISR failed to capture the breadth and interconnectedness of the challenges facing the DoD in this space. The paper defines information broadly to encompass activities that might traditionally be considered information operations as well as ISR. Likewise, the paper defines command broadly in the manner of Martin van Creveld's *Command in War*—comprising command, control, communications (C3), and supporting processes.[7] Where necessary, the paper delineates between the different aspects of C3.

Seeing Red: Chinese and Russian Approaches to Information and Command

This section of the paper describes how China and Russia think about information and command in the context of military confrontation and conflict with the United States.[8] China and Russia have different national histories, present conditions, and future trajectories.[9] Their thinking about international relations, inter-state competition, and warfare are likewise distinct. With that said, Chinese and Russian armed forces share many characteristics, patterns of thought, and (admittedly translated) terminology regarding military strategy and future operations against the United States.[10] This section begins by discussing why China and Russia would want to limit any conflict with the United States and how this desire introduces tensions into their military strategies. Next, it describes how China and Russia are using information operations to gain a "peacetime" advantage in the information environment. After that, this section discusses the ways in which China and Russia would use ID/CD approaches to prevail in the techno-cognitive confrontation in the event of war, with a particular focus on space, cyberspace, and the electromagnetic spectrum. Finally, the section concludes by summarizing recent Chinese and Russian command-and-control reforms that speak to their theories about modern warfare.

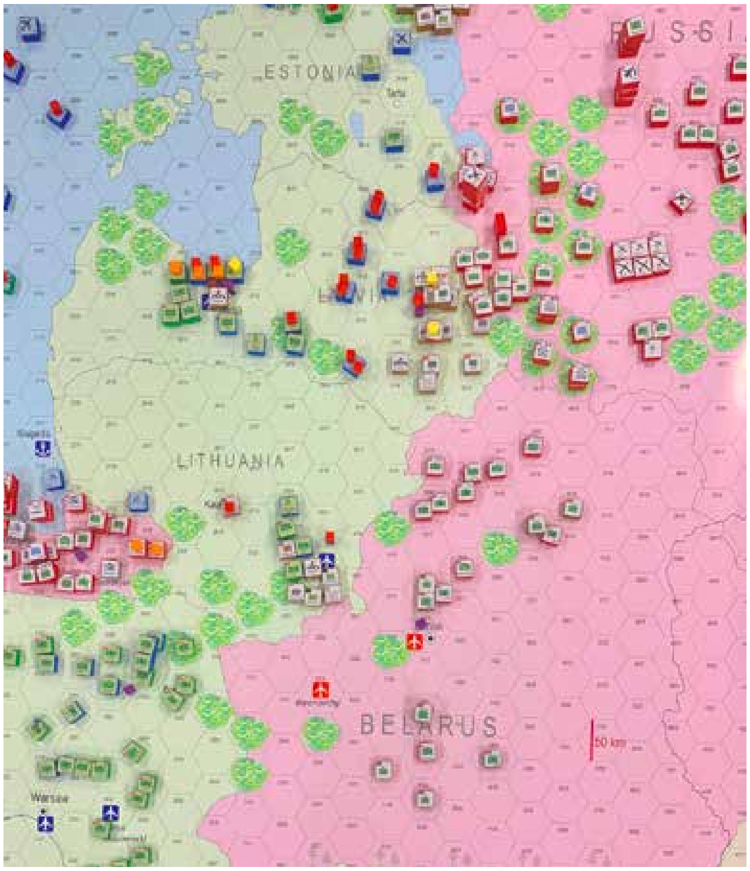
Keep the Conflict Limited

Within the 2030 timeframe of this paper, both China and Russia likely would prefer to avoid armed conflict with the United States or, if war were unavoidable, limit and localize the conflict.[11] On the Western Front of World War I, France and Britain developed a concept called "bite and hold," in which they seized limited objectives and deterred or halted German counterattacks through massive artillery barrages. China and Russia likely will follow similar patterns strategically and operationally in the event of war, something Russian expert Michael Kofman of the Center for Naval Analyses has called "bite and attrite," and Billy Fabian of CNAS has called "strategic bite and hold." The following discussion will explain the logic behind China and Russia's desire to limit conflicts, and the tensions this creates with their military strategies and concepts for fighting the United States.

First, nuclear-armed states can rationally go to war with each other over less than absolute objectives using only limited means, since initiating a total war would carry a high risk of nuclear response. This is not to say that leaders always will behave rationally, but rather that this outcome is far more likely to be the result of miscalculation and escalation within an extant conflict rather than the adversary's opening gambit.

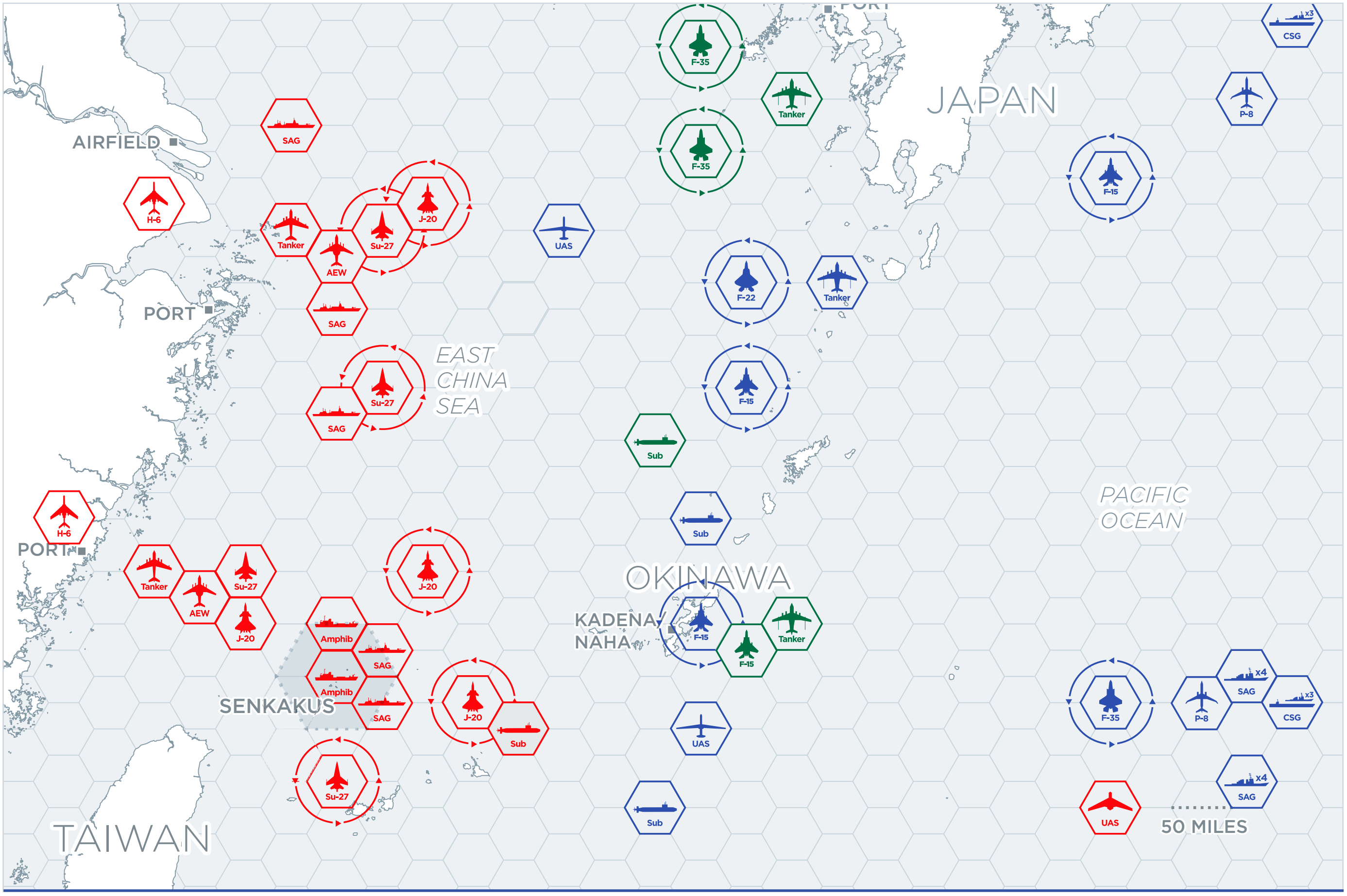
Second, limiting or localizing a conflict to areas on their immediate peripheries ensures that the war is more important to China or Russia than it is to the United States. This asymmetry of interest may deter the United States or its allies and partners from intervening or limit the size and character of the intervention.

Third, a limited or local conflict would enable China or Russia to achieve a favorable correlation of forces by avoiding combat with the entirety of the U.S. joint force and a large U.S.-led coalition. China and Russia may threaten or execute global operations as part of a limited war strategy, but these actions would be intended to deter a U.S. or coalition military response or, failing that, to delay or degrade the response such that China and Russia could achieve their objectives.



This map from a CNAS wargame shows the density of Russian threats in a Baltic scenario and the attrition to U.S. forces—represented by the red cubes—shows the risks these defenses would pose to U.S. operations in contested environments. (CNAS)

LIMITED WAR: EAST CHINA SEA



As shown on this map based on a CNAS wargame, China can achieve an advantageous balance of forces in a local, limited conflict over the Senkaku Islands.

Fourth, limited, local conflicts would play to Chinese and Russian strengths in information and command, while offsetting their weaknesses by enabling the Chinese and Russian regimes to maintain centralized, direct control over military operations in ways that might be unfeasible in a broader or more distant conflict. The nearer the conflict is to Chinese or Russian territory, the more the regimes can depend on relatively secure, reliable, and redundant forms of terrestrial communications while minimizing reliance on more vulnerable long-range networks such as satellite communications.

Fifth, fighting close to home allows Chinese and Russian forces to operate on interior lines under the cover of land-based systems such as integrated air defense systems, anti-ship missiles, electronic warfare, and counter-space systems. These systems help protect Chinese and Russian information and command systems against attack while contesting U.S. forces' freedom of maneuver on exterior lines in the air, maritime, space, and electromagnetic domains, and they are central to helping their forces "bite" their initial objective and deter or defeat a counterattack.

Finally, localizing the conflict presumably will ensure that China and Russia have greater familiarity with the area compared to the United States and any extra-regional allies and partners. China and Russia could leverage their knowledge of the terrain and local populations, as well as networks of friendly agents to gain greater situational awareness and prepare the information environment in ways that the United States may not be able to match.

There is an inherent tension between Chinese and Russian strategic desires to limit a conflict with the United States and their operational goal of disrupting, degrading, or destroying the system-of-systems that undergird U.S. military power either preemptively or immediately at the outset of a conflict.[12] In the event of a crisis or an imminent conflict, China and Russia would face a difficult choice regarding attacks on U.S. forces and assets, and particularly those located in third-party countries (e.g., U.S. forces in Japan during a Taiwan crisis). Striking these forces and assets aggressively would maximize China's or Russia's windows of operational advantage, during which they could seize their objectives. On the other hand, such an aggressive move might undermine the strategic goal of limiting a conflict. Attacks on U.S. bases in Japan during a Taiwan crisis, for example, might push Japan to offer greater military support to U.S. and Taiwanese operations. Likewise, heavy U.S. casualties might harden American resolve much as they did following the attacks on Pearl Harbor and the Philippines in 1941—rather than restraining U.S. commitment, public opinion might push for a more aggressive and expansive response.

This tension is particularly acute for information and command systems, since as will be discussed in greater detail below, seizing immediate or preemptive advantage in these areas is central to Chinese and Russian military strategy and operational concepts for conflict with the United States. During CNAS wargaming, exploiting this tension proved effective at forcing China and Russia into this dilemma between unfavorable escalation or expansion on one hand, or insufficiently disrupting or degrading U.S. combat capability on the other. In Pacific wargames, the Chinese red teams deliberated at length over attacking Japan, South Korea, Singapore, Australia, and other states hosting U.S. forces and information systems. Of these, kinetic attacks against Japan were the most consequential, as the red teams feared bringing Japan and the significant capabilities of their Self-Defense Forces fully into the fight. In European wargames, the Russian red teams aggressively attacked NATO airbases, logistics networks, and information and command systems in hopes of inflicting "unacceptable damage" and coercing NATO to back down. These and other escalatory actions stood in rather stark contrast to the limited incursion that Russian forces made into eastern Latvia.

Use Information to Prepare the Environment and Manipulate Perceptions

China and Russia perceive themselves to be in a long-term struggle or confrontation with the United States that is characterized by ebbs and flows in tensions and, possibly, outbreaks of open hostility or armed conflict. The persistent nature of this confrontation places a great deal of emphasis on continual preparatory operations in the information environment to gain advantage in the larger confrontation as well as to ensure a more favorable correlation of forces in the event confrontation spills over into crisis or conflict. This emphasis on preparatory action is critical, because preparation is key to how China and Russia hope to offset U.S. advantages in information and command systems, while also enabling their forces to deal with the speed and complexity of modern informatized warfare.

Both China and Russia operate in the information environment psychologically to alter the perceptions, beliefs, and motivations of key foreign and domestic audiences at the strategic level, and to manipulate the perceptions, motivations, and behaviors of adversary military forces at the operational and tactical levels. China and Russia also use technical methods like cyberattacks and electronic warfare at the strategic, operational, and tactical levels as means to gather or manipulate information, and degrade adversary systems during conflict.[13] China and Russia perceive these activities as both offensive and defensive, with a focus on offense in practice.[14]

Chinese thinking on information warfare focuses on "winning without fighting" or, if necessary, using information to defeat a militarily superior foe.[15] This approach requires concerted preparation of the information environment as part of a continuous "struggle" with the United States, rather than as a discrete action in a crisis or conflict.[16] China calls this approach "Three Warfares," which comprises public opinion, psychological, and legal warfare.[17] Public opinion warfare, as its name implies, shapes the opinions of public audiences in China, the region, and beyond, with a particular focus on populations that hold key strategic positions. While public opinion warfare can take place during a crisis or conflict, its focus is primarily preparatory. Legal warfare attempts to establish legal justification for Chinese claims or actions. This approach works synergistically with public opinion warfare to bolster Chinese narratives and undermine opposing claims. Psychological warfare, by contrast, aims to deter or coerce a target by weakening its will to fight, or defeat it by confusing its understanding of the situation and degrading its cognitive cohesion and ability to make decisions.[18] Psychological warfare activities can occur as peacetime demonstrations, but focus primarily on crises and conflicts, and therefore concentrate more on operational or tactical targets.[19]

The creation of the Strategic Support Force (SSF) in 2015 is another indicator of the People's Liberation Army (PLA) thinking about information warfare. The SSF brought together virtually all of the PLA's strategic and operational organizations and assets responsible for military information operations, including space, cyberspace, electronic warfare, and psychological operations. This integration reflects Chinese thinking that information is the core function, and that domains are media for the execution of information warfare.[20] The SSF, like the PLA Rocket Force, is under the direct operational control of China's Central Military Commission, which implies both that the SSF is vital to China's military strategy and that, despite its designation as a support force, it likely will conduct independent "supported" operations.[21]

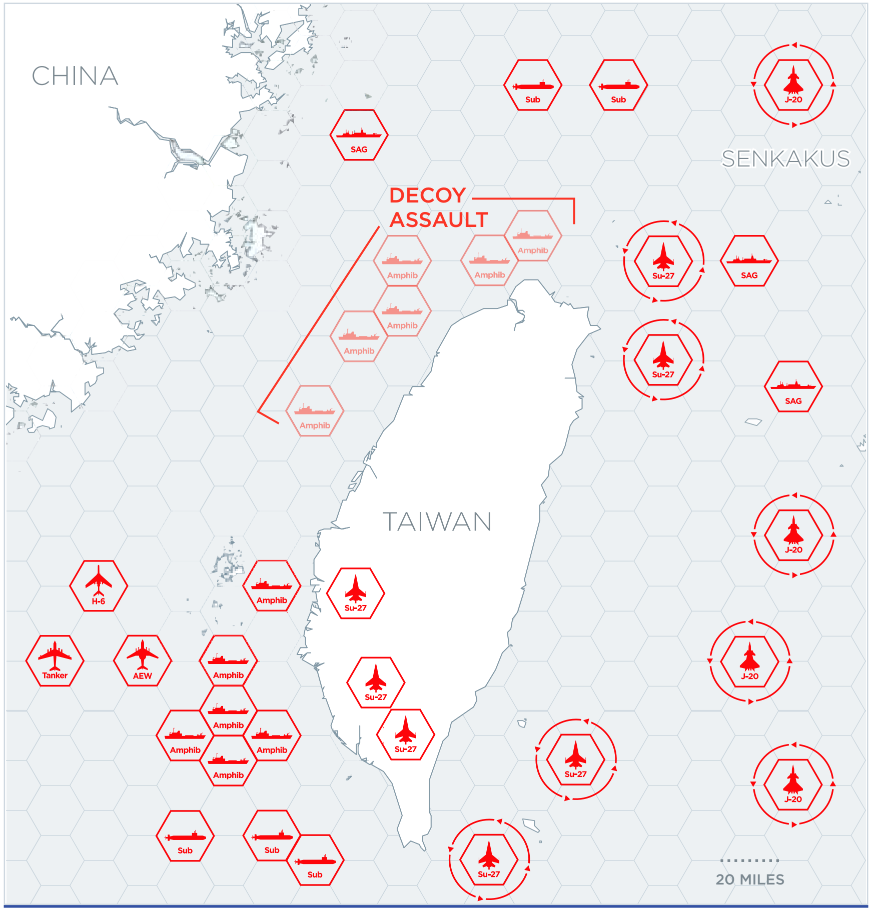
In CNAS wargames, Chinese red teams sought to operationalize these concepts in many ways. One red team created a narrative that Taiwan's position was hopeless and its leaders were hapless by disseminating "deepfake" videos showing Taiwan's president and the chief of the general staff surrendering. The same team also used AI-generated "deepfake" videos to show numerous PLA echelons ashore on Taiwan, when only one echelon was clinging to a narrow beachhead, and to confuse Taiwanese forces about the central thrust of the PLA assault, thereby encouraging them to commit limited reserves to the wrong location. One could imagine how such disinformation could confuse key Taiwanese personnel—such as those manning coastal defenses or those responsible for defending key ports—during a critical moment, creating a window for the PLA to seize certain objectives.

Russia views information warfare as the crux of modern interstate competition and conflict.[22] Russian concepts and actions in the information space fall into roughly two categories: political warfare, sometimes referred to by its former Soviet nomenclature "active measures," and information confrontation, which some refer to in the old Marxist-Leninist vernacular as "information struggle."[23] Unlike the relatively domain-centric thinking that predominates in the U.S. defense ecosystem, Russian military thinkers view information and its cognitive and psychological impacts as the central object and information confrontation as the overarching umbrella that covers cyber, space, electronic warfare, denial and deception (*maskirovka*), and psychological operations.[24]

The advantage of this coherent information-centric perspective is that it unifies and drives their activities in non-technical areas in a way that the domain-centric view of U.S. and NATO forces does not. The disadvantage is that this perspective might inhibit Russian conceptual development of the cyber, space, and electromagnetic spectrums as warfighting domains in themselves, rather than as conduits and repositories of information. Regardless, this perspective drives a much greater Russian focus on using technical means to create psychological or cognitive effects relative to U.S. military thinking, or arguably compared with Chinese discussions on this topic.

Political warfare is a broad term describing state and non-state entities aggressively pursuing Russian foreign policy objectives while also defending Russia against foreign entities conducting similar operations.[25] The objectives of Russian offensive political warfare are threefold. First, Russia seeks favorable policy outcomes, such as a repeal or limitation of sanctions, or financial policies that protect illicit Russian overseas assets.[26] Second, Russia works to install or support friendly or

PEOPLE'S LIBERATION ARMY DECEPTION VERSUS TAIWAN



The People's Liberation Army could use deception and information operations to get Taiwan to commit its limited defensive forces to the wrong location.

non-hostile regimes where possible and otherwise seeks to weaken Western states and institutions, all with the goal of reducing organized opposition to Russia and gaining greater freedom of action. Finally, Russia sows disorder and discord in Western societies and institutions by exacerbating and exploiting political and social divisions and by abnegating the very idea of objective "truth." The objective here simply is to weaken and distract its competitors, thereby contributing to Russia's broader goal of delegitimizing Western ideals (e.g., democracy and human rights) and institutions (e.g., NATO and the European Union) that threaten Russian interests, ultimately giving the Kremlin a freer hand.

> **It is difficult to overstate the importance of information confrontation for how Russian armed forces plan to compete with and fight the United States and NATO.**

By contrast, information confrontation is a Russian Armed Forces concept that grew from a combination of traditional Russian/Soviet information operations and more recent, post–Cold War thinking about "New-Type Warfare." New-Type Warfare (sometimes called New-Generation Warfare) is Russia's high-level description of the character of warfare.[27] Russian writing on this topic describes the current and future character of warfare and also posits conceptual means to exploit the opportunities therein.[28] It is difficult to overstate the importance of information confrontation for how Russian armed forces plan to compete with and fight the United States and NATO. Russian thinking about New-Type Warfare has reemphasized Soviet beliefs that the period of time directly preceding the conflict and the opening days of combat—what Russians call the "initial period of war"—likely will decide the outcome.[29] This belief, combined with the speed of modern combat, has pushed Russia toward persistent, aggressive information-psychological operations in order to coerce adversaries, shape the environment, and prepare for conflict.[30] Russian military thinkers believe that, in the pre-conflict or crisis phase of modern warfare, non-military means such as information will weigh in at a ratio of 4 to 1 with military means.[31] Other influential Russian military strategists have argued that success in modern warfare is predicated on information superiority above all else.[32]

Information confrontation comprises two related lines of effort: information-psychological and information-technical. Information-psychological, as the name implies, manipulates the perceptions, beliefs, motivations, and cognitive functions of targets. Information-technical targets the systems that contain or transmit information. Though separate, these two functions work together closely. Technical exploitations of adversary systems using cyberattacks or electronic warfare deliver information that achieves a psychological effect, as was the case when Russian hackers broke into the computer systems of the Democratic National Committee and released information harmful to the Democratic Party in the 2016 election. Conversely, psychological operations could cause an opponent to question the validity of their information systems. Given their fear of U.S. attacks on Russian society and information systems, Russian forces apply these concepts for defensive as well as offensive purposes.[33]

Information-technical aspects of information confrontation have two purposes: as a means to infiltrate or exfiltrate information to achieve a psychological effect (or to defend against the same), and to disrupt, degrade, or destroy adversary systems (or prevent the same from happening to Russian systems). These efforts require constant preparatory action in peacetime. As Timothy L. Thomas puts it in *Russian Military Thought: Concepts and Elements*, "The speed of cyber operations indicates that forces must be prepared now for the initial period of war (IPW). Planning tomorrow for a surprise attack is more than a day late, as the cyber IPW may result in the conflict's end before it starts."[34] The mere threat of information-technical means can have profound psychological effects, which makes them particularly effective for coercion. The possibility of Russian cyber hacks of the U.S. power grid, for example, created a mild panic in 2018 and the recent SolarWinds attack will likely keep such threats in the calculus of U.S. policymakers considering actions to counter Russia.[35]

Reflexive control (also sometimes referred to as perception management) is a key part of Russian thinking on information confrontation, and it spans both psychological and technical aspects as its effects are psychological, while its delivery mechanisms can be technical. Reflexive control entails managing the perceptions of a potential target such that applying a stimulus to the target results in a relatively predictable response that places them in an unfavorable position.[36] For instance, Russian red teams executed reflexive control in CNAS wargames by fomenting unrest in multiple Baltic cities with major Russian populations, such as Narva in Estonia. Predictably, this prompted local security forces and NATO units to converge on these cities and, in several cases, caused incidents that the red team exploited to intervene to protect ethnic Russians. These distractions tied down NATO forces so that the main Russian effort could seize a chunk of eastern Latvia almost unopposed.

Both Chinese and Russian red teams used civilian casualties—whether real or fake—to undermine public support for U.S. and coalition operations, rally their own populations, and bolster their narratives. One particularly devious Chinese red team loaded the first wave of ships crossing the Taiwan Strait with political prisoners, then recorded and publicized the "civilian" casualties that resulted from U.S. and Taiwanese anti-ship attacks. After the first wave of U.S. attacks to suppress air and missile defenses in Kaliningrad caused legitimate civilian casualties, a Russian red team moved its air defense systems into more densely populated areas, thereby creating more civilian casualties and supporting Russia's narrative of victimhood. While the wargames did not fully adjudicate the political and international consequences of these actions, it is not difficult to imagine their potential negative impact on coalition cohesion or U.S. domestic political support.

Degrade Information and Disrupt Command to Prevail in the Techno-Cognitive Confrontation

Witnessing the overwhelming conventional warfighting advantage that information and command "systems-of-systems" conferred on U.S. armed forces beginning with the Gulf War, China and Russia responded by developing operational concepts and supporting capabilities to rapidly gain and maintain an advantage in the "techno-cognitive confrontation," through information degradation and command disruption. This approach is at the core of their concepts for attacking the central nervous system of the joint force. This section will discuss critical aspects of this techno-cognitive confrontation, how China and Russia plan to win it through ID/CD, and how the DoD can gain and sustain its advantage by achieving degradation dominance.

The lines of effort that comprise ID/CD take place across multiple domains. Acknowledging that the PLA and the Russian Armed Forces view these domains as part of a coherent approach toward gaining superiority in the information environment, this section breaks down the characteristics of the techno-cognitive confrontation into three critical domains—space, cyberspace, and the electromagnetic spectrum—for the purpose of analytic clarity.

SPACE

Projecting modern information and command systems globally requires access to space.[37] Every function of C4ISR and position, navigation, and timing (PNT) relies to some degree on space, and this reliance (or the cost and difficulty of alternatives) grows sharply as a function of the range and dispersal of operations. As a global military power that often operates at long ranges in a highly dispersed fashion along exterior lines, the United States is

In a CNAS wargame, civilian casualities were represented with white cubes. Each cube represented 100 civilian casualities. The blue team was forced to engage targets that were hidden in dense population centers in Kaliningrad and throughout the Baltic states. (CNAS)

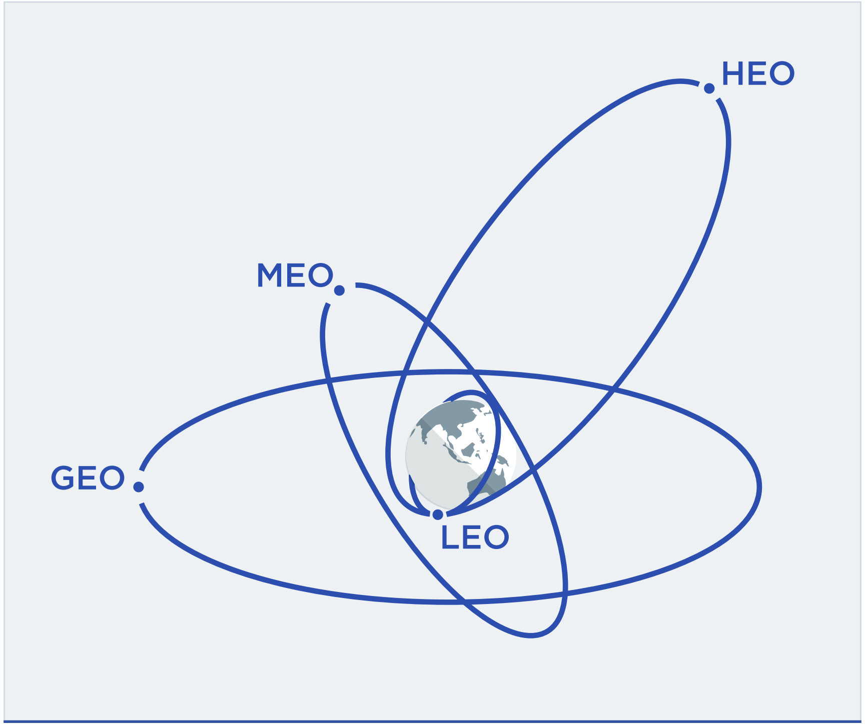
In an example of "reflexive control," a Russian red team stoked civil and armed unrest in eastern Latvia to draw in U.S. and NATO forces before badly attriting them with long-range artillery. (CNAS) particularly reliant on space for information and command. According to several Russian military theorists,

> …the present-day leading states accomplish communications, navigation, reconnaissance, and all command and control of strategic nuclear, missile defense, and precision-guided munitions through space. A breakdown of this entire systems [sic] by electronic and other asymmetric assets can largely reduce this advantage…[38]

Chinese military strategists think similarly, stating that “whoever controls space will control the earth.”[39] The first shots in a future great-power war therefore may not be bullets or missiles; instead, they are likely to be cyber weapons and electromagnetic radiation. Their primary targets may not be ships or bases or ground units, but rather space operations centers, satellites, and ground-control stations.

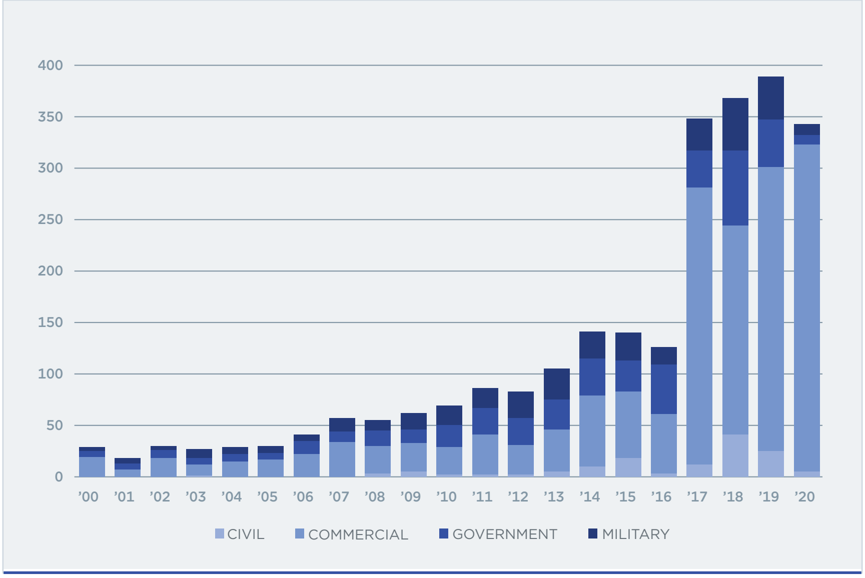
It is important to note, however, that the character of the competition in space is changing in ways that may constrain certain Chinese and Russian actions in space. The period of U.S. space dominance is ending, or perhaps has ended. China and Russia are building, or in the case of Russia, rebuilding space constellations that will enable them to conduct long-range military operations. At the same time, the number of countries and commercial entities relying on space for functions like communications, weather, agriculture, mapping, banking, and navigation has grown massively over the last two decades and likely will grow further over the next 10 years.

This proliferation of space capabilities has radically altered the strategic context of space operations in a relatively short period of time. This change may encourage China and Russia to limit their space operations—particularly kinetic actions—at least during a crisis and the initial phases of a conflict, to avoid damaging their own systems or those of neutral parties.[41] Instead, China and Russia will look to win the techno-cognitive confrontation in space by preserving their own assets and disrupting or degrading U.S. systems without unfavorably



An artistic rendition of low earth orbit (LEO) (up to 2,000 km), medium earth orbit (MEO) (2,000 to 35,000 km), highly elliptical orbit (HEO) (40,000 km at apogee), and geosynchronous earth orbit (GEO) (36,000 km).[40] (Defense Intelligence Agency)

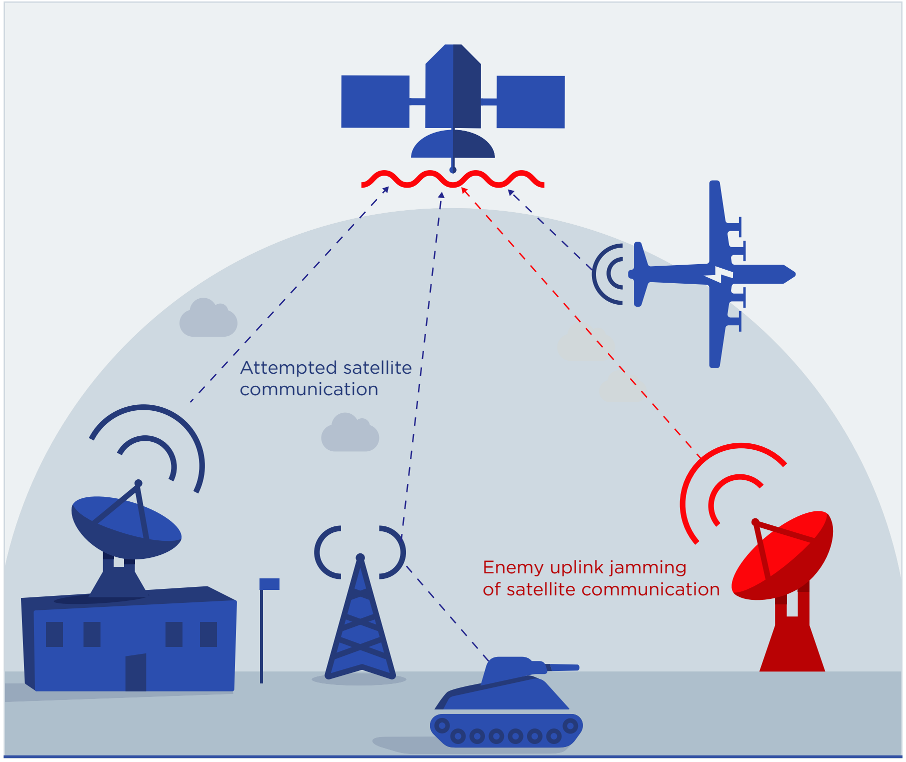
SATELLITE LAUNCHES OVER THE PAST 20 YEARS



This chart showing every unclassified or public satellite launch over the last 20 years demonstrates the rapid proliferation of space systems, driven largely by commercial entities.

Source: UCS Satellite Database, (Union of Concerned Scientists, 2020), https://www.ucsusa.org/resources/satellite-database.

SATELLITE UPLINK JAMMING


Attempted satellite communication
Enemy uplink jamming of satellite communication

Uplink jamming uses radio frequency "noise" to prevent terrestrial users from communicating "up" to a satellite.

expanding or escalating the conflict. Accordingly, teams in CNAS wargames were reluctant to use kinetic attacks in orbit.[42] This seems to be consistent with Chinese and Russian desires to limit a potential conflict, but it remains to be seen if China or Russia would avoid kinetic actions if a conflict went poorly or if, as appears to be the case, they develop kinetic weapons capable of disabling satellites with minimal debris.

Within this context, Chinese and Russian space operations against the United States likely will focus on four lines of effort targeting: 1) space situational awareness and control; 2) satellite communications; 3) PNT; and 4) space-based ISR.

Space situational awareness and control. Space situational awareness systems monitor space-based and terrestrial activities to detect, identify, and track objects and activities, thereby creating a common operating picture in space. Space control systems operate and maneuver friendly space-based systems. Without a common operating picture in space and an ability to control its own space systems, it is impossible for a country to counter enemy actions in space or establish and maintain space superiority. China and Russia's opening salvos in space therefore would likely attack U.S. space situational awareness and control systems. Cyberattacks would disrupt operations and corrupt information across these systems while non-kinetic weapons or co-orbital anti-satellite weapons would disable on-orbit sensors such as space radars to enable follow-on operations as needed.[43] Where possible, China and Russia might conduct non-kinetic attacks on ground-control stations such as the Combined Space Operations Center at Vandenberg Air Force Base in California, or kinetic attacks against forward operations centers and ground-control stations.

These attacks could cripple U.S. space and counter-space operations and create a window for China or Russia to seize space superiority and operate with greater freedom in other domains. The downside is that they risk strategic escalation, including the use of nuclear weapons. Space situational awareness, along with missile warning and nuclear command, control, and communications, is closely tied with the ability of a country to respond effectively to a strategic first strike. Fear of escalation likely offers a partial explanation for why teams limited their attacks on space situational awareness systems in CNAS wargames.[44]

Satellite communications. U.S. armed forces depend heavily on satellite constellations to communicate, share data, and command and control forces (particularly unmanned forces) over long distances.[45] China and Russia therefore emphasize disrupting and degrading U.S. satellite communications in their counter-space operations. Jamming, and particularly uplink jamming (broadcasting large amounts of radio-frequency "noise" from the earth's surface toward a communications satellite) are the most common attacks on space-based communications. However, China and Russia also likely conduct downlink jamming (downward toward earth) or on-orbit cross-link jamming (between satellites in orbit).[46] In addition to jamming, China and Russia can also conduct cyberattacks against the computer systems that operate satellite communications networks, or attack the ground infrastructure that enables their operation.

In CNAS wargames, Chinese and Russian red teams leveraged all of these techniques, with uplink jamming being the most widespread, while cyberattacks and kinetic attacks on ground stations were also relatively common. The goal of these attacks was to limit the U.S. blue teams from being able to communicate and command and control forces over long distances, thereby isolating dispersed U.S. forces and preventing the coordination and synergy on which joint or multi-domain operations depend. When successful—and they often were, given Chinese and Russian electronic warfare capabilities and the vulnerability of satellite communications to jamming—these attacks effectively disintegrated the joint force into smaller service- or domain-specific units constrained by the range of resilient line-of-sight communications. Rather than achieving synergy by combining effects from all domains, these smaller units largely fought in isolation using the weapons and systems available within their immediate span of control.

Space-based position, navigation, and timing. Space-based PNT, such as the U.S. Global Positioning System (GPS) and similar Chinese (Beidou), Russian (GLONASS), and European (Galileo) systems, allow military forces to know where objects are in space, where they are headed, and what time it is with a high degree of accuracy and precision. Much as these systems have become ubiquitous in civilian life through the proliferation of GPS and other PNT-enabled devices, they are woven deeply into the fabric of modern military operations across a range of missions. Space-based PNT allows for precise, and increasingly automated navigation, which directly enables a host of key systems including precision-guided weapons like the Tomahawk Land-Attack Cruise Missile and the Joint Direct-Attack Munition, and a variety of unmanned vehicles.

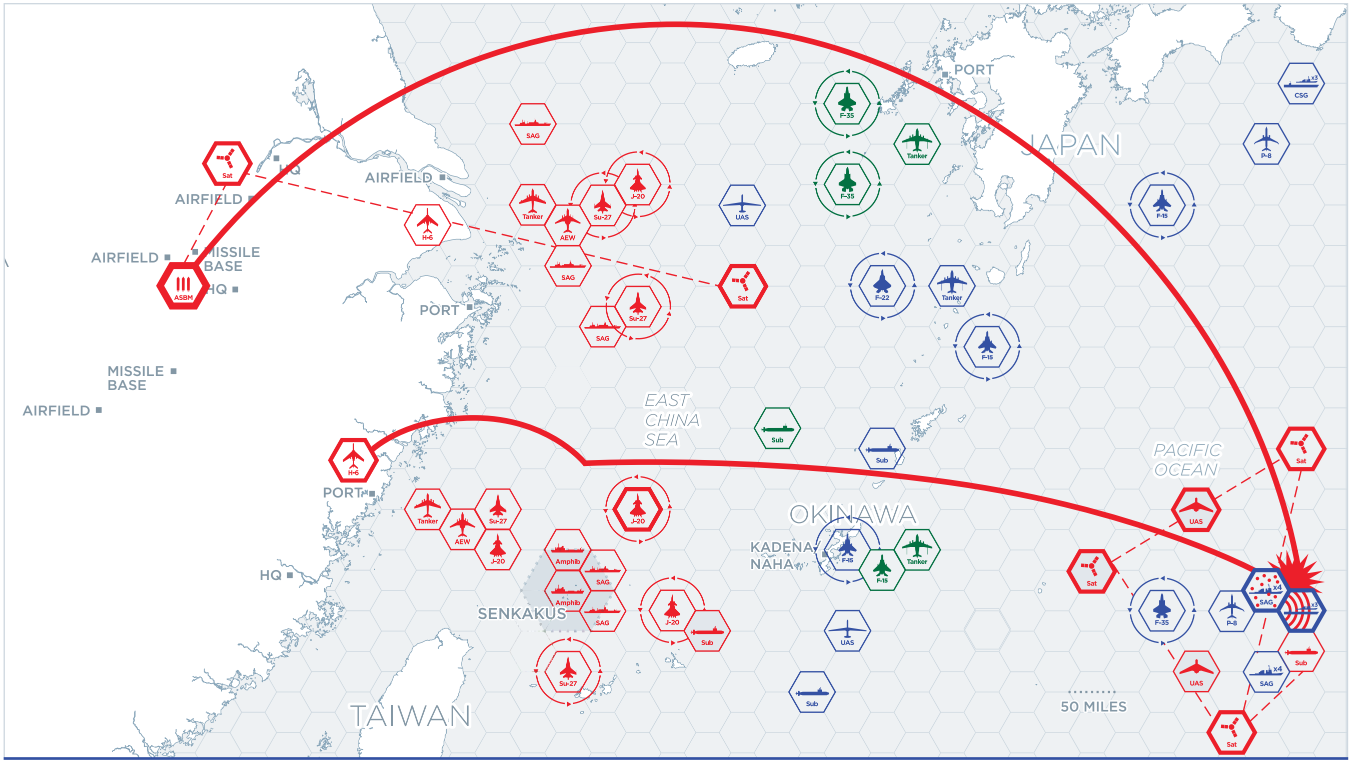
Beyond navigation, PNT enables tracking of friendly forces and, combined with intelligence, accurate positioning of enemy forces to create a common operational picture. This picture, or COP, gives commanders and subordinates a shared understanding of the dispositions of their own forces and those of their adversaries. Such a shared understanding has long been critical to success in warfare—hence the famous Sun Tzu aphorism about the importance of knowing oneself and one's adversary. However, the changes in the character of warfare wrought by the proliferation of long-range precision-guided weapons arguably have made this picture even more critical because it is foundational for precisely targeting expensive, and therefore relatively scarce munitions.

China and Russia emphasize degrading and, where possible, exploiting GPS to foil U.S. operations. In CNAS wargames, Chinese and Russian red teams used cyberattacks and electromagnetic spoofing to disrupt GPS. Red teams used the former to disrupt the entire GPS system, while the latter fooled specific systems such as GPS-guided weapons to push them away from a target or, more deviously, to push them into hospitals or schools to create an opportunity for an information operation. Red teams leaned heavily on uplink jamming to disrupt in-theater use of satellite communications. Several red teams attacked ground stations kinetically, but no team physically attacked GPS satellites.

Space-based intelligence, surveillance, and targeting. The use of space to gather intelligence, surveil adversary forces, and target them for attack is a critical component of modern warfare. Satellites—whether performing wide-area surveillance and cueing, precise multi-INT targeting, communicating targeting updates, or providing damage assessments—comprise critical parts of long-range kill chains against ships at sea and forces on land.[47] Moreover, given the extreme difficulties and costs associated with defeating large salvos of precision-guided missiles and the relative vulnerability of satellites, space is an area where both sides perceive an opportunity to seek a potentially decisive advantage by attacking and degrading these kill chains.

China and Russia have invested heavily in a variety of active and passive capabilities and techniques to interfere with U.S. space-based surveillance and targeting. Consistent with Chinese and Russian emphasis on rapid, even preemptive action to gain advantage in warfare, these actions likely would begin well before any conflict. China and Russia would use deception and counter-surveillance techniques to prevent the United States from gaining rapid and accurate indications and warning of an impending attack or critical intelligence about their force dispositions. This would give Chinese and Russian forces an element of surprise and delay any U.S. or allied response. At the outset of a conflict, China and Russia likely would take more active measures to disrupt and degrade U.S. space-based observation and targeting. These measures might include blinding or dazzling electro-optical and infrared sensors with lasers, and jamming space-based radars and signals intelligence satellites using radio-frequency (RF) attacks. In CNAS wargames, Chinese and Russian teams used laser dazzlers and blinders and RF jammers and spoofers to create large "blind spots" in which U.S. space systems couldn't observe their operations or contribute to precise targeting.

MARITIME TARGETING BATTLE IN THE PACIFIC



Long-range strikes against moving targets, like carrier strike groups, require exquisite over-the-horizon targeting and communication, as seen here in a Pacific scenario from a CNAS wargame.

Chinese and Russian counter-surveillance and targeting operations combine these active countermeasures with more traditional techniques in ways that further hinder U.S. targeting. In CNAS wargames, for example, Chinese teams used electronic warfare and laser dazzling/blinding combined with emissions control (EMCON), decoys, and intentional cluttering of the Taiwan Strait with derelict ships to hinder U.S. surveillance and targeting of their invasion fleet.[48] Chinese and Russian armed forces use camouflage, concealment, and deception (CCD) and EMCON and exploit complex terrain and civilian traffic and signals to mask their signatures. In CNAS wargames, Russian red teams mixed EMCON with rapid maneuver, complex terrain, and redundancy to keep their integrated air defense system functioning while evading U.S. attempts at suppression.[49] Used in concert with attacks on U.S. satellite communications, EMCON, CCD, and integrated air defense systems, these counter-space weapons grant Chinese and Russian ground forces greater freedom of maneuver within and near their own territory.

CYBERSPACE

China and Russia both engage in concerted, widespread cyber espionage and preparatory cyber operations, and their actions in cyberspace in the event of a crisis or conflict with the United States and its allies and partners likely would share many characteristics. Both emphasize preemptive or extremely rapid actions against U.S. information and command systems to collect information, confuse and deceive forces, and disrupt the ability of the United States and its allies and partners to respond quickly and effectively.[50] Their attacks likely will focus on systems that are simultaneously vulnerable to cyber intrusion and would create widespread or cascading effects if disrupted. For example, China and Russia could attack U.S. Transportation Command (TRANSCOM) logistics networks that control critical logistics functions, like the disposition of U.S. Air Force aerial refueling tankers. Many such networks are unclassified and allow trusted access to contractors lacking stringent cyber security practices.[51] These early actions would sow distrust in computer systems and networks more generally, which could cripple the effectiveness of a U.S. response. China and Russia also would likely accompany these focused attacks with broader attacks against U.S. government or commercial networks in an attempt to cognitively overload any U.S. response, an approach Russia took during the 2008 Georgia war.[52]

After the initial attacks, Chinese and Russian cyber operations likely would escalate to more aggressive attacks to degrade or even destroy U.S., allied, and partner systems under the belief that they would have to use their exploits or risk losing them. This is one area where Chinese and Russian operations may diverge. Russian writing on cyber warfare and recent experience from Ukraine suggest that—consistent with the cognitive/psychological focus of Russian information operations—Russia may be willing to keep a cyber exploitation "open" to leverage it for disinformation, vice using more aggressive means to shut down a key network. Nevertheless, both China and Russia likely would accompany attacks on U.S. military systems with strategic attacks designed to overwhelm political decision makers (and limited numbers of cyber operators), deter intervention, or coerce wavering coalition members.

In CNAS games, Chinese and Russian red teams pursued all these approaches, using preparatory actions to gain access to TRANSCOM networks and the time-phased force deployment data that shows the timeline of U.S. force deployments. Similarly, they attacked U.S. combined air operations centers (CAOCs) and other command centers to exfiltrate critical information about U.S. plans and posture, including the Common Operational Picture and the Air Tasking Order. To sow cognitive disorder, they also attempted to penetrate GPS, the Autonomic Logistics Information System for the F-35, the database for Common Access Cards, power grids and commercial internet in areas surrounding U.S. and allied bases, and the computer systems for commercial air traffic control.

China and Russia also would closely integrate their cyber operations with electronic warfare. China refers to this approach as Integrated Network and Electronic Warfare (INEW), while Russia suffuses this holistic perspective throughout their writing on, and execution of information confrontation.[53] Both emphasize cyber operations prior to and at the outset of a conflict and transition toward electronic warfare as cyberattacks burn through network exploitations, adversaries patch their systems, and as adversary forces increasingly use radio frequency, vice computer network communications.[54]

Cyberspace exists simultaneously as a conceptual domain and actual physical locations through which data passes or in which it rests. This duality enables armed forces to threaten it physically as well as digitally. China and Russia have plans to do exactly that by attacking the undersea cables on which so much internet traffic depends.[55] In CNAS wargames, Chinese and Russian red teams launched aggressive attacks on undersea cables, specifically where they "land" ashore. In nearly every case, these attacks allowed red teams to disrupt and degrade U.S., allied, and partner communications, and contributed to confusion and distraction at the strategic level as governments were forced to respond to sudden losses of connectivity.

Chinese red teams attacked undersea cables throughout the Indo-Pacific theater. These attacks often resulted in the loss of terrestrial internet connectivity on Taiwan, Japan, Guam, and Hawaii and forced these islands to rely on lower bandwidth and more vulnerable satellite communications. In Europe, Russian red teams often had ambitious goals to conduct massive, crippling attacks against trans-Atlantic undersea infrastructure, but these teams' limited special-purpose submarine capacity could not quickly eradicate the dense cable communications between North America and Europe.

When total internet isolation was not possible, some red players suggested using physical attacks to "herd" U.S., allied, and partner internet traffic onto networks that might be more vulnerable to electronic warfare (EW) or susceptible to other forms of exploitation like cyber. While certainly possible in theory, red teams in CNAS wargames failed to achieve this level of discrete control over blue and other friendly communications in practice—more typically they simply degraded blue communications across the board.

One proverbial "dog that didn't bark" in CNAS games was physical threats to data centers. As the DoD transitions more of its data, information, and supporting services to the cloud, it should anticipate a broad range of threats to these assets, including physical attacks against data centers using either long-range strike, special operations forces, or covert/clandestine means to degrade their operations.

THE ELECTROMAGNETIC SPECTRUM

Chinese and Russian thinkers best summarize the importance of the electromagnetic spectrum (EMS) to their respective military strategies. People's Liberation Army Air Force (PLAAF) spokesperson Shen Jinke said that, "in information systems combat operations, *the side that seizes control of the electromagnetic spectrum, the electromagnetic power, will control the course of the war* [emphasis added]."[56] Major General Yuriy Lastochkin, head of the Russian Defense Ministry's radio-electronic warfare force, stated:

> EW is the most effective, fast-moving and cost-effective means of neutralizing the technical advantages of the opposing side … In the near future, qualitative changes in the development of EW forces and means *will make it possible to decide the fate of all military operations* [emphasis added].[57]

China and Russia see electromagnetic spectrum operations as central to gaining an advantage in the techno-cognitive confrontation, largely because it serves as the common domain linking space, cyberspace, and electronic warfare. Its salience in their operations grows in conflict as mobile military forces increasingly rely on wireless RF communications.[58] Accordingly, they see EW as critical to disrupting and degrading U.S. operations by attacking the radio-frequency sensors and communications networks that U.S. forces use to gather and transmit information while on the move. Chinese and Russian forces also rely heavily on EW systems to gather information on enemy forces as a key part of their intelligence and targeting apparatus. The aim of these operations is to negate U.S. communications and sensors by degrading key parts of the EMS, or to exploit U.S. dependence on the EMS by infiltrating wireless networks or using RF emissions to target U.S. and friendly forces.

> **'In information systems combat operations, the side that seizes control of the electromagnetic spectrum...will control the course of the war.'**
>
> —Shen Jinke, PLAAF spokesperson

Consistent with their view that the EMS is a component of the broader information environment, China and Russia both tightly integrate EW and cyber operations. China calls this approach INEW, and sees it as central to their concept for gaining advantages in information and command against the United States. For Russia, mixing EW and cyber enables them to combine the information-technical and information-psychological aspects of information confrontation. For example, Russian forces in Ukraine have used a mix of EW and cyberattacks to send text messages to Ukrainian forces saying "leave or you will die" before artillery attacks.[59]

Chinese and Russian red teams used almost all these methods in CNAS wargames. All red teams heavily jammed U.S. communications and radars in the primary operating environments, all the way from GEO down to terrestrial very high frequency (VHF) communications. However, Russian red teams jammed much more broadly and intensely, shifting relatively quickly from "spot" jamming of specific frequencies and waveforms to "barrage" jamming of broad portions of the EMS. The Russian teams calculated that any decrement to their ability to use the EMS would be more than offset by the impacts of jamming on U.S. operations. In the games, neither China nor Russia could wholly deny U.S. communications; as one player noted, the EMS is remarkably broad and impossible to jam every frequency all the time. Still, Chinese and Russian jamming decremented U.S. and friendly communications and key sensors like synthetic aperture radars. Both Chinese and Russian red teams also used EW to target U.S. forces—and particularly maritime forces—and used this information to cue or target long-range precision-strike assets.

Centralize and Automate Command and Control

China and Russia have taken steps in recent years to improve their command and control.[60] These reforms are part of a broader trend within the People's Republic of China (PRC) and the Soviet Union/Russian Federation to improve their command-and-control structures and processes, but they have taken on new urgency in light of technological changes and the demands of modern warfare against an opponent such as the United States. China and Russia spend a great deal of time forecasting the character of future warfare. Within these forecasts, both have determined that the best way to coordinate effects from multiple domains—given the speed, chaos, and lethality of the modern operating environment—is to centralize and streamline decision-making and to leverage automation and artificial intelligence to decrease the cognitive load on commanders, accelerate decision cycles, and reduce the chances for human error.

Consistent with their thinking about the character of modern war and the importance of the initial period of warfare, this approach allows Chinese and Russian commanders to tightly control or "script" the opening sequences of combat the way an American football coach might script an opening sequence of plays. While Chinese commanders may emphasize Sun Tzu–influenced stratagems and Russians may emphasize using reflexive control to manipulate an adversary, the end result of this script in the early phase of combat is often quite similar in wargames. China and Russia leverage centralized and automated command and control to coordinate ID/CD actions to seize the initiative in the techno-cognitive confrontation by knocking U.S., allied, and partner forces back on their heels in physical, cognitive, and psychological domains. By the time U.S. forces recover—if they can—China and Russia have seized their objectives and are prepared to impose exorbitant costs for reversing their gains.

Toward this end, the PLA has undertaken massive reforms in its command structures under Xi Jinping's leadership, including the establishment of joint theater commands directly subordinate to the Central Military Commission led by Xi. These reforms had many purposes, but chief among them was to reassert the authority of the commission through a direct line of command in both peace and war.[61] The PLA also has been investing heavily in the development of artificial intelligence and automated or autonomous systems that can help it overcome what Xi referred to as the "five incapables," "Some [PLA] commanders cannot 1) judge the situation, 2) understand the intention of higher authorities, 3) make operational decisions, 4) deploy troops, and 5) deal with unexpected situations."[62] These shortfalls—which have persisted after decades of reforms and investments—severely impede the ability of the PLA to operate jointly or use all of its advanced weaponry effectively.[63]

Perhaps the most interesting aspect of recent PLA reforms is the elevation of the PLA 2nd Artillery into a full service as the PLA Rocket Force and the integration of Chinese space, cyber, electronic warfare, and psychological warfare units into the PLA Strategic Support Force.[64] Tellingly, both of these units are under the direct control of the Central Military Commission, suggesting how crucial these units and missions are to the PLA's conception of future warfare, and how the PRC's leadership feels the need to maintain direct, centralized control over them in order to direct and coordinate their actions.

Over the last decade, Russia also has streamlined, further centralized, and automated its military command and control.[65] Russia reformed its command structure into joint strategic commands in 2010 and established a National Defense Management Center to centrally command and control its forces in 2014.[66] In addition, Russia has been pursuing AI and other means to augment and automate its command and control from the strategic to the tactical levels through an "automated control system" and a "combat control information system," the purpose of which is to accelerate and improve Russian forces ability to gather, process, and act on information from disparate sources.[67]

As with the PLA, Russian desires for automation are partly related to longstanding deficiencies in personnel and a preference for direct control of the armed forces by political leadership. The New Look reforms instituted since 2008 have vastly improved conditions in the Russian Armed Forces, and the personnel situation is nowhere near as dire as the nadir of the mid-2000s.[68] However, Russia's forces continue to lag U.S. forces in terms of education and training. Much as the Soviet Red Army did, today's Russian Armed Forces compensates for this gap through automation, direct control, and heavy use of scripted "battle drills."[69]

Operational Vignette: Eastern Latvia 2030

Preceding paragraphs have broken down the Chinese and Russian approaches to information operations into discrete lines of effort. But in practice these actions would coalesce into coherent Chinese and Russian concepts of operations for gaining and maintaining an advantage in the techno-cognitive confrontation with the United States and its allies and partners. While individually discomfiting, these actions likely would be much more jarring and dislocating because of the totality of their impact on the ability of U.S. forces to perceive, understand, decide, and communicate quickly and accurately enough to keep pace with Chinese and Russian onslaughts. These concepts don't just parry strengths and attack weaknesses; they upend assumptions by turning strengths into weaknesses.

Outside of participating in realistic wargames and exercises, it can be difficult to comprehend the total cognitive and psychological impact of these concepts. To help address this gap, the following section describes a fictional operational vignette set in the Baltic region during the 2030 time frame. The vignette is based on Russian and American thinking on future warfare filtered through CNAS wargames. Its purpose is to describe how Russian techniques attack assumed U.S. strengths to create cognitive and psychological dislocation.

The Charlie Company commander dismounted from her Joint Light Tactical Vehicle (JLTV) alongside her Latvian counterpart and translator. She surveyed the situation—at least a hundred people in a raucous but apparently peaceful protest for greater civil rights and representations for ethnic Russians in the city of Rēzekne in eastern Latvia. These protests had become common since the unrest in Belarus following that country's attempt to develop closer ties with the European Union and NATO. Russia perceived this as yet another "color revolution," and was pushing back hard in the Baltics and keeping the commander and her NATO counterparts busy responding to a variety of provocations.

The Russians used their ties to local ethnic Russians and their control over the local Russian-language media to whip up discontent with the central government in Riga, and they were doing the same thing in Estonia and Lithuania. The commander felt like her job was to play "protest whack-a-mole" by driving out and observing these protests alongside a company of Latvian troops. It was frustratingly reactive and utterly disconnected from any broader strategy to counter Russian influence and information operations. This wasn't exactly the Battle for the Suwalki Gap that she'd prepared for at the National Training Center. But at least her company was doing something, and the constant activity probably looked good on the metrics that battalion headquarters reported to brigade headquarters (and hence her Officer Evaluation Report), so she kept her reservations to herself.

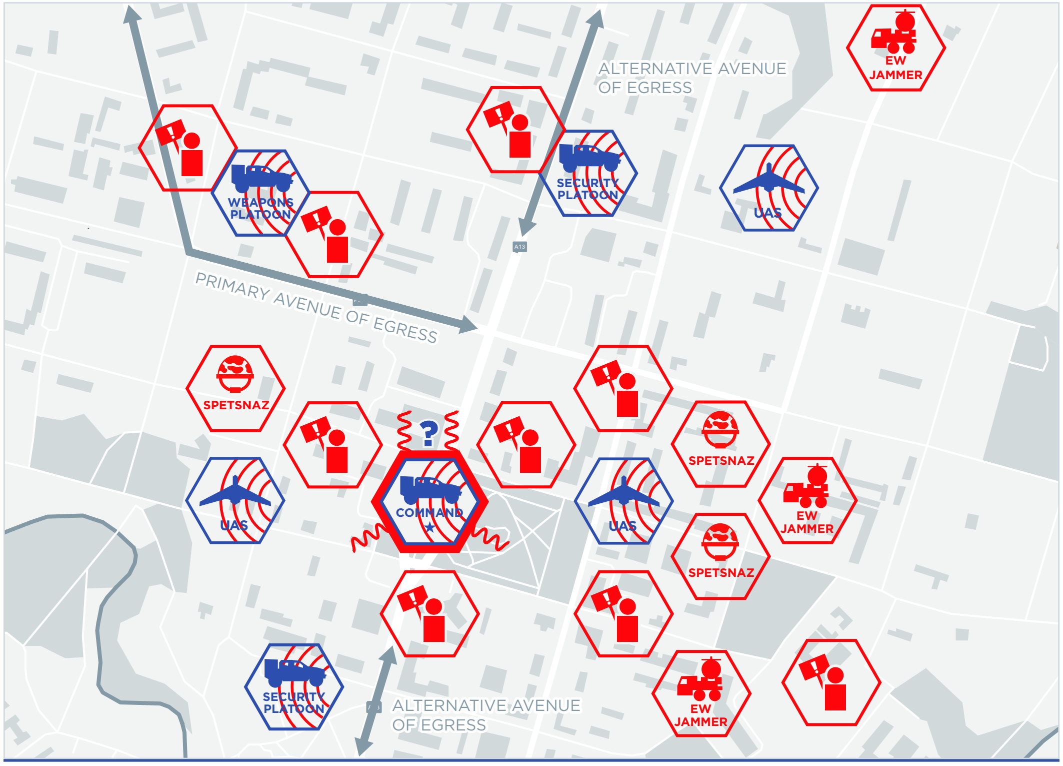
She and her Latvian counterpart strolled toward the plaza at the center of the city and chatted up the local police chief. Her translator began to interpret, but she didn't need him to get the gist: She understood the near-universal body language of the shoulder shrug, and sigh, "what are you gonna do?" affectation. She'd seen it the last 10 times they'd responded to calls like these. She wished that she and her troops were on better terms with their allies, but it was difficult to generate trusting relationships in just a year-long rotation, and her understanding of Latvian was limited to the basics.

To make matters worse, the Russians had done an excellent job driving wedges between the U.S. and Latvian forces. Among other things, they'd created social media profiles for male soldiers under her command, then leaked fake posts in which they bragged of their sexual exploits with the local women. It didn't help that the story certainly wasn't historically inconceivable—the Brits had complained that American GIs were "oversexed, overpaid, and over here," in World War II, for example. Either way, her chain of command had sent the soldiers in question home, but relations with her Latvian military counterparts and civilian authorities had been frosty ever since. It was frustrating, but she couldn't blame them. She'd have felt the same way in their place.

Approaching Rēzekne, she'd had her recon detachment launch four low-flying drones to give her situational awareness and ensure that she could record any potential incident. She radioed the detachment leader and asked him for an update. He came back and told her that the birds were up but malfunctioning. None of the birds was transmitting video or responding to commands, and one might have crashed—he was going to send a member of his squad to recover it. She told him to hold off. A little doubt crept out of her mind and into the pit of her stomach. Boredom and frustration gave way to a quick hit of adrenaline. These drones were pretty reliable. She might buy one or two malfunctioning simultaneously, but four at once? Wasn't the old saying, "Once is an accident, twice is a coincidence, and three times is enemy action?" Well, what about four times?

She turned to her radio telephone operator (RTO) and asked him

TACTICAL VIGNETTE IN RĒZEKNE, LATVIA



The Charlie Company commander's situation in Rēzekne.

to contact battalion headquarters outside Riga using satellite communications (SATCOM) and ask for an update on any suspected Russian activity in the area. The battalion intelligence officer had briefed her and her platoon leaders and senior noncommissioned officers about Russian covert and clandestine activities every couple weeks, but it wasn't in the briefing for this mission. Her unit's intel folks worked hard, but the Russians ran circles around them—particularly since the Latvians weren't very cooperative anymore. She'd actually written her senior thesis at West Point on how operations-intelligence fusion used in counterterrorism operations could be applied to countering unconventional coercion. She had floated the idea to the battalion commander and staff in a meeting once, and it went over like a lead balloon. She just dropped it. Now she was kicking herself for not pushing harder as she realized how little she really understood what was happening on the ground after being in Latvia for six months.

She turned back to her RTO. He couldn't raise anyone on SATCOM. He'd even tried the old trick of chucking a spool of antenna wire into a tree, like a teenager TP'ing a house on Halloween, to create a long-range very high frequency (VHF) antenna. Still nothing. He was restarting the radios, rechecking his frequencies and the aim of his antenna, and reloading his cryptography. He was the kind of kid who had checklists for his checklists; it was why she'd made him her RTO. He hadn't screwed up—someone was jamming their comms. She told him to keep trying to raise someone, anyone, on the net.

The nearest unit was Bravo Company—they were over 50 miles away down in Daugavpils responding to a similar protest there, while Alpha Company was back in Riga. Her mission didn't include dedicated air cover; why would it have? It was utterly routine. She looked up almost involuntarily in search of aircraft. Even if there were birds overhead, she was pretty sure her ultra high frequency (UHF) comms were jammed, too. Her RTO must have seen her scanning the sky, because he chimed in that he was getting nothing on UHF either.

The pressure of her situation pushed down on her chest as though her body armor had suddenly doubled in weight. Her company was totally isolated in a city that likely was thoroughly infiltrated by Russian intelligence and maybe covert Spetsnaz troops, some of whom now were jamming her comms. Her company was in JLTVs instead of their Strykers and not in full battle gear to avoid reinforcing Russian propaganda that NATO troops were an occupying force. Her Latvian allies probably saw her troops that way anyhow. She had no broader situational awareness, no air cover, and no means to call for any even if it were available. She felt unmoored. If her company were caught in an ambush, everyone down to the most junior private would know exactly what to do, but she had no past training or doctrinal template to guide her in this moment.

She'd read about the Russian concept of "reflexive control," or manipulating the adversary to make predictably bad decisions. At the time, she'd thought it sounded farcical and joked to herself that only an idiot could fall prey to something like that. She now realized how the Russians had played her, her battalion, and likely a host of other units by luring them into a false sense of security before rendering them deaf, dumb, and blind at the precise moment they were too far away to support each other. Her internal monologue was a series of increasingly vile expletives combined with statements of self-doubt. Externally, she tried to project the aura of calm and competence that she called "command face" and remembered something her mom used to tell her: "Fake it 'til ya make it."

The shattering of broken glass as a cobblestone collapsed a nearby storefront brought her back to the moment. It was simultaneously shocking and yet not surprising, like the sting of a punch she'd seen coming. The riot was turning violent, and she had a good idea of where this situation was headed. It was time to get out of Rēzekne.

Achieving Degradation Dominance in the Techno-Cognitive Confrontation

The preceding vignette paints a grim picture, and similar vignettes set in an INDOPACOM CAOC or forward Joint Task Force headquarters would perhaps be even more unsettling. Wargaming and analysis suggest that U.S., allied, and partner armed forces lack the concepts, capabilities, training, and proper organization to operate effectively against China or Russia with contested and degraded information and command systems. Time after time in CNAS wargames, U.S. blue teams found themselves untethered from the sensors, networks, and computer systems they relied on to perceive, process, and communicate their understanding of the operating environment. Surveillance; targeting; command, control, and communications; and critical logistics and sustainment networks all broke down and left them operating less effectively or more slowly than their red team opponents. These blue teams eventually adapted and found workarounds, but these responses generally were too little or too late to change the outcome of the conflict for the better.

Fortunately, the insights and lessons from these games, along with the computer modeling and simulation that accompanied them, point toward potential solutions to the challenges facing the DoD in the information and command. Based on these insights, the following section lays out a concept for how the DoD can achieve degradation dominance versus China and Russia. It begins by discussing how the DoD can use its information and command systems to force China and Russia into strategic and operational dilemmas. It continues by describing how the DoD must begin to push back on Chinese and Russian information operations to level the information playing field. Next, it describes how to achieve degradation dominance in the techno-cognitive confrontation of information and command systems in space, cyberspace, and the electromagnetic spectrum. Finally, it concludes with a series of specific recommendations at the joint, service, and domain level.

Force China and Russia into Dilemmas about Expanding or Escalating a Conflict

China and Russia would prefer to achieve their objectives without fighting, so a combat-credible forward posture that is closely linked with allies and partners must be the foundation of any military strategy or concept for deterring or defeating Chinese or Russian aggression. The *National Defense Strategy* contains a layered “Global Operating Model” that is a useful starting point.[70] In this construct, “Contact Layer” forces work by, with, and through allies and partners to contest coercion below the level of armed conflict. Forward “Blunt Layer” forces serve as a clear declaration of U.S. capability and intent, as well as the core of a force capable of denying or delaying Chinese or Russian aggression. Together, these layers raise the stakes for them by removing the possibility of uncontested coercion or limited acts of aggression. If China and Russia want to pierce the U.S. security perimeter, the DoD must be ready to make them pay for it dearly at every step.

Time after time in CNAS wargames, U.S. blue teams found themselves untethered from the sensors, networks, and computer systems they relied on to perceive, process, and communicate their understanding of the operating environment.

In the event of war with the United States, China and Russia want to fight the smallest possible counter-coalition. U.S. strategy and concepts therefore should force them to choose between broadening a conflict or leaving critical systems unharmed. This not only would increase the size of the conflict, but it also would increase its complexity, which would tax Chinese and Russian command and control. Advantageously exploiting these tensions should be central to U.S. military strategies and operational concepts for deterring or defeating Chinese and Russian aggression. Alongside allies and partners, the DoD should take steps that force China and Russia into dilemmas about: attacking in force, attacking a broad coalition of states, attacking kinetically, and attacking the U.S. homeland. Given the centrality of rapid, even preemptive attacks on information and command systems in Chinese and Russian thinking about warfare, these systems present an excellent opportunity to exploit these tensions, create dilemmas, and improve deterrence. There are myriad ways of achieving this effect, but four stand out from CNAS wargaming and analysis.

Limit the effectiveness of non-kinetic and reversible attacks. In CNAS wargames, Chinese and Russian red teams sought to avoid escalation by using reversible or temporary non-kinetic attacks on key information and command systems. Such attacks allowed them to achieve their operational goal of disrupting and degrading U.S. and allied systems with reduced risk of expanding or escalating the conflict. Limiting or interfering with their ability to assess the effectiveness of non-kinetic attacks might be particularly effective in this regard, as it would undermine their confidence in such attacks and encourage use of more definitive kinetic weapons. As will be discussed below, this approach could be particularly effective in space, where China and Russia are both reluctant to take aggressive kinetic action due to concerns about degrading the space environment and harming their own access to space.

Disperse information and command systems. A more dispersed posture would come with additional logistical burdens and a consequent loss of efficiency, but it would force China or Russia to attack a larger number of states that otherwise might have stayed out of a conflict. It has the added benefit of complicating Chinese and Russian targeting. This posture does not necessarily need to consist of combat forces, basing access for these often can be politically sensitive. Placing critical support facilities such as satellite ground stations in key states might be more feasible and still would present China or Russia with a dilemma: strike these facilities and potentially expand or escalate a conflict, or allow these systems to continue functioning.

Increase multilateral cooperation in key mission areas that would be high-priority targets for China and Russia. Cooperation could focus on critical areas such as space situational awareness, airspace awareness, maritime domain awareness, cyber security, electromagnetic spectrum management, and satellite communications. For example, China and Russia might be willing to attack U.S. military communications satellites, but they might be far more reluctant to attack an international constellation. The United States also could work through the so-called "Quad," which includes Japan, Australia, and India, to develop a cooperative maritime domain awareness (and antisubmarine warfare) coalition across the Indo-Pacific. The United States historically has been reluctant to enter into such agreements, as they can limit freedom of action. However, the strategic benefit of forcing China and Russia to attack broad coalitions would be more than worth the constraints and headaches of multilateral cooperation.

Force China or Russia into dilemmas about attacking the U.S. homeland. This seems counterintuitive, since the ultimate purpose of the DoD is to defend the American people, which would seem to preclude any action that might encourage an adversary to even consider attacking the homeland. However, moving critical systems to the homeland appeared to be an effective counter to Chinese and Russian attempts to limit the conflicts in CNAS wargames. The most interesting of these came when a Russian red team attacked the Combined Air Operations Center (CAOC) at Ramstein Air Base in Germany. The U.S. blue team rapidly shifted the CAOC to Pope Air Force Base in the same way that the U.S. Air Force's Central Command shifted its CAOC from al Udeid Air Base to Shaw Air Force Base in 2019.[71] This move perplexed and frustrated the red team, since they wanted to disrupt or degrade the U.S. ability to command and control air forces in the European theater, but they were wary of the potential escalation caused by striking so deep into the U.S. homeland. Moving critical information and command facilities from Hawaii to the continental United States when needed might give pause to Chinese planners in a Pacific scenario. When combined with actions to limit the effectiveness of non-kinetic attacks, such moves could leave adversaries with few good responses, all of which may be risky or carry deleterious side effects.

Level the Playing Field in the "Peacetime" Information Environment

Chinese and Russian information operations pose a "Catch-22" for U.S. military strategists and operational planners. On one hand, they cannot ignore these operations, since they are so central to how China and Russia are confronting the United States and its allies and partners today, as well as how they might fight a U.S.-led coalition in the future. On the other hand, the DoD historically has eschewed these activities, particularly in "peacetime," and faces significant cultural, organizational, and sometimes legal hurdles in shifting this perspective.[72] China and Russia have exploited this gap to tilt the information playing field to their advantage. While the DoD is not solely responsible for filling this gap, if it continues to remain on the sidelines and treat information confrontation as a sideshow to kinetic military operations, it will find itself at a severe disadvantage when war comes. Or worse, China and Russia may achieve their objectives without firing a shot.

Any concept for countering Chinese and Russian information and command concepts must therefore include the DoD playing a larger role in the U.S. government's response to Chinese and Russian information warfare. However, this role must acknowledge organizational and legal constraints, as well as the fact that "peacetime" information operations in foreign theaters are unlikely ever to be the DoD's core competency. The DoD therefore should act predominantly as an enabler and a "systems integrator" for the efforts of allies, partners, and other U.S. government agencies.

> **Any concept for countering Chinese and Russian information and command concepts must therefore include the DoD playing a larger role in the U.S. government's response to Chinese and Russian information warfare.**

Chinese and Russian information operations are broad and touch on myriad aspects of inter-state competition and confrontation outside of military affairs. Given resource and legal constraints, the DoD cannot and should not attempt to counter every aspect of these operations. Instead, it should target its information operations on sustaining alliance or coalition cohesion, enhancing situational awareness, and positively influencing public opinion regarding U.S./coalition forces and operations. The following five lines of effort would enable the DoD to level the information playing field without requiring it to eschew its core competencies.

Gain the proper authorities and de-conflict with other government agencies. Working with Congress to obtain the proper authorities to conduct peacetime information operations is the first step in leveling the information playing field. Absent clear legal authorization and oversight now—well in advance of a crisis—the remaining aspects of this concept are unfeasible. These authorities should allow for greater cooperation and information-sharing between the armed forces and the intelligence community to maximize situational awareness in the information environment and minimize the risk of "information fratricide," in which military and intelligence information operations work at cross purposes.

Train and prepare for information confrontation with China and Russia. To deal with information confrontation, U.S. and coalition forces must gain a cognitive advantage by preparing for these operations just as they would prepare for typical combat operations. All U.S. military personnel should receive basic education in identifying misinformation, and threat-specific training upon deploying. Personnel at all levels should use virtual and synthetic training to develop their cognitive skills and their ability to sift good information from bad and rapidly make decisions with imperfect information. Unit commanders and high-level staff should conduct repeated exercises and wargames against red teams versed in reflexive control and psychological manipulation. Combined training with allies and partners should include realistic representations of psychological operations across the strategic, operational, and tactical levels of warfare. This will require a greater emphasis on regional expertise and knowledge of local conditions and actors.

U.S. and coalition forces should prepare to exploit and attack these operations—not simply counter them defensively. U.S. and coalition information operations should use Chinese and Russian aggressiveness in the information environment against them by luring them into blind alleys that negate their operations, or into bad decisions that expose their perfidy and belligerence. The DoD is conducting some operations like this today—CNN's coverage of P-8A patrols in the South China Sea has exposed Chinese bellicosity to a broader audience, for instance—but they are piecemeal and seemingly uncoordinated.[73] U.S. and coalition forces should develop detailed understandings of Chinese and Russian cognitive tendencies and prepare to use these to manipulate their counterparts well in advance of an actual conflict. Once the conflict has begun, it's too late to get inside the opponent's head.

In addition to training and education, the DoD should look to develop—or more likely acquire from commercial vendors—software systems that automatically help identify patterns in adversary information operations. While such technology would not be a substitute for good judgment developed through proper training and education, it might enable commanders to understand the information environment and identify attempts at deception or reflexive control more quickly.

Leverage allied and partner expertise with Chinese and Russian information operations. Allies and partners must be central to U.S. information operations against China and Russia. First, these operations take place largely in their territory and with their populations as a key audience; their full-throated cooperation is therefore a prerequisite. Second, U.S. allies and partners are on the front lines of information confrontation with China and Russia and have been for decades, if not longer in many cases. They possess a depth of knowledge, experience, and familiarity with Chinese and Russian approaches that U.S. armed forces cannot hope to match. U.S. armed forces therefore should play the role of enablers through technical and financial assistance where necessary, and as a theater-wide systems integrator in the Indo-Pacific, which lacks a ready-made body for coordination such as NATO.

The first aspect of this collaborative coalition approach to information operations is to sustain and enhance trust and cohesion in alliances and partnerships. Weakening these relationships is at the forefront of Chinese and Russian information operations because they recognize how dependent U.S. armed forces are on allies and partners for basing access, overflight, information sharing, logistic support, and force contributions.[74]

This emphasis on cohesion and mutual trust is even more important within the context of this concept and the broader thrust of the 2018 *National Defense Strategy*. This concept recommends taking actions that would force China or Russia to expand or escalate a conflict under the belief that the threat of fighting a larger coalition would serve to deter aggression. While this notion is a longstanding aspect of military alliances and coalitions, it is discordant with the history of the post–Cold War era. For almost 30 years, U.S. military dominance provided most allies and partners, and particularly NATO allies, with defense and deterrence with minimal risk of attack. Moreover, the DoD increasingly concentrated U.S. forces and facilities in a handful of countries like South Korea, Japan, and Germany. Moving forward, the DoD needs to posture forces in more states, with the express purpose of putting U.S. forces and host populations at risk. Explaining how, paradoxically, this will make these states safer from aggression will require close cooperation and clear and consistent messaging.

At the same time, the NDS is shifting the weight of U.S. overseas presence operations from focusing on assuring allies toward deterring China and Russia. This shift may seem semantic, but it already has impacted U.S. forward posture, with the cessation of the Air Force's continuous bomber presence on Guam being a prime example. This move makes sense from a deterrence perspective, as it shifts key strategic assets out of Guam, where they might be vulnerable to a Chinese first strike, and allows them to deploy more flexibly, thereby increasing the potential for operational surprise. However, the move could undermine U.S. INDOPACOM's ability to assure allies that these forces would come to their defense. U.S. information operations will be critical to explaining this action and thwarting any Chinese attempt to use it to drive a wedge between the United States and its allies and partners in East Asia.

Align information operations with military operations. This leads directly to the next point—generating the trust necessary for cohesive coalition operations requires closely aligning military operations and information operations in both peacetime competition and conflict. China, Russia, and any anti-U.S. forces in allied and partner nations will ruthlessly exploit any gaps between U.S. words and deeds to foment mistrust and erode the cohesion necessary for effective coalition operations. While surprise, secrecy, and operational security cannot be ignored, clear, consistent messaging about strategic commitment closely linked to actions that credibly demonstrate resolve are key to keeping allied and partner governments and their military forces committed to the common cause. This linkage between message and action will have to be particularly creative, since huge portions of the fight—such as cyber, space, electronic warfare, stealth aircraft, and undersea warfare—might be mostly or wholly invisible to U.S. allies and partners.

Avoid civilian casualties. Finally, U.S. and coalition forces should make every effort to avoid civilian casualties. In CNAS wargaming, Chinese and Russian red teams both highlighted and exaggerated civilian casualties to erode support for the coalition war effort. The outcome of these stratagems in CNAS games was not decisive; however, it is easy to imagine how gruesome images might sap the fighting spirit of allies and partners whose populations may already have been lukewarm toward intervention. Should conflict erupt, U.S. and coalition rules of engagement do not need to be as restrictive as U.S. forces have become accustomed to during the post-9/11 wars, but nor should commanders possess a carte blanche.

Achieve Degradation Dominance in the Techno-Cognitive Confrontation in Space, Cyberspace, and the Electromagnetic Spectrum

The PLA and Russian Armed Forces have spent the last two decades thinking about, investing in, developing, and exercising ways and means to attack the system-of-systems that enabled the U.S. armed forces' overwhelming victory in the Gulf War of 1990–91. They brandish these weapons in hopes of convincing the United States (and its allies and partners) that intervention in their affairs is either bound to fail or unlikely to be worth the enormous costs. This threat is eminently credible because, as outlined above, the system-of-systems underpinning U.S. information and command capabilities is inherently vulnerable in certain critical areas. If this deterrent threat fails, their ability to attack U.S. systems in space, cyberspace, and the electromagnetic spectrum will rapidly give them an advantage in information and command, and with it a window of opportunity to seize their strategic objectives before the United States and its allies and partners can respond. U.S. armed forces need a concept for gaining and maintaining an advantage in the techno-cognitive confrontation, and can look to relatively recent history for a guide.

In 1992, following the Gulf War, an Indian general is purported to have said, "Never fight the U.S. [sic] without nuclear weapons."[75] Had he made that comment just 15 years before in the aftermath of Vietnam, he could have said, "Never fight the U.S. except at night." This notion seems strange today, since U.S. armed forces pride themselves on their night-fighting prowess. However, night fighting was a persistent U.S. weakness at the outset of World War II against the Imperial Japanese Navy, in the Korean War against North Korean and later PLA troops, and in Vietnam against the Vietcong and the North Vietnamese Army.[76] Fighting skillfully at night allowed these adversaries to evade U.S. advantages in airpower and firepower. Like the PLA and Russian Armed Forces today, these adversaries saw the Achilles' heel in U.S. military power and exploited it effectively.

Following the Vietnam War, the DoD decided that henceforth it would own the night. By combining technology (night vision), doctrine, organization, and training, U.S. armed forces evolved into arguably the world's premier night-fighting force. In fact, from the Gulf War onward, U.S. forces have *preferred* to fight at night despite the difficulties it entails, because their advantage over adversaries in the dark is so great.[77] This shift presented U.S. adversaries with a dilemma: fight the United States during the day and expose oneself to U.S. air and firepower superiority, or operate at night and expose oneself to U.S. night-fighting superiority.

To prevail in modern warfare, the DoD needs to initiate a similar paradigm shift in the techno-cognitive confrontation for information and command. This confrontation is predominantly taking place in three domains—space, cyberspace, and the electromagnetic spectrum—where offense predominates over defense. And yet the DoD's current concepts and capability investments largely focus on sustaining and defending extant systems, often at exorbitant costs for little benefits. Shifts are under way—witness the emphasis on resilience vice survivability in the *National Defense Strategy* and consequent programmatic developments. However, they are piecemeal and still oriented around a focus on sustaining current methods and concepts predicated on widespread, high-bandwidth connectivity—witness the focus on "connecting every sensor to every shooter" within the JADC2 program.[78] Put another way, the DoD is still trying to keep the lights on, when it needs to be willing to turn out the lights and operate in the dark. This is easy to write, but difficult to implement. The remainder of this section outlines concepts and capabilities that—based on CNAS wargaming and analysis—could enable a new joint method of operating focused on achieving dominance with degraded information and command systems-of-systems.

Enable people and build trust across command echelons, organizations, and with critical systems. To gain degradation dominance, the DoD must focus on enabling its people and building trust across command echelons, organizations, and with critical information and command systems. This is not to argue that the DoD should embrace Luddism and avoid technological competition, but rather that it must view this competition through the lens of leveraging—rather than ignoring or obviating—its advantages in human capital. This may seem counterintuitive, given the technical aspects of the techno-cognitive confrontation, but several points from preceding sections bear repeating. First, like past adversaries that fought U.S. forces at night, China and Russia believe they could gain an advantage in certain technological aspects of the techno-cognitive confrontation. Second, China and especially Russia would use a technical advantage in the techno-cognitive confrontation as a way of disrupting U.S. forces cognitively and psychologically. Put another way, China and Russia see U.S. forces' dependence on technology as a strength that they can turn into an exploitable cognitive and psychological weakness. Third, China and Russia view the quality of their personnel relative to the U.S. All-Volunteer Force as a persistent shortcoming, and are seeking technological means to overcome this disadvantage. Collectively, these adversary actions suggest that the DoD must figure out how to use technology to defend and extend its human/cognitive advantage, rather than see technological achievement as an end in itself.

Adopt policies and demonstrate capabilities to proportionally attack Chinese and Russian information and command systems. China and Russia want to leverage their counter-information and command systems for coercion in competition, and to disrupt U.S., allied, and partner forces systemically in the event of a conflict. By doing this quickly, aggressively, and in some cases preemptively, China and Russia hope to gain a nearly insurmountable advantage in the information environment before their adversaries can respond. China and Russia also have taken steps to defend themselves against the possibility that U.S. forces would launch similar attacks against their information and command systems. Both have invested in creating resilient command-and-control systems featuring hardened, buried, and air-gapped fiber-optic networks with redundant C2 nodes.[79] They also have intentionally mixed nuclear and conventional forces in critical areas to create ambiguity and thereby potentially deter attacks on those forces or, more germane here, their information and command systems.[80] Put simply, China and Russia want to render U.S., allied, and partner forces deaf, dumb, and blind while making it difficult or extremely risky to do the same to their forces.

This situation presents a conundrum for U.S. forces. They cannot hope to deter conflict or prevail without credible means of attacking Chinese and Russian information and command systems. At the same time, operational concepts for defeating China and Russia cannot rest on a strategically untenable approach. This tension cut to the heart of the "blinding campaign" that was central to AirSea Battle, which was the first major, public operational concept to describe how to fight the modernized PLA. The blinding campaign envisioned widespread kinetic attacks on Chinese "battle networks" (i.e., information and command systems), many of which are located deep inside mainland China.[81] While operationally sound, this approach wasn't credible strategically, as U.S. political leadership would rightly be reluctant to move so aggressively against Chinese (or Russian) territory early in a conflict.

Solving this conundrum requires a mix of policies and capability demonstrations. First, the United States should issue a declaratory policy that it will respond proportionally, although not symmetrically, to any attacks on its information and command systems. This policy would authorize targeting of any adversary systems involved in these types of attacks, regardless of location or commingling between nuclear and conventional systems. Crucially, this policy would not proscribe other attacks on Chinese and Russian information and command systems, but it would put the onus of escalation on them by clearly signaling U.S. intent to respond proportionally. China and Russia could then choose to attack U.S., allied, and partner systems—and thereby open themselves to attacks—or restrain their actions and limit their vulnerability.

Such a policy is not without risks and downsides. The first is that the policy would not be credible. Capability development and targeted demonstrations—particularly of less-escalatory non-kinetic weapons—would be critical to ensure that China and Russia believe U.S. threats. Even if they do not completely believe this threat, Chinese and Russian military planners likely will have to factor it into their calculus in ways that may induce doubt and contribute to deterrence. Second is a risk of escalation, although this risk already exists even without such a policy. Chinese and Russian strategy and operational planning already assume that U.S. forces will attack their information and command networks. Making this policy clear actually might reduce the risk of escalation through miscalculation, as China and Russia would understand the consequences of their actions. Third is the possibility that this grants control over the scope, scale, and tempo of a conflict to China and Russia. Since this paper—based on U.S. strategy and planning—assumes that China or Russia would initiate any conflict with the United States, they arguably already have a great deal of control over a putative conflict's course and contours. Moreover, the policy would not proscribe other actions—it would just threaten proportional responses to any Chinese or Russian actions. The key is that China and Russia clearly understand that there would be no plausible scenario in which the United States would allow them to render its armed forces deaf, dumb, and blind, while their armed forces enjoy uncontested use of their information and command systems. Either both sides fight in the light, or both sides fight in the dark.

Develop the ability to operate "loose" to fight effectively in degraded and contested conditions. The DoD must prepare to fight with degraded information and disrupted command systems. Even with this declaratory policy and demonstrated capabilities, it is likely that China and Russia would still threaten to, or actually attack U.S., allied, and partner information and command systems. There is no plausible scenario in which U.S. forces enjoy the sort of information dominance they had in the Gulf War or any of the post–Cold War conflicts to date.

At the same time, there is a growing consensus across the DoD that future warfighting concepts will require greater integration and coordination across all warfighting domains and armed services. Whether one adopts the of-the-moment phrases "multi-domain operations," or "all-domain operations," or simply sees this as the next iteration of joint or combined-arms operations, the imperative is clear. The side that can synchronize and coordinate actions across multiple domains to create multiple dilemmas for the adversary likely will have a significant operational advantage. The ability to use effects from multiple domains makes operations more difficult to defend, more resilient to countermeasures, and more likely to induce cognitive or psychological disruption in target forces. CNAS wargames and analysis did not prove this hypothesis, but they indicated that it could be effective in warfighting scenarios against China or Russia.

The imperative to adopt more integrated joint or multi-domain operations raises two paradoxes for information and command. The first concerns echelons of command. The joint command and control necessary to execute these sorts of operations has existed at higher echelons of command—often three- or four-star joint task forces or Geographic Combatant Commands. This reflects a long-standing aspect of military command: The greater the scope and complexity of operations, the higher the echelon of command and the larger staff structure it requires. These higher echelons of command will have to manage rapid, dispersed, multi-domain operations with contested communications while under kinetic and non-kinetic attack. Creating and disseminating a common operating picture and commander's intent fast enough to maintain pace with the tempo of operations will be a monumental task under these conditions.

Simultaneously, however, future great-power warfare is likely to have an extremely rapid operational tempo and, as previously mentioned, highly contested information environments. Moreover, the lethality and range of modern weapons is pushing armed forces on all sides—but particularly the United States—toward increasingly dispersed and non-linear operations in which there is no contiguous “front line,” but rather pockets of forces and combat distributed widely in time and space. In this environment, dispersed tactical echelons of command may lack reliable long-haul communications to higher echelons or even adjacent or supporting units that may be quite distant or in different domains and chains of command.

This creates a paradox that, if left unresolved, could be unfavorable to U.S. forces. The complexity of multi-domain operations will tend to push control and coordination higher up the chain of command, while the need for high tempos and the contested information environment will tend to push initiative toward lower echelons at the tactical edge. Since U.S. forces will be operating in a dispersed posture on exterior lines and rely more heavily on long-range RF and satellite communications than either Chinese or Russian forces, this challenge will be more pressing for U.S. forces than their opponents.

The second paradox regards the communications demand of multi-domain operations. Advocates of this type of warfare often speak of “linking every sensor to every shooter” so that the entire joint force functions as a massive, dense network or “kill web” that can rapidly and efficiently allocate the right sensor and weapon for every target. It is a compelling vision that could be quite effective. However, it relies on a level of persistent, long-range connectivity and data sharing, as well as rapid decision-making that may not be possible in the context of a techno-cognitive confrontation with China or Russia. Chinese and Russian forces would contest these communications or exploit the signals for surveillance and targeting. Furthermore, if the DoD connects every sensor to every shooter through radio communications, any penetration or exploitation of this network could give Chinese and Russian forces a granular understanding of the U.S. order of battle in the theater.

These paradoxes call into question current DoD concepts, as well as the intellectual foundation underpinning emerging concepts and programs. Illustrating this more clearly requires deeper analysis of a specific operational challenge. While there are many challenges within the techno-cognitive confrontation, the need to strike large numbers of mobile and relocatable targets inside highly contested environments has proven the most salient in CNAS wargames and analysis. This challenge demanded that U.S. blue teams coordinate and synchronize effects from multiple domains and pushed them to adopt a number of adaptations collectively defined as “loose” operations, to differentiate them from current methods, defined as “tight” operations.

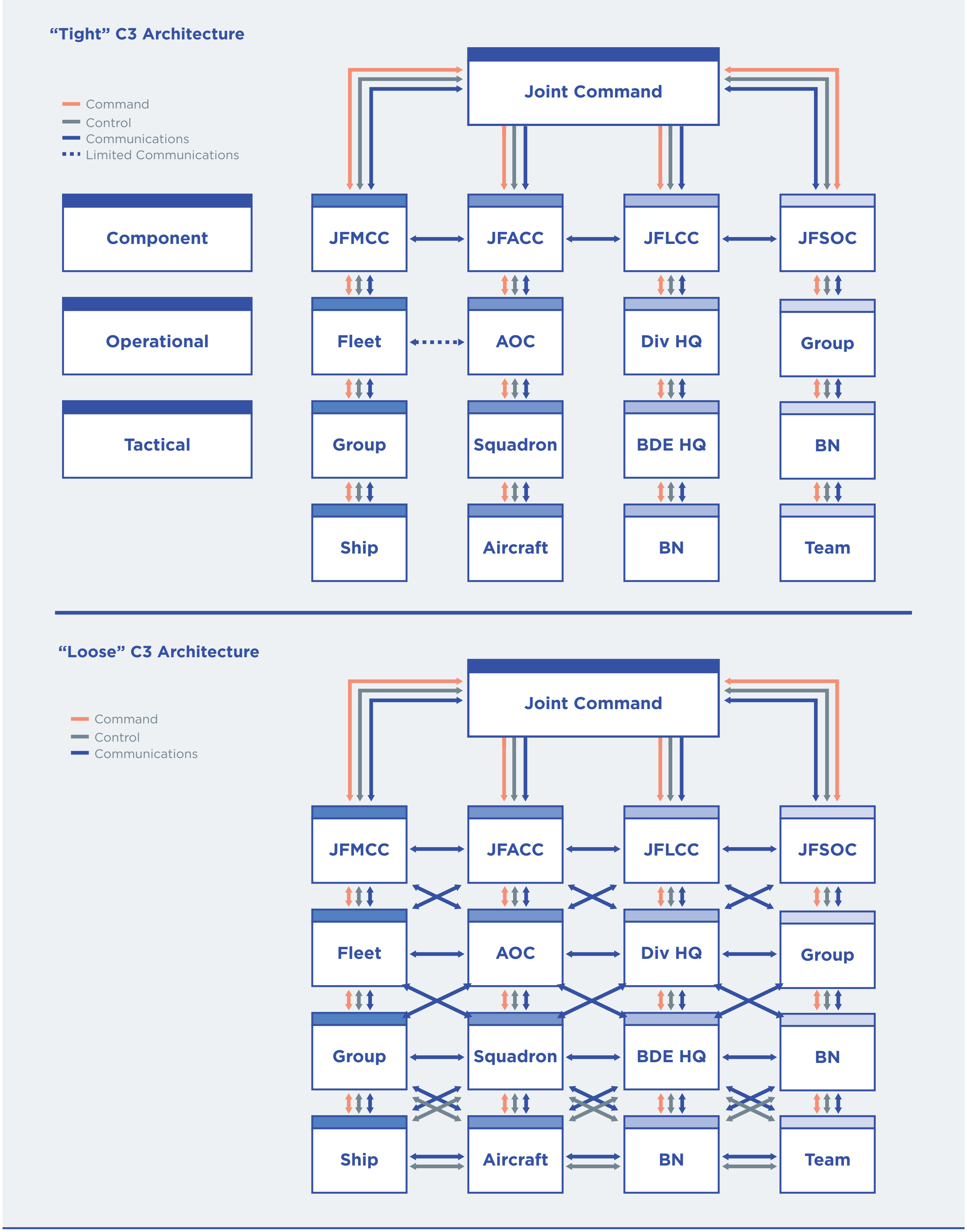
Operating loose is a fundamental shift for the DoD after decades in which operations became ever more tightly controlled and precise. It entails accepting degradation and designing it into concepts, doctrine, plans, and programs, rather than attempting to design it out. It is a move away from defending or increasing the survivability of current systems, and toward designing resilient, mission-oriented, federated systems. This way of operating sacrifices some efficiency and potentially accepts greater attrition to weapons and platforms to enable commanders to make “good enough” decisions much more quickly than the adversary. In many ways, it is the Pareto Principle—80 percent of the outputs come from 20 percent of the inputs—applied to warfare.

Crucially, loose operations maintain unity of command, but they envision changes to how commanders control subordinate forces. Technological developments over the last several decades—including high-bandwidth satellite communications and

COMPARING TIGHT AND LOOSE OPERATIONS

Attribute	Tight	Loose
Paradigm	Prevent degradation, efficient, precise	Operate degraded, resilient, rapid
Command	Unified, directive, instructive	Unified, mission, shared picture & intent
Control	Hierarchical, centralized, defined	Peer-to-Peer, decentralized, content-based
Span	Fixed, based on echelon	Fluid, based on reliable comms
Comms	Hierarchical, linked to control	Mesh, cross-matrixed, ad hoc
Targeting	Precise	Sufficient
Sensors	Few, exquisite	Many, expendable
Security	Trusted networks	Trusted entities
Cyber	Network, internet protocol, strategic	Off-net, RF, tactical
Space	Large, expensive, GEO, government	Small, affordable, LEO, commercial
RF	Omni-directional, voice	LPI/LPJ, directional, data bursts
PNT	Space-based (GPS)	Alternatives to space

TIGHT AND LOOSE C3 ARCHITECTURES



These charts contrast the current "tight" C3 architecture, in which command, control, and communications are tightly linked, against a loose structure that allows for more flexible and resilient operations in contested environments.

full-motion video ISR—have made possible an unprecedented degree of remote micromanagement of military operations.[82] The so-called "10,000-mile screwdriver" has accustomed commanders and subordinates to a degree of connectivity, direction, and oversight that arguably has undermined operational and tactical initiative.[83] Constant, high-bandwidth connectivity is very unlikely to exist in a conflict with China or Russia, and even if it did, using it to wield a 10,000-mile screwdriver would constipate decision-making.

Instead, U.S. commanders must make greater use of mission command and other forms of decentralized and delegated command philosophies such as command-by-negation, at least in contested environments.[84] Despite officially being "the preferred method of exercising C2," according to the joint staff, there is ample evidence that mission command is not the dominant command philosophy for U.S. armed forces.[85] While proponents of mission command such as Donald Vandergriff have long pushed for its adoption by U.S. armed forces, the operational demands of warfare with China or Russia—and particularly the techno-cognitive confrontation for information and command—make it imperative.

Within the context of "loose" operations, mission command allows for effective, decentralized control at lower echelons, which maintains initiative, speed, and resilience to degraded communications. Freed from exercising direct control over subordinates, higher echelons can focus on winning the techno-cognitive confrontation, developing and disseminating a more accurate operational picture, and allocating scarce operational resources.[86]

Loose operations require decentralized networks to pass information between systems, especially sensors and "shooters" from multiple domains and armed services. Current military communications networks are largely "stovepiped," with communications closely linked to service- or domain-specific lines of command-and-control authority. Today, joint integration of these networks occurs either at high echelons of command or on unique systems such as the Battlefield Airborne Communications Node, or BACN, which is an aircraft that enables networks using different frequencies and waveforms to share data. In essence, these aircraft serve as "universal translators" for DoD communications networks.

To achieve loose communications networks, the DoD should widely distribute this universal translator function across the joint force to create "Rosetta Stone" networks that could pass data freely using multiple paths across service, domain, and waveform boundaries. This would shift the DoD from a network-centric communications architecture toward a network-agnostic, data-centric architecture. This type of systems architecture would enable the DoD to create resilient mesh networks on the fly, connecting every sensor to every shooter across multiple pathways. Such a loose network would be more resistant to jamming and potentially would be able to share data at long ranges without persistent access to space.

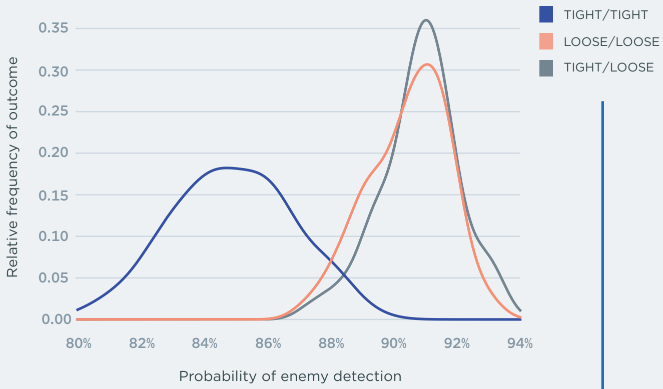
Fully exploiting mesh, ad hoc communications networks to enable true multi-domain operations also likely will require decentralized, peer-to-peer control of forces across domain and organizational boundaries. CNAS modeling and simulation suggest that altering methods of control to enable, for example, Air Force fighters to directly task Army long-range fires can increase effective weapons delivery against mobile and relocatable targets in contested environments. This decentralized, peer-to-peer control model could make tactical forces much more flexible, agile, and resilient by reducing the need to constantly route requests from one tactical unit up through a service chain of command to joint headquarters, then back down a second service chain of command to another tactical unit.

> **The DoD should create 'Rosetta Stone' networks that shift it from a network-centric communications architecture to a network-agnostic, data-centric architecture.**

As seen in the graphs to the right, loose communications (mobile, ad hoc networks, or MANETS) and control structures (content-based control) could increase the effectiveness and resilience of U.S. armed forces in one of their most difficult operational challenges: finding and attacking mobile forces in highly contested environments. In this case, the modeling examined attacking Russian ground forces in eastern Latvia. However, the broad contours of this analysis likely would apply—with obvious caveats—to attacking PLA transports and ground forces ashore in a Taiwan scenario, since both involve large numbers of mobile targets in cluttered environments characterized by contested air, space, cyberspace, and electromagnetic domains.

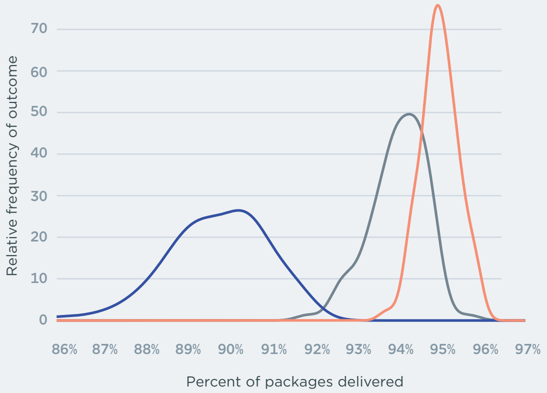
While loose structures offer benefits in certain operational challenges, the chart below suggests that they do not confer significant benefits in striking fixed targets such as ports and airfields. Moreover, CNAS wargaming and research strongly suggest that higher echelon commanders still will wish to exert direct control over

MODELING COMBAT OUTCOMES FROM TIGHT AND LOOSE ARCHITECTURES



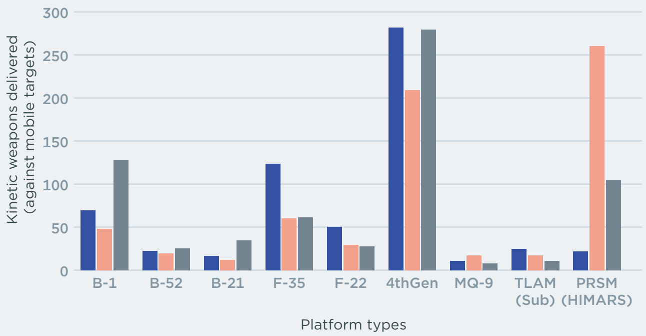
Enemy Detection Rates

This graph represents a probability density function—or the relative likelihood of a given outcome across thousands of model runs—along the y-axis, and the percentage of enemy targets sensed along the x-axis. Both "loose" models outperformed the current "tight" hierarchical model by sensing a greater percentage of enemy forces more frequently with a lower standard deviation. (Source: Group W)



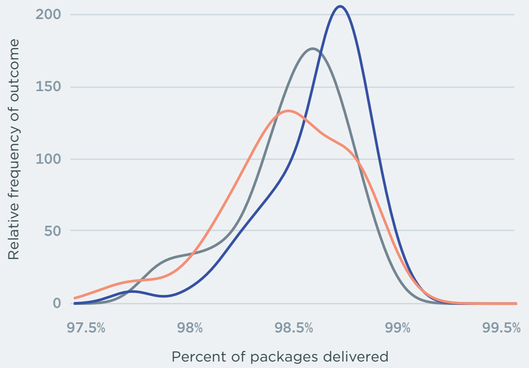
Kinetic Mobile packages Delivered

The above graph has a probability density function on the y-axis, but this time the x-axis denotes the percentage of munitions delivered on target. Both loose systems outperform the current, hierarchical C3 system. (Source: Group W)



Kinetic Mobile Weapons Delivery by Platform

Using standard, hierarchical C3, tactical aircraft carry almost 75 percent of the weapons delivered to mobile targets in a contested environment. (Source: Group W)



Kinetic Strikes on Fixed Targets

Hierarchical C3 still functions well against fixed targets, suggesting there may not be a single dominant model, but rather a need to shift flexibly between tight and loose structures as dictated by missions and conditions. (Source: Group W) critically scarce assets and actions with strategic consequences and risks of escalation. In CNAS games, for example, commanders were willing to operate "loose" against Russian ground forces and PLA forces in the Taiwan Strait, but were "tighter" when attacking fixed targets in Russian or Chinese territory, or when using hypersonic missiles or other scarce weapons.

This finding suggests that there likely will not be a single dominant operational paradigm in future warfare with China or Russia. Instead, the side that is able to operate tight and loose flexibly or even simultaneously depending on missions and conditions is likely to have a significant advantage. The ability to fluidly shift operating models and structures in this way will demand flexible and adaptable personnel and organizations, and realistic training to make these shifts as seamless as possible. These are all areas in which U.S. armed forces enjoy persistent, if not structural advantages over Chinese and Russian armed forces.

In addition to these communications and control architectures, loose operations in CNAS wargames adopted different ISR and targeting concepts to create sufficient, rather than exquisitely precise, targeting solutions. The impetus behind this shift was the tendency of Chinese and Russian red teams to present large numbers of relatively low-value targets in highly cluttered environments mixed in with large quantities of decoys, jammers, and air and missile defenses capable of shooting down platforms and munitions. Rather than fuse a large "stack" of intelligence sources from multiple domains to create a targeting solution for a small number of very precise (but expensive) weapons, teams relied more heavily on attritable unmanned aerial systems (UAS) and unattended ground sensors to create area targeting solutions, then blanketed a "kill box" with relatively affordable area-effects weapons such as cluster munitions. The teams anticipated a certain amount of attrition and weapons wastage, but calculated these would be more than offset by the sheer volume of destructive power they could bring to bear against these area targets. The DoD will have to scope this kind of "loose" targeting system through rules of engagement and risk/reward tradeoffs to ensure that it avoids excessive collateral damage and civilian casualties.

During counterterrorism and counterinsurgency operations in Iraq and Afghanistan, U.S. special operations forces (SOF) found that existing targeting processes such as "find, fix, track, target, engage, assess," (F2T2EA) were too slow, methodical, and insufficiently capable of exploiting the fleeting intelligence opportunities created by a successful attack. In response, SOF integrated targeting and intelligence into a more rapid, cyclical process they dubbed, "find, fix, finish, exploit, assess, disseminate," or F3EAD.[87] While this exact process may not be appropriate for conflict with China or Russia, the DoD should experiment with how to leverage rapid, cyclical targeting processes like F3EAD to enable faster, more flexible, and decentralized targeting of enemy forces in contested environments using degraded information and command systems. The current, centralized, staff-intensive process of F2T2EA within the context of a 72-hour air tasking order simply won't suffice given the chaos and pace of future combat with China or Russia.

By design, the concept of operating "loose" places a great deal of responsibility in the hands of lower echelons of command. The idea of hyper-enabled tactical multi-domain forces operating under a decentralized, peer-to-peer control system is compelling for many reasons. It could accelerate U.S. decision cycles, improve the ability of U.S. forces to rapidly and flexibly apply capabilities from multiple domains, and center the techno-cognitive competition with China and Russia in an area of persistent U.S. advantage: the skills, critical thinking abilities, and initiative of U.S. personnel. At the same time, pushing these responsibilities to lower echelons will enable operational commanders to focus on winning the techno-cognitive confrontation and managing a broader campaign, vice micro-managing tactical decisions.

> **The DoD should conduct experiments and technology demonstrations that explore the use of artificially intelligent systems and networks, as well as increasingly autonomous weapons platforms, sensors, and weapons within 'loose' operations in contested and degraded environments.**

There is one obvious downside: tactical forces have to dedicate enormous cognitive bandwidth to their primary function—attacking the enemy and evading the enemy's attacks. One reason that cognitive staff functions reside in rear areas is that the relative absence of immediate danger allows personnel to focus on staff work and battle management, vice operating a weapons system. Pushing some of these functions to lower levels could increase responsiveness and flexibility, but only if personnel at those echelons are capable of managing the cognitive load. The answer cannot be to create miniature "staffs" to manage these processes for tactical commanders—they will have to happen automatically.[88]

Toward this end, the DoD should conduct experiments and technology demonstrations that explore the use of artificially intelligent systems and networks, as well as increasingly autonomous weapons platforms, sensors, and weapons within "loose" operations in contested and degraded environments. The goal of these experiments should be to determine how the DoD can use technology to: 1) enable loose operations; 2) improve decentralized, peer-to-peer communications and control regimes; 3) allow for smooth transitions between tight and loose operations; and 4) enable lower echelon forces to access multi-domain capabilities and unmanned systems without distracting from their primary combat functions.

Chinese and Russian military decision-making processes depend to a great extent on detailed calculations of the regional correlation of forces. Likewise, their initial operations would rely heavily on predetermined and pre-targeted attacks on critical U.S. and allied systems with an eye toward quickly shifting the correlation of forces to their advantage. U.S. rules of engagement may preclude aggressive operations to degrade Chinese and Russian targeting systems prior to the onset of hostilities, and even after combat begins, some systems may be risky to target. Within this constraint, military deception is an important way of gaining an information advantage in the techno-cognitive confrontation, deterring adventurism, and achieving degradation dominance in conflict.

While there are myriad forms of military deception, the DoD should focus its energies on means and methods of systemically deceiving Chinese and Russian cognitive processes by attacking automated, artificially intelligent, or other algorithmically enhanced systems. China and Russia both are pursuing these sorts of systems to enhance their ability to make sense of their operating environment and make rapid, data-driven decisions, sometimes with minimal human oversight. Former Deputy Secretary of Defense Robert Work has described the competition between these systems as "algorithmic warfare," and has suggested that it will be a critical component of modern combat.[89] Developing means to degrade China and Russia's ability to trust these systems could have profound impacts on perceptions of the military balance, deterrence, and combat outcomes.

Organize and train for degraded multi-domain operations. Coordinating operations across multiple domains in contested environments also will require different command structures from Geographic Combatant Commands down to the tactical echelon. The following organizational changes all are designed to improve the ability of U.S. armed forces to gather, transmit, process, and act on information more quickly and effectively in highly contested or degraded environments than Chinese and Russian armed forces. To accomplish this, they focus on instilling familiarity and trust across current organizational barriers, devolving and decentralizing control to lower echelons, and organizing around effective information sharing.

The first, and likely most controversial change, would be to put combat back in the Geographic Combatant Commands. Over the last 30 years, the combatant commands—and particularly U.S. European and U.S. Indo-Pacific commands—have evolved from standing joint operational staffs to become broader military-diplomatic organizations. Setting aside the reasons for this shift, it has decreased these commands' focus on operational planning, command and control, and joint concept development.[90]

At the same time, and perhaps not coincidentally, the DoD has increased the use of ad hoc joint task forces to respond to crises or conduct ongoing operations.[91] While these organizations provide a great deal of command flexibility, their ad hoc structure decreases the trust and familiarity necessary to operate effectively against capable opponents in contested or degraded environments. Put simply, the DoD cannot treat confrontation or conflict with China or Russia as a "pick-up game." Paradoxically, to operate "loose" in contested environments, the interpersonal relationships within the command structure must be tight. Trust and familiarity can't be left to luck—it has to be inculcated over time.

Toward this end, the DoD and Congress should consider reforms to the Geographic Combatant Commands that refocus them on planning and execution of campaigns against China and Russia. Given the difficulty of this task, and the reality that bureaucratic entities seldom devolve or divest responsibilities, a more feasible interim step would be to create standing Joint or Multi-Domain Corps under EUCOM and INDOPACOM. Consistent with historical usage of the term, these corps would consist of a command structure and associated forces capable of operating independently for a given period of time. These corps would comprise "contact" and "blunt" layer forces from the *National Defense Strategy* and would be laser focused on planning, training for, and executing competitive and conflict campaigns against China or Russia, as well as developing and experimenting with future concepts. The corps structures obviously would be different in each theater, with a greater emphasis on maritime forces in the Pacific, and a larger contingent of ground forces in Europe.

Along with creating standing, theater-specific corps, the DoD should flatten the command structures of operational forces and push joint or multi-domain commands to lower echelons. Increasing joint or multi-domain integration at lower levels, such as the battalion, squadron, and group level, could greatly increase tactical flexibility and lethality in contested environments. CNAS wargaming suggests that concentrating multi-domain capabilities—particularly co-locating of sensors, shooters, and "deciders"—at lower echelons of command can enable more rapid decision-making as information and command systems degrade. Instead of relying on tenuous long-haul communications to overtaxed task force headquarters or combatant commands, these forces can leverage mission command to create responsive and resilient multi-domain units capable of independent action.

Further wargaming, analysis, and experimentation are needed to determine the sweet spot between limiting the number of organizational impediments to rapid decision-making and creating organizations with unwieldy spans of control. Toward this end, the DoD should explore optimizing organizational spans of control around the ability of joint or multi-domain forces to communicate and share a common operational picture in highly contested or degraded information environments.

U.S. armed forces will need to train differently to prepare for operating with degraded information and disrupted command systems by increasing the frequency of joint and combined training and by increasing the fidelity of simulated threats to information and command systems.

The most basic tenet of military training is "train how you fight," and yet most pre-deployment training is service- and domain-specific. Joint or multi-domain training occurs largely within the combatant commands. Unfortunately, this division of training is not effective at developing the familiarity, trust, and cohesion for truly joint or multi-domain operations under degraded conditions. To remedy this situation the DoD should increase the frequency of pre-deployment joint or multi-domain training by repurposing some Combatant Commanders Exercise Engagement and Training Transformation (CE2T2) funds for this purpose. Additionally, CE2T2 resources should focus on experimentation and development of joint warfighting concepts for operating with degraded information and command systems.

Another hurdle to increased joint or multi-domain training is the difficulty in using or simulating systems and effects from multiple domains in live, physical training. Most training ranges are not equipped to integrate large numbers of different systems from multiple domains, and particularly space, cyberspace, and the electromagnetic spectrum. Many advanced systems need tightly controlled or extremely remote ranges to prevent revealing their capabilities. To remedy this shortfall, the DoD should increase investments in developing synthetic training environments that can incorporate effects from all domains to replicate the contested and degraded information environments that U.S. forces will need to operate in during any conflict with China or Russia.[92]

Domain-Specific Concepts and Capabilities

In addition to the joint, multi-domain concepts from the preceding section, CNAS wargaming and research highlighted a number of domain-specific concepts and capabilities for winning the techno-cognitive confrontation. Derived from wargaming and analysis, these recommendations begin with a simple assumption: in the event of a crisis or conflict, China and Russia will faithfully execute their concepts and doctrines calling for aggressive, even preemptive attacks against critical information and command systems. This simple shift in perspective is a radical departure from the assumptions of the post–Cold War era, and serves to illustrate how vulnerable those flawed assumptions have left the joint force.

Space

Consistent with the core precept of operating effectively while degraded and contested, the DoD should develop concepts and invest in space capabilities that are designed around the assumption that China or Russia would strike first and strike hard against U.S. space systems. The emphasis should be on building resilience, particularly against the most likely or least escalatory threats posed by China and Russia.

Increase the resilience of space situational awareness (SSA). The side that quickly can gain and maintain an advantage in SSA is likely to have an enormous advantage in future military conflicts. Therefore, concepts and capabilities that enable U.S. armed forces to achieve this edge quickly at the outset of a conflict ought to be the highest priority of the newly formed Space Force. These capabilities should include: accurate and timely indications and warning for adversary space operations; aggressive use of non-kinetic weapons to disrupt and degrade both adversary SSA and their attacks on U.S. and friendly SSA systems; increasing the resilience of U.S. SSA systems, particularly to non-kinetic attacks; and increasing cooperation with allies and key partners to develop shared SSA systems.

Prioritize resilience to non-kinetic attacks. China and Russia would prefer to gain space superiority without resorting to the sorts of kinetic attacks that might damage their own orbital systems or the systems of neutral parties or fence-sitting U.S. allies and partners. Increasing the resilience of U.S. space systems to non-kinetic attacks such as RF jamming and laser dazzling therefore should take precedence over improving defenses against kinetic attacks, and particularly debris-causing direct-ascent attacks.

> **The DoD and the nascent Space Force should work to develop strategies and concepts for space combat, not just as an adjunct or sideshow to combat on earth, but as a potential centerpiece of modern warfare.**

Develop true space warfighting concepts. Current U.S. concepts of space operations and warfare come from a terrestrial view, i.e., they consider space as a warfighting domain only insofar as it impacts operations on earth. The increasing salience of space in warfare and the growth of the economic and political value of space as "critical terrain" is likely to change this earth-bound perspective. The DoD and the nascent Space Force should work to develop strategies and concepts for space combat, not just as an adjunct or sideshow to combat on earth, but as a potential centerpiece of modern warfare.[93]

Leverage commercial, allied, and partner systems. China and Russia want to limit any conflict with the United States and avoid actions that would create or solidify a large counter-coalition. U.S. Space Force should exploit this desire by increasing its use of, and integration with commercial, allied, and partner space systems. In the event of a conflict, this would present China or Russia with a dilemma: leave these systems alone and allow U.S. forces relatively uncontested access to space, or attack these systems and risk escalating or expanding a conflict.

Create distributed, long-range, line-of-sight alternatives to satellite communications. Blue and red teams across CNAS games used UAS and other long-endurance aircraft as part of an ad hoc long-range communications network that stood in for degraded satellite communications. While long-endurance UAS played the most obvious role, building the data and waveform-agnostic "Rosetta Stone" network described above would allow U.S. armed forces to pass diverse forms of data across myriad platforms, thereby spanning huge theaters using resilient line-of-sight communications. ISR, aerial refueling, and transportation aircraft; surface vessels; and ground installations could all act as translators or pass-throughs to create massive, jam-resistant mesh networks. While lacking the dedicated bandwidth and global coverage of satellite communications, these networks would provide a valuable backup as satellite communications degrade.

PNT investments. The DoD should significantly increase its investments in jamming or spoofing adversary space-based PNT systems such as GLONASS and Beidou. To counter Chinese and Russian jamming and spoofing of GPS, the DoD should accelerate development and deployment of alternatives to space-based PNT.

Cyberspace

Concept development and capability investments in cyber should start from the reality that DoD networks have been penetrated, and these penetrations will only get worse during a crisis or a conflict. The DoD should not attempt to have a fully clean and secure network, but rather figure out how to operate effectively enough even while badly penetrated.

Build a trust advantage. Cyber discussions often focus on offense and defense, but at times this lens can obscure a critical aspect of the techno-cognitive confrontation: trust. In all likelihood, neither side in this competition will be able to trust its networks or encryption. So how can U.S. forces trust the information on their networks? How can they trust their systems to operate as intended? Can they trust the data they've exfiltrated from adversary systems? How can they reduce adversaries' confidence?

Achieving trust on U.S. networks likely will mean shifting away from a trusted network paradigm in which every entity on the network is trustworthy because they have access to a restricted network, and toward a trusted entity paradigm. This would be more akin to peer-to-peer file sharing networks, in which sophisticated trust and rollback algorithms help sort trusted entities and information from malicious actors and malware.

This also will entail the use of honeypots, deception, and hackbacks to reduce adversaries' trust in the data that they exfiltrate from U.S. networks.[94] At the same time, aggressive offensive cyber actions against adversary systems will reduce their trust and confidence in their own networks. In CNAS wargames, for example, blue teams expected many red attacks against TRANSCOM and the CAOCs and prepared hackbacks and planted false data for the red teams. Blue teams launched their own attacks against industrial control systems at ports and railyards, C3 for IADS, targeting systems for long-range strike weapons, and Chinese (Beidou) and Russian (GLONASS) PNT systems. U.S. teams also used cyber weapons to create cognitive overload, attacking the "Great Firewall" that censors and controls internet access in China and the systems that China uses to maintain internal security in places like Xinjiang.

Push cyber to the tactical edge. Given the increasing salience of cyber actions at the tactical and operational level and the rise of integrated electronic warfare and cyber capabilities, the DoD needs to explore ways of incorporating offensive and cyber capabilities at lower echelons of command. Currently, most U.S. cyber capabilities are centralized in U.S. Cyber Command and its Joint Cyber Warfighting Architecture, which almost assuredly will be off-limits to forward commanders. The DoD needs to increase its concept and capability development in this area and work to find ways to push cyber and integrated EW-cyber capabilities forward to the tactical edge where possible.

Train for degraded/penetrated network operations. The DoD operates under a degree of persistent cyber threats; however, these threats pale in comparison to the degree of disruptions and penetrations likely to occur during a crisis or full-blown conflict with either China or Russia. DoD personnel across the enterprise need to train and prepare to operate effectively under these conditions. In future cyber conflict, both sides are likely to suffer massive network and system disruption. The advantage is likely to accrue to the side that copes with and moves past these disruptions with a minimal amount of cognitive degradation. Every unit in the DoD should spend time training on how they would execute their missions—both peacetime and wartime—with degraded or penetrated networks. This emphasis should also carry over into joint and combined training and exercises.

Electromagnetic Spectrum Operations

Electromagnetic spectrum operations have seemingly taken a back seat to space and cyberspace in discussions of future warfare and in the DoD investment portfolio. China and Russia do not share this perspective and, to paraphrase Leon Trotsky, the DoD may not be interested in electromagnetic spectrum operations, but electromagnetic spectrum operations are interested in the DoD. The imbalance between the threat and current investments is so large that myriad investments are necessary, but two stand out from the wargames and research.

> **To be able to 'turn out the lights' on China and Russia, the DoD needs to get serious about developing the necessary concepts and capabilities to attack their sensor and communications systems.**

Increase and refocus investments in electronic attack (EA). DoD investments in electronic attack persistently have lagged investments in electronic attack, and the primary EA investments over the last 30 years have been in countering improvised explosive devices. While this was a worthwhile effort, it should no longer be the focus of EA investments under the 2018 *National Defense Strategy*. To be able to "turn out the lights" on China and Russia, the DoD needs to get serious about developing the necessary concepts and capabilities to attack their sensor and communications systems.

Create counter-EA hunter-killer capabilities. To counter Chinese and Russian electronic attack systems, the DoD should develop counter-EA hunter-killer teams that seek out and provoke adversary EA systems into radiating, thereby exposing them to attack by anti-radiation munitions. Attacking ground emitters might be an excellent mission for manned-unmanned teams, with manned aircraft managing operations from a relatively safe distance while a variety of unmanned aircraft and smart munitions hunt down enemy emitters.

Air

U.S. air forces have become accustomed to dominating the air and information domains, and coupling these advantages to deliver devastating effects against adversaries like Iraq, Yugoslavia, Libya, al Qaeda, ISIS, etc. The erosion of U.S. air dominance is a subject for another time, but U.S. air forces must truly grapple with their eroding information advantage. For 30 years, these forces have focused on becoming more connected, gathering more information, and targeting with more precision. Now, they must begin to consider what air operations look like if they cannot have that level of connectedness, their information is limited or degraded, and their targeting is contested and imperfect.

Focus current programs like Advanced Battle Management System (ABMS) and JADC2 on enabling flexibility between tight and loose operational models. This paper intentionally has eschewed discussing current programs for many reasons. However, these programs are potentially so critical to the development of systems-of-systems capable of operating along the lines described in this paper that they merit an exception.

Initial signals from the Air Force suggest that the leaders of these programs understand the need to create more resilient, federated networks to enable "true" multi-domain operations.[95] However, CNAS wargaming and analysis suggests that there is a disconnect between the Air Force's vision and the information and command demands of operations against China or Russia. Moreover, there is a risk that, in focusing on rapidly developing underlying technologies, the Air Force underemphasizes the cognitive, organizational, and training challenges inherent in developing radically new command-and- control architectures.

Developing networks that can share data rapidly and reliably across domains and organizational boundaries in complex, contested environments with degraded systems is a remarkably difficult engineering and operational challenge. However, CNAS research suggests that the Air Force could benefit from shifting its focus from a technological "C4ISR" approach to a cognitive, information, and command-centric approach. The ultimate test of these systems isn't whether they pass data effectively, but rather whether they contribute to victory by enabling U.S. forces to make better decisions on tighter timelines than the adversary.

Accelerate development and deployment of low-cost attritable aircraft. CNAS wargaming and analysis repeatedly demonstrated a demand for affordable unmanned systems that could conduct ISR, strike, electronic warfare, and communications missions inside contested airspace without endangering a pilot or a high-value aircraft. Accelerating development and deployment of such an aircraft would contribute significantly to enabling "loose" operating structures in contested environments. A word of caution is in order, however. CNAS wargaming also suggested that operators wanted to load these low-cost, "attritable" aircraft with myriad multi-mission capabilities, at which point they likely would cease to be low-cost or attritable. The Air Force will need to maintain discipline to avoid "requirements creep" on these programs.

Increase investments in area-effects and other "precise-enough" weapons. Operations over the last 20 years have accustomed U.S. air forces to employing weapons with a high degree of precision enabled by exquisite ISR collection and relatively methodical planning and targeting against relatively limited target sets. Though there certainly have been exceptions to these conditions, this exquisite, meticulous process is the goal. In conflict with China or Russia, targeting information won't be exquisite—it will be spotty or "dirty" because of degraded data, decoys, deception, and cluttered environments. Planning and targeting processes won't be meticulous because air planners and targeteers won't have that kind of time. Targeting and weaponeering will have to embrace "good enough" information and "precise enough" weapons including cheaper weapons for saturation attacks, area-effects weapons, and weapons with more sophisticated terminal seekers that can find targets with imperfect information.

Maritime

Operating across three diverse physical domains (four if you include Marine amphibious operations), all of which place different stresses on information and command systems, U.S. maritime forces face unique challenges. The overarching maritime concern in the techno-cognitive confrontation is the targeting battle. Given the precision maritime-strike capabilities possessed by the United States, China, and Russia, the side that can rapidly build, maintain, and disseminate an accurate "picture" of the battlespace will likely have a decisive advantage.

Develop cooperative maritime domain awareness networks in the Indo-Pacific. The U.S. Navy already works closely with allies and partners in the Indo-Pacific on developing maritime domain awareness, both as a combined function and as a lasting capability within allied and partner navies. Increasingly, the Navy should work with allies and like-minded partners to develop a persistent, shared maritime domain awareness network stretching at least from northern Japan through the First Island Chain to Malacca. Ideally, this network also would cover the Indian Ocean, the Southern Pacific down to Australia, and the Western Pacific eastward to Guam and the Marianas.

Comprising a mix of space, airborne, land-based, surface, and—possibly with select allies like Japan and Australia—undersea assets, such a network would provide multilateral detection and tracking of illicit or coercive maritime activity. Making this network multilateral would help smaller states resist targeted peacetime Chinese coercion, or "salami slicing." During conflict, such a network would force China to attack a wide range of assets owned by multiple nations in order to disrupt wide-area maritime surveillance and targeting of its vessels.

Resolve the tension between distributed operations and avoiding detection through techniques like emissions control (EMCON). Threats from China's long-range maritime surveillance-strike complexes are pushing the Navy to operate in ways that may be contradictory, at once becoming more distributed and more connected, while also attempting to avoid detection through EMCON. For some time, the Navy has been pursuing methods and means to operate in a more distributed fashion—what the Navy calls "Distributed Maritime Operations (DMO)."[96] The idea is to avoid concentrating ships, thereby bringing fires from multiple axes, making ships more difficult to detect and target, and reducing potential losses in the event that China finds and targets a group of ships. The Navy intends to enable and accompany this shift away from concentrated fleet operations with two other initiatives: the Cooperative Engagement Capability (CEC) and Distributed Lethality.

> **The DoD should work with allies and partners to explore using unmanned undersea systems and other automated systems to monitor and defend undersea cables against attack.**

Long before most defense thinkers were interested in connecting every sensor to every shooter, the Navy was working toward making this a reality for the fleet with the CEC.[97] Distributed Lethality, meanwhile, entails arming a wider array of Navy ships, thereby reducing the concentration of the Navy's firepower in aircraft carriers and large surface combatants. When combined through DMO, this should create a larger, more distributed—and highly connected—fleet that confounds adversary targeting while still acting in a coordinated fashion to bring effective fires to bear when and where they're needed.

There's just one rather large catch to this vision. Though some communications and data-sharing can be accomplished using line-of-sight and low-probability of intercept/low-probability of jamming (LPI/LPJ) datalinks, maintaining CEC and other forms of connectivity in widely distributed operations will require long-range, high-bandwidth connectivity. In a fight with China, such links will either be disrupted by jamming and attacks on satellite communications, or they will give away ships' positions to SIGINT collection. In either case, the Navy will need operational and technical means to resolve this tension between dispersal, connectivity, and EMCON.

Integrate undersea assets into multi-domain operations. Undersea assets, whether submarines, unmanned underwater vehicle (UUVs), or unattended undersea systems, are a critical U.S. advantage in future conflict with China or Russia. Fully exploiting their capabilities as part of a multi-domain approach will require linking them into broader joint information and command systems. Unfortunately, the same opacity to most high-frequency electromagnetic radiation that makes undersea assets stealthy also limits their ability to send and receive high-bandwidth communications. Finding creative ways and means to overcome or work around this problem ought to be high priorities for the DoD and the Navy.

Use unmanned and automated systems to monitor and defend undersea cables. Russia has made little attempt to conceal its ability and intention to tap into, interfere with, or destroy the undersea fiber optic cables that carry most information traffic across the world's oceans.[98] One Russian red team in CNAS wargames cut critical transatlantic cables while attacking satellite communications networks in hopes of severing communications links between Europe and the United States. Chinese red teams cut the cables connecting Taiwan to the rest of the world and targeted U.S. cable networks across the western Pacific.

Russia's overt actions in a situation that ordinarily calls for covert and clandestine activity suggest that their behavior may be more for signaling vice actual warfighting capability. Nevertheless, both China and Russia could threaten these critical information conduits. The DoD should work with allies and partners to explore using unmanned undersea systems and other automated systems to monitor and defend undersea cables against attack. Since many of these attacks occurred at or near the places that cables "land" ashore, these unmanned and automated systems may not necessarily need to traverse huge swathes of open ocean to be effective.

Develop means to lay fiber optic cables rapidly. The Navy should explore concepts and capabilities that would enable it to lay fiber optic cables rapidly to augment or replace damaged undersea cables, or as an alternative to RF communications in contested or degraded environments.

Ground

U.S. ground forces face a strange transition from the wars of the last 20 years toward the emerging techno-cognitive confrontation. On one hand, U.S. ground forces, in collaboration with the rest of the joint force, have developed truly unprecedented abilities to gather, process, transmit, and act on information. On the other hand, these systems and processes were oriented toward irregular tactical threats, and depended on absolute air dominance and relatively uncontested use of space, cyberspace, and the electromagnetic spectrum. The key for ground forces therefore will be accepting that their understanding of the battlefield likely will never be as good as it has been over the last 20 years, and adapting or updating their systems, processes, and training accordingly.

Develop concepts and capabilities to enable "good enough" connectivity in degraded and contested environments. Over the last 20 years, ground forces have become accustomed to nearly ubiquitous network connectivity. Systems are still subject to friction and fail unexpectedly, but U.S. ground forces have not faced an adversary with sophisticated electronic support (ISR and targeting) or electronic attack (jamming and spoofing) such as the Chinese or Russian armed forces. To deal with this threat, U.S. ground forces will have to develop LPI/LPJ communications capabilities and concepts to enable effective communications in contested, degraded information environments, to include data burst communications and exploitation of "transceivers of convenience" such as commercial systems, cellular, and Wi-Fi networks.

Increase and focus investments in EA and counter-EW. The Army and Marine Corps have, generally speaking, underinvested in electronic warfare, and particularly electronic attack over the last two decades. They focused their relatively limited investments on defeating RF-triggered improvised explosive devices (IEDs) and other improvised threats. While this focus was understandable during the wars in Iraq and Afghanistan, current threats from China and Russia necessitate a new focus on jamming or spoofing adversary communications networks and sensors, as well as attacking adversary jammers and spoofers with anti-radiation munitions.

Integrate tactical UAS and other unmanned systems into multi-domain operational pictures. Presently, ground forces operate a wide array of unmanned systems, including aerial vehicles, ground vehicles, and unattended sensors. These systems provide ground forces with increased situational awareness; however, their information generally is stovepiped and fed directly to tactical commanders. A UAS providing overwatch and situational awareness to a company-sized ground element does not generally contribute to the creation of a broader operational picture in the way that, for example, an Air Force MQ-9 aircraft might. This lack of integration wastes an enormous amount of information that otherwise might contribute to creating a more detailed, accurate, and resilient operational picture.

Rēzekne Revisited: Eastern Latvia 2030

At 0545, the Charlie Company commander sat in the squadron briefing room outside Riga, which was just a few rows of cheap chairs on threadbare and stained maroon industrial carpet in a cinderblock box on the outskirts of Riga. Someone had tried to spruce things up with the flags, guidons, and crests of their combined multi-domain squadron and its subordinate units, but the juxtaposition of the bright colors with the quasi-Soviet decor somehow made things worse. The buzzing fluorescent lights weren't doing the room or the commander's headache any favors, either.

She turned to greet her Latvian counterpart as he walked in to join the assembled group of officers and senior NCOs. She called him "Ozo," which was short for Ozoliņš. They'd bonded over the famous hockey player Sandis Ozoliņš—her dad had been a big Colorado Avalanche fan growing up in Denver and imparted that love to his daughter. She'd played growing up and turned down Division I scholarship offers to attend West Point. It was still a point of semi-jocular friction with her dad.

She and Ozo had known each other for over a year by this point. After Russia stepped up its Baltic operations in 2027 in response to Belarus' move for closer relations with NATO and the EU, the United States augmented Canada as the enhanced forward posture lead in Latvia. Ozo's unit actually had deployed to the States to train with their squadron in late '28 before they did a combined training rotation at Drawsko-Pomorskie in Poland with other members of the EMDC, or European Multi-Domain Corps. The whole thing culminated in a massive NATO exercise across the Baltic region and other parts of Europe.

Their squadron was part of larger U.S.-NATO effort to change the organization and command structures of joint and combined forces. The idea was to train and deploy repeatedly as joint and combined units to develop cohesion across the services and with allies. The name "squadron" was a bit of a running joke, but the brass had selected it because it was the one tactical echelon shared by all four services. Their next command up was a "multi-domain group," and above that was a corps. The Army won that naming fight in Europe at least.

She could tell Ozo was hurting. He had eight-month-old twin girls at home. She flipped him a tin of Copenhagen and he grinned. ″That'll kill you," she scolded, and he gave an exhausted smile in response. She never touched the stuff, but it was popular with the Latvians, so she always kept a tin in her pocket. He offered it back and she refused: "Keep it—on one condition: I'd better not have to clean one of your spit bottles out of the vehicle again." He nodded in assent and tucked the tin into a uniform pocket.

With that, the squadron commander walked in with the commander of the Latvian battalion in the squadron, followed by their operations and intel officers, the senior-ranking joint officers assigned to this multi-domain unit, and a handful of civilians she'd recognized but whose names she didn't know. Or didn't need to know, she thought, wrinkling her eyebrow and chuckling to herself. The commander said "at ease" before anyone had a chance to stand. He had less than zero time for the pomp and circumstance of command, and his subordinates adored him for it.

The commander stepped to the lectern, bade them all good morning, then directed a razor-sharp knife hand right between her eyes. "I'd like to thank the captain here for the idea behind our operations today. For those of you who don't know, she wrote her thesis at West Point on the potential use of ops-intel fusion for countering sub-conventional coercion." She suddenly felt as though someone had rubbed Tiger Balm all over her face and neck. She knew she was turning red as a beet and she internally cursed her Irish heritage for her pale skin and lack of stoicism. Had she been anywhere else, she'd have slunk lower in her chair, but not with that knife hand staring her down in front of her commander and all her peers. So, she sat there with what she hoped was a polite grin, but she was pretty sure was an awkward grimace.

The commander continued, "Our operations over the last several months have been designed to closely link with our partners in U.S., NATO, and Latvian intelligence to identify and root out Russian malign influence. The captain's ideas were at the heart of this. Kudos to her." She could feel every invisible stare on her scalp and face as though everyone in the room were painting her with a laser target indicator. Of course, this was the day she sat in the front row for the briefing. Of course.

Thankfully, the commander turned the floor over to the ops and intel officers. The began with a rundown based on the intel they'd collected from the squadron's previous operations. The Russians had been using agents provocateur and disinformation to provoke minor protests in cities with large ethnic Russian populations. They used these protests and the possible presence of covert Russian forces as a lure for U.S. and Latvian forces. They were observing U.S. and Latvian tactics, techniques, and procedures while hoping to lull them into a false sense of security.

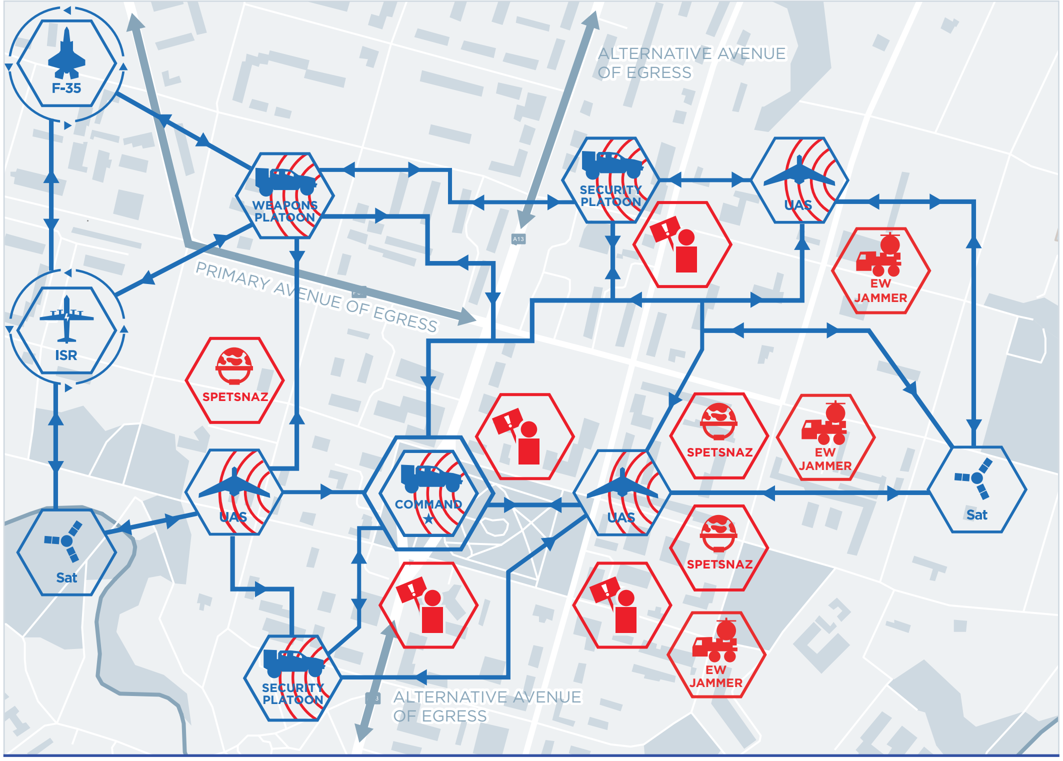
Intelligence had detected a major uptick in Russian activity near a city in eastern Latvia called Rēzekne. The intel folks weren't exactly sure what the Russians wanted to do—maybe they wanted to demonstrate their ability to spring a trap on NATO forces to monitor their response. Or, more worryingly, maybe they were hoping to capture some NATO personnel. It would be a significant escalation of the ongoing crisis, but not out of the realm of possibility. Either way, this was what the squadron's operations had been building toward.

They would be springing a counter-trap on the Russians. The objective of the operation was to find and track the Russian operatives and forces in the city to uncover their physical and human networks and maybe enable Latvian police or intelligence forces to capture anyone in the country illegally. It was an adaptation of counterterrorism tactics for what the Russians called "information confrontation." The operation would integrate satellite surveillance, cyber and radio-frequency monitoring of communications, airborne surveillance with ground moving target indicators, pre-placed unattended sensors, and a network of Latvian agents.

Her company's job, along with Bravo Company and their Latvian counterparts, was to serve first as the bait, and then as the hounds that flush the prey. There was some risk in this operation. Her company would have to roll into the town in their standard posture, otherwise they'd give the game away. That meant JLTVs instead of Strykers, limited body armor and heavy weapons, and no lethal unmanned ground vehicles. Also, their air support couldn't *look* like air support—a four-ship of F-35s circling overhead might be suspicious—so it would be out over the Baltic Sea conducting what looked like a standard air patrol. The nearest supporting ground unit would be 50 miles away down in Daugavpils—too far away to be much help in the event things went sideways. Alpha Company would be on standby with helos as a quick reaction force (QRF), but they'd still take about 30 minutes to get to Rēzekne from outside Riga.

The intel projected around 50 Russian operatives in Rēzekne—a mix of intel and Spetsnaz. She really hoped they were right. She trusted her intel team. They worked hand-in-glove with Latvian, NATO, and U.S. intelligence.

TACTICAL VIGNETTE IN RĒZEKNE, LATVIA—REVISITED



The Charlie Company commander's situation in Rēzekne. Successful NATO information operations and tight integration with allied forces have reduced support for Russian infiltration. Resilient mesh networks enable connectivity and situational awareness in the midst of heavy Russian electronic attacks.

Still, the Russians were wily, and it was *her team* that would be exposed in the middle of a city with no nearby support.

After the briefing, she and Ozo mounted up and headed east on the E22 toward Rēzekne with the rest of Charlie Company. They shouldn't have been in the same vehicle in case they came under attack, but they'd developed this habit as a way of demonstrating their close relationship to the Latvians they met, and they didn't want to do anything that indicated that something might be up. The whole battalion had even been in digital lockdown for a week to stop leaks. To prevent the lack of digital traffic from tipping off the Russians, they used bots to mimic standard communications and social media behavior based on past activities. The two companies were otherwise transmitting normally in RF and not practicing EMCON. They *wanted* the Russians to hear them coming.

She looked down at a screen on the back of the seat in front of her. It carried a "feed" from the tactical drones her company used for situational awareness. It wasn't actually a live video feed, although the drones were recording video. It was a tactical update of moving objects overlaid on a sophisticated, pre-built 3D terrain model. By limiting transmissions just to changes in states for certain objects instead of full-motion video, the drones could transmit short bursts in small little bands of the EM spectrum. They could also intelligently pass data among themselves to find the best pathway to transmit back to her and her platoon leaders. They were almost impossible to jam, and the Russians had tried. The best part was that the drones did all of this and flew autonomously. The data just showed up on her screen or in her helmet reticle.

They were meshed into a big network with the vehicles in her company, and they were pumping all this data back to the squadron command center and to the F-35s out over the Baltic. Everyone in the squadron had the same picture she was seeing, and they could use that picture to task each other as needed. It wasn't easy—she remembered how her first sergeant just shook his head at the goat rodeo that had ensued the first time the squadron had conducted synthetic training using these systems with Air Force, Navy, and Latvian units. But after two years training and operating together, it had become completely natural.

As her company entered the town, she watched on her screen as platoons wordlessly split off to take up their blocking and security positions and fire teams pushed out farther and clambered up buildings to take up observation posts. It was basic tactics, but there was something beautiful in the fluidity of a simple thing executed perfectly without any need for communication. It was hard to believe that she was watching two companies from totally different countries and backgrounds. They weren't "interoperable." They just *were*.

Her command detachment moved toward the commotion in the center of the town. The mayor and police chief walked over to greet them as they dismounted their JLTV. The police chief, Arturs, was a no-BS guy and didn't like the Russians messing about in his town. He had no neck and a huge brow—he looked like he'd only recently begun to walk upright. The mayor, Edgars, on the other hand, relied on a significant amount of ethnic Russian support (and, according to intelligence reports, Russian funding). He fancied himself a smooth political operator. He'd learned that she was from Colorado and now always greeted her with a loud "howdy" because in his mind, that meant she was a cowgirl. It was somehow more annoying because she'd done gymkhana as a kid.

Arturs started telling Ozo what was happening, but Edgars cut him off pretty quickly. She'd picked up a bit of Latvian, but it was tough to hear over the noise of the protesters. She still could read body language, and Arturs looked downright pissed. He was trying to hide it, but his nostrils had flared into two angry black holes. Arturs and Edgars said goodbye and headed back toward the edge of the town center to keep an eye on the protestors.

They walked back to the JLTV and Ozo whispered out of the corner of his mouth, "Get ready. It's coming now." The noise from the crowd seemed to grow, and her helmet reticle showed four, five, then six red dots indicating electronic warfare systems transmitting and jamming sensors and communications. They jumped back in the vehicle, and she pulled up a different setting on her screen—this was a sophisticated electronic support readout of the frequencies the Russians were jamming, as well as triangulated estimates of the jammers' location. It looked like they were trying to cut them off from GPS, VHF line-of-sight, UHF to aircraft, and multiple bands of satellite communications. They'd expected this and drilled for it, but adrenaline was sizzling through her all the same.

She turned to her RTO and showed him the readout. "Do we still have external comms if we need them?" she asked. "Yes ma'am, we'll have to use bursts and hop around a bit, but I can get messages out." "What about internally," she asked, "do we have comms with our platoons?" "Roger, ma'am," he replied, "we can bounce data around our radios, even off of the drones if we need to. We're one big mesh net and they can't take out the whole thing with the systems they have here."

OK, now came the hard part—she had to act like vulnerable prey and wait for help. She had the feeling that the first part wouldn't be too hard. As soon as the thought crossed her mind, the protestors had begun removing cobblestones from the sidewalks and hurling them into the windows of the buildings around the central plaza. The mob, armed with stones and who knew what else, was ambling in her direction.

The platoon leaders had seen the same data update from the drones, and were using bounding overwatch to collapse back to a more defensible perimeter. Based on the tactical picture from the drones and quick-burst text messages from her platoon leaders, it looked as though the mob had split into three, with the main group pressing in on her command element in the center, and two wings attempting to encircle them to the north and south. She'd known something like this was coming, but still, it was unsettling to let an enemy—even if just a mob armed with cobblestones—outflank and possibly surround her.

Ozo turned to her and beamed, which was gross because she saw his big plug of dip and his yellow-brown teeth. He gave her some good news. The mob was smaller than they'd feared and made up of a large percentage of Russians. This was heartening—it appeared that the nonstop information operations they'd been conducting had some effect amid the barrage of Russian propaganda and disinformation. Then he started laughing uncontrollably. She thought he was going to choke on his spit he was laughing so hard. She asked him what was so funny. He said the southern wing of the mob had been halted in a park by . . . a large contingent of grandmothers.

It seems that the older women, who still could remember Soviet rule, were not too pleased about a group of foreign goons taking over their town, so they'd gone down to this park, gathered into a semi-phalanx, and begun banging pots and pans. The mob leaders didn't know what to do—they couldn't attack grandmothers, so they outflanked them, but now they were on the wrong bank of the Rēzekne River and disorganized.

Just then, her RTO turned to her. "Ma'am, airborne and space assets are overhead and are tracking their targets, QRF forces have taken up positions on the northern and southern flanks of the town. I'm directly quoting from higher when I say: It's time to get these Russians out of Rēzekne."

Conclusion

After nearly 30 years of unchallenged conventional military dominance, U.S. armed forces must grapple with the realities of Chinese and Russian military power and the resultant changes that power has wrought on the character of warfare. The United States, alongside its allies and partners, is in a competition for military advantage in East Asia and eastern Europe that likely will go a long way toward determining the political and economic futures of these key regions. The techno-cognitive confrontation will be central to this larger competition for military advantage, and its importance likely will grow as China, Russia, and the United States attempt to shift from informatized to intelligentized warfare through the development of artificial intelligence and autonomous systems.[99]

To deal with this new reality, the DoD must abandon outdated and unrealistic notions of gaining and maintaining information dominance. This notion depended on a degree of military advantage that is unlikely to return any time soon. Rather than fighting the future or attempting to spend its way back to the 1990s, the DoD needs to embrace the advantages that it has within this new type of warfare. To do this, the DoD must attack the tension in Chinese and Russian strategies by forcing them to choose between operational advantages and the strategic disadvantages of expanding or escalating a conflict. The DoD must work closely with allies and partners to seize the initiative in the information environment away from China and Russia. The DoD must develop the concepts, capabilities, organizational structures, and training regimens necessary to win the techno-cognitive confrontation by leveraging its structural advantage in human capital.

Collectively, these steps would undercut Chinese and Russian theories of victory predicated on gaining superiority in the techno-cognitive confrontation. Demonstrating U.S. capability and intent to execute these concepts as needed would prove a powerful deterrent both to sub-conventional coercion and outright aggression, and would enable the United States to uphold critical security commitments and preserve the free and open international order that has made the United States secure and prosperous for more than 70 years.

1. Regarding attacks on physical command nodes, see Michael S. Chase and Andrew S. Erickson, "The Conventional Missile Capabilities of China's Second Artillery Force: Cornerstone of Deterrence and Warfighting," *Asian Security*, 8 no. 2 (2012), 115–137.

2. See, for example, Barry D. Watts, "The Evolution of Precision Strike," Center for Strategic and Budgetary Assessment, 2013; Andrew F. Krepenevich, "Maritime Competition in a Mature Precision-Strike Regime," Center for Strategic and Budgetary Assessment, 2015.

3. For more on how China and Russia have worked to erode U.S. strategic and operational advantages since the Gulf War, see Chris Dougherty, "Why America Needs a New Way of War," CNAS, June 2019, https://s3.amazonaws.com/files.cnas.org/CNAS+Report+-+ANAWOW+-+FINAL.pdf.

4. John R Hoehn, "Joint All Domain Command and Control (JADC2)," Congressional Research Service, September 2020, https://fas.org/sgp/crs/natsec/IF11493.pdf.

5. For example, see Jay Koester, "JADC2 'Experiment 2' Provides Looking Glass into Future Experimentation," U.S. Army, April 23, 2020, https://www.army.mil/article/234900/jadc2_experiment_2_provides_looking_glass_into_future_experimentation; Jon Solomon, "21st Century Maritime Operations Under Cyber-Electromagnetic Opposition," Information Dissemination, October 21, 2014, http://www.informationdissemination.net/2014/10/21st-century-maritime-operations-under.html.

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

7. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985) 5–9.

8. The author is neither a China nor a Russia area specialist and does not speak or read Mandarin or Russian. The sources on Chinese and Russian military thinking contained herein are therefore secondary sources, or translations and compilations of primary sources. Any errors in interpretation are the author's.

9. China and Russia may have different trajectories, but many in the defense community have been too quick to dismiss Russia as a near-term threat facing deep structural issues. This attitude brazenly disregards the numerous near-death experiences in Russian history that preceded miraculous recoveries. For more on this, see Michael Kofman, "Russian Demographics and Power: Does the Kremlin have a Long Game?" War on the Rocks, February 4, 2020, https://warontherocks.com/2020/02/russian-demographics-and-power-does-the-kremlin-have-a-long-game/.

10. One interesting and somewhat surprising outcome of the research behind this paper is the surprising degree of convergence between Chinese and Russian military thought regarding the character of war and military strategy and operational concepts for confronting, coercing, or, if necessary, fighting the United States. The author would submit that greater cross-pollination between the China and Russia military studies communities would be quite beneficial.

11. This is a crucial difference compared with Nazi Germany and Imperial Japan, both of which actively sought conflict for ideological reasons. This assessment might change over time, should the risk/reward calculus of either China or Russia change, but at present this suggests that a properly executed U.S. strategy of deterrence by denial should remain effective. For more on the logic of limited war, see Elbridge Colby, "America Must Prepare for 'Limited War,'" *The National Interest*, October 21, 2015, https://nationalinterest.org/feature/america-must-prepare-limited-war-14104; Elbridge A. Colby and Burgess Laird, "Managing Escalation and Limiting War to Achieve National Objectives in a Conflict in the Western Pacific," CNAS, August 2016, https://www.hsdl.org/?abstract&did=; Elbridge Colby, "How to Win America's Next War," *Foreign Policy*, Spring 2019, https://foreignpolicy.com/2019/05/05/how-to-win-americas-next-war-china-russia-military-infrastructure/; and Elbridge A. Colby, *Great Power: The Future of U.S. Defense Strategy* (New Haven, CT: Yale University Press, forthcoming).

12. As Dave Johnson and others note, this tension is particularly acute in Russia's military strategy. On one hand, Russia seeks to localize and limit conflicts and avoid a broader war with NATO or a regional coalition of states. On the other hand, Russia's strategy to achieve this localization involves aggressive preemptive strikes to create "unacceptable damage" against their adversaries' weaknesses, while threatening further escalation to force conflict termination on terms favorable to Russia. See Dave Johnson, "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds," Livermore Papers on Global Security No. 3, Lawrence Livermore National Laboratory, February 2018, 20.

13. The paper will discuss these latter technical activities in a subsequent section.

14. See John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," China Strategic Perspectives 13, Institute for National Strategic Studies, October 2018, 44–47, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

15. Costello and McReynolds, "China's Strategic Support Force," 7, 45.

16. Costello and McReynolds, "China's Strategic Support Force," 45.

17. It is unclear if "Three Warfares" is the overarching concept for Chinese influence campaigns, or just a broad description of Chinese thinking about such campaigns. Nevertheless, it serves as a useful guide for understanding China's approach.

18. Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief*, 16 no. 13 (August 22, 2016), https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

19. Kania, "The PLA's Latest Strategic Thinking on the Three Warfares."

20. Costello and McReynolds, "China's Strategic Support Force," 4.

21. Costello and McReynolds, "China's Strategic Support Force," 15.

22. Some Russian military theorists even argue that the ability to alter perceptions and policies through information operations, combined with the ability to deliver information effects through cyberattacks and electronic warfare, may have radically altered the character of warfare and rendered "traditional" military operations unnecessary, or subordinate aspects of warfare. See Keir Giles, "Handbook of Russian Information Warfare," Fellowship Monograph 9, NATO Defense College, November 2016, 3–5, http://www.ndc.nato.int/news/news.php?icode=995; Timothy L. Thomas, "Russian Military Thought: Concepts and Elements," MITRE Corporation, August 2019, 9-1 through 9-29, https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf.

23. Thomas, "Russian Military Thought;" Giles, "Handbook of Russian Information Warfare," 6–11; Lesley Kucharski, "Russian Multi-Domain Strategy against NATO: information confrontation and U.S. forward-deployed nuclear weapons in Europe," Center for Global Security Research, 2018, https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf; Dmitry (Dima) Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Papers 54, Institut français des relations internationals Security Studies Center, November 2015, https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf; and Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspirations," Defense Intelligence Agency, 2017, 38, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937.

24. Giles, "Handbook of Russian Information Warfare," 6–10.

25. Mark Galeotti, "Controlling Chaos: How Russia Manages its Political War in Europe," European Council on Foreign Relations, September 1, 2017, https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe.

26. Galeotti, "Controlling Chaos."

27. This is consistent with past patterns of Russian and Soviet military thinking, in which there is a great deal of intellectual effort spent defining the characteristics of the warfare regime or "generation." See Adamsky, "Cross-Domain Coercion," 22–23; Kucharski, "Russian Multi-Domain Strategy against NATO," 9–10.

28. Some Western analysts have discussed "new-generation or new-type war" in conjunction with the Western concept of hybrid warfare that came into vogue following the 2006 Lebanon War. Most Russian writers see hybrid warfare as a Western/U.S. method and see its application in the "color revolutions" in former Soviet republics. This Russian misperception is awash in irony, since A) there is no agreement in the U.S. defense community as to what constitutes hybrid warfare and, due to this vagueness, the term has fallen out of vogue; B) insofar as there was a singular idea of what constituted hybrid warfare in the United States, it was the approach used by Lebanese Hezbollah in 2006; and C) the color revolutions in no way represent mainstream U.S. thinking on hybrid warfare. This torturous hall of mirror-imaging is instructive for two reasons. First, it indicates the odd dialectic that seems to be occurring between U.S. theories and operations and Russian counter-theories and operations. This is an important factor to consider in concept development and strategy. Second, it should encourage U.S. analysts to be wary of ascribing singular, conclusive definitions of foreign concepts. Just as there is no single common definition of hybrid warfare in the United States, so too might Russian military thinkers have different understandings and interpretations of new-generation and new-type warfare. See Thomas, "Russian Military Thought," 5-1 through 5-12, 9-1 through 9-23.

29. Thomas, "Russian Military Thought," 1-3.

30. Thomas, "Russian Military Thought," 8-5.

31. Adamsky, "Cross-Domain Coercion," 23.

32. Thomas, "Russian Military Thought," 5-8, 10-6, 11-17.

33. Giles, "Handbook of Russian Information Warfare," 6-7.

34. Thomas, "Russian Military Thought," iii.

35. Brian Naylor, "Russia Hacked U.S. Power Grid — So What Will The Trump Administration Do About It?" NPR, March 23, 2018, https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it; Tom Kelly, "Russian Hackers Penetrate US Power Stations," BBC, July 24, 2018, https://www.bbc.com/news/technology-44937787.

36. See Thomas, "Russian Military Thought," 4-1 through 4-12; Giles, "Handbook of Russian Information Warfare," 19–21.

37. See the excellent Norman Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter through Three World Wars* (Naval Institute Press, 2009), it describes the lengths to which navies went to craft maritime information and command networks in the pre-space era. While these efforts were admirable for their ingenuity and effectiveness, they often had massive geographic and temporal gaps in the maritime domain, and could not support landward information and command beyond the immediate littoral.

38. D. Rogozin, A. Zabrodsky, A. F. Ioffe, and M. Gareyev, "Defense Establishment: Strategic Goals of National Security: Military Science Must Forecast and Plan the Development of Arms and Military Equipment in the Spirit of the Times," *Military Industrial Courier*, August 2, 2013, cited in Thomas, "Russian Military Thought," 5-9.

39. Kevin Pollpeter, Senior Research Scientist, CNA, testimony before the U.S.-China Economic and Security Review Commission Hearing on "China in Space: Strategic Competition, U.S. Senate, April 2019, 1, https://www.uscc.gov/sites/default/files/Kevin%20Pollpeter%20USCC%2025%20April.pdf.

40. "Challenges to Security in Space," Defense Intelligence Agency, 2019, 12, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications%2FSpace_Threat_V14_020119_sm.pdf.

41. UCS Satellite Database, Union of Concerned Scientists, 2005, https://www.ucsusa.org/resources/satellite-database.

42. While this accords with Chinese and Russian strategies of limitation and aligns with other wargaming and analysis, a note of caution is in order. First, our wargames only explore the opening days and weeks of a conflict; it is possible that actions in space might get more aggressive as the fight continues and escalates. Second, it is possible that this outcome is a mixture of wish-casting and mirror-imaging on the part of the American players representing Chinese and Russian military planners. In other words, these players subconsciously hoped China and Russia want to avoid destroying the space environment, so they "cast" this mirror image onto Chinese and Russian planners and enacted this point of view during the game.

43. See Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, "Space Threat Assessment 2019," Center for Strategic and International Studies, April 2019, 5, https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf#page=22.

44. Only one (Russian) red team attacked space situational awareness using reversible means. One blue team used cyberattack to disrupt a Russian red team's common operating picture in space. Despite its increasing salience in modern warfare, space remains an arcane and highly classified topic in defense circles. It is not surprising, therefore, that the blue and red players who advocated attacking their opponents' space situational awareness were space experts who were savvy as to the possible advantages to degrading their adversaries' understanding of what was happening in space. There is likely a broader lesson here regarding the necessity of incorporating subject-matter experts on space, cyberspace, electronic warfare, and information operations into command staffs and traditional military planning staffs. Without experts versed in the arcane intricacies of these topics, it is likely that operations and planning staffs will underutilize, or even misuse these capabilities.

45. While China and Russia both possess their own communications satellites and PNT constellations, neither are as dependent on these systems as the United States in conflicts that occur near their territory.

46. For China, see U.S. China Economic and Security Review Commission, *2015 Report to Congress*, November 2015, 295–296, https://www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF; Kevin Pollpeter, Eric Anderson, Jordan Wilson, and Fan Yang, "China Dream, Space Dream: China's Progress in Space Technologies and Implications for the United States," Institute on Global Conflict and Cooperation, March 2, 2015, 17–18, https://www.uscc.gov/sites/default/files/Research/China%20Dream%20Space%20Dream_Report.pdf. For Russia, see Bart Hendrickx, "Ekipazh: Russia's top-secret nuclear-powered satellite," *The Space Review*, October 7, 2019, https://www.thespacereview.com/article/3809/1.

47. For a detailed description of China's maritime surveillance and targeting systems, see Eric Heginbotham et al., "U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017," RAND Corporation, 2015, 154–165.

48. Consistent with the PLAN's so-called "cabbage strategy," of protecting critical assets such as disputed maritime territory or oil and gas platforms with successive rings of "commercial," government, and military vessels, the Chinese red teams launched massive fleets, with the key amphibious ships moving under EMCON at the center of concentric rings of military surface vessels and commercial ships designed to defend against or absorb missile attacks. The team then interspersed numerous decoys through the fleet to further degrade the effectiveness of Blue's missiles. For more on the cabbage strategy, see Robert Haddick, "The Struggle for a Strategy," U.S. Naval Institute *Proceedings*, 141 no. 1 (January 2015), https://www.usni.org/magazines/proceedings/2015/january/struggle-strategy.

49. Russian red teams used CCD, EMCON, and mobility to protect their integrated air defense system (IADS) in Kaliningrad. The red teams limited their emissions to short bursts, moved systems quickly, hid them in complex urban terrain, and used decoy systems. Collectively, these actions significantly increased the sorties, weapons expenditures, and aircraft attrition that the blue U.S. team

needed to suppress the Kaliningrad IADS. It also increased the number of Russian civilian casualties caused by blue strikes, which fed into the red teams' information operations campaign.

50. Thomas, "Russian Military Thought," iii; Timothy L. Thomas, *China Military Strategy: Basic Concepts and Examples of its Use* (Fort Leavenworth, KS: Foreign Military Studies Office, 2014), 142–43. China and Russia also assume that the United States is taking similar measures against them and defend their own systems accordingly. However, Chinese and Russian sources on cyber operations tend to argue that offense predominates in cyber operations (a view many American sources share), and therefore put more emphasis on deterrence and rapid, preemptive attack than defense. For more, see Costello and McReynolds, "China's Strategic Support Force," 46; Thomas, *China Military Strategy*, 142–43; and Scott Boston and Dara Massicot, "The Russian Way of Warfare: A Primer," RAND Corporation, 2017, 3, 12, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE231/RAND_PE231.pdf.

51. Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," statement to the U.S.-China Economic and Security Review Commission, March 7, 2012, 33–38, https://www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

52. Sarah P. White, "Understanding Cyberwarfare: Lessons from the Russia-Georgia War," Modern Warfare Institute, March 2018, 18, https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.

53. For China, see: John Costello and Peter Mattis "Chapter 6: Electronic Warfare and the Renaissance of the Chinese Information operations," in *China's Evolving Military Strategy,* Joe McReynolds, ed. (Washington: Jamestown Foundation, Kindle, 2016), location 2483–2582; White, "Understanding Cyberwarfare," 13–22; Lauren Cerulus, "How Ukraine became a test bed for cyberweaponry," Politico, March 14, 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/; Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," Wired, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; and David Gilbert, "Inside the massive cyber war between Russia and Ukraine," Vice, March 29, 2019, https://www.vice.com/en_us/article/bjqe8m/inside-the-massive-cyber-war-between-russia-and-ukraine.

54. Costello and Mattis, "Chapter 6: Electronic Warfare and the Renaissance of the Chinese Information operations;" White, "Understanding Cyberwarfare," 13–22; Cerulus, "How Ukraine became a test bed for cyberweaponry;" Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar;" and David Gilbert, "Inside the massive cyber war between Russia and Ukraine."

55. For general threats, see Office of the Director on National Intelligence, *Threats to Undersea Cable Communications*, https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf; Nadia Schadlow and Brayden Helwig, "Protecting undersea cables must be made a national security priority," *Defense News*, July 1, 2020, https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/; and James Griffiths, "The Global Internet Is Powered by Vast Undersea Cables. But They're Vulnerable," CNN, July 26, 2020, https://www.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html. For China, see Justin Sherman, "The US-China Battle Over the Internet Goes Under the Sea," *Wired*, June 24, 2020, https://www.wired.com/story/opinion-the-us-china-battle-over-the-internet-goes-under-the-sea/; Meaghan Tobin, "US-China Tech War's New Battleground: Undersea Internet Cables," SCMP, December 14, 2019, https://www.scmp.com/week-asia/politics/article/3042058/us-china-tech-wars-new-battleground-undersea-internet-cables; and "Taiwan Undersea Cables 'Priority Targets' by PLA in War," *Asia Times*, December 6, 2017, https://asiatimes.com/2017/12/taiwan-undersea-cables-priority-targets-pla-war/. For Russia, see David Larter, "Navy Grapples with Russian Threats to Undersea Cables," *Navy Times*, October 30, 2015, https://www.navytimes.com/news/your-navy/2015/10/30/navy-grapples-with-russian-threats-to-undersea-cables/; Garrett Hinck, "Evaluating the Russian Threat to Undersea Cables," Lawfare blog, March 5, 2018, https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables; H I Sutton, "How Russian Spy Submarines Can Interfere With Undersea Internet Cables," *Forbes*, August 19, 2020, https://www.forbes.com/sites/hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/#7aaaafe53b04; David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *The New York Times*, October 25, 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html; and Louise Matsakis, "What Would Really Happen If Russia Attacked Undersea Internet Cables," *Wired*, January 5, 2018, https://www.wired.com/story/russia-undersea-internet-cables/.

56. Zhang Miling Li Yan, "Kōngjūn shízhàn huà xùnliàn tuīchū "qíng diàn" tíshēng diànzǐ zhàn nénglì" ["Air Force combat training launched 'Dynamic' to enhance electronic warfare capabilities"]," Zhèjiāng.cn [Zhejiang], October 14, 2019, http://china.zjol.com.cn/gnxw/201910/t20191014_11181855.shtml; From, Peter Wood, ″New PLA Air Force Training Exercise Focuses on Electronic Warfare,″ U.S. Army Foreign Military Studies Office, December 1, 2019, https://community.apan.org/cfs-file/__key/docpreview-s/00-00-17-98-10/2019_2D00_12_2D0[...]Exercise-Focuses-on-Electronic-Warfare-_2800_Wood_2900_.pdf.

57. 54 Alexander Stepanov , “Nad rossiyskimi bazami v Sirii razvernut kupol, zashchishchayushchiy ot raket” [“Over Russian bases in Syria deployed a dome that protects against missiles”],” mk.ru, April 15, 2020, https://www.mk.ru/politics/2018/04/15/nad-rossiyskimi-bazami-v-sirii-razvernut-kupol-zashhishhayushhiy-ot-raket.html.

58. For more on Chinese and Russian thinking on electronic warfare and electromagnetic spectrum operations, see Jeffrey Engstrom, “Systems Confrontation and Systems Destruction Warfare,” RAND Corporation, 2018, https://www.rand.org/pubs/research_reports/RR1708.html; Roger N. McDermott, “Russia’s Electronic Warfare Capabilities to 2025,” International Centre for Defence and Security, September 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

59. “Sinister Text Messages Reveal High-tech Front in Ukraine War,” VOA, May 11, 2017, https://www.voanews.com/europe/sinister-text-messages-reveal-high-tech-front-ukraine-war.

60. For more on this tendency toward centralization in the PLA, see Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005), 267–268, cited in *The Chinese Navy: Expanding Capabilities, Evolving Roles*, ed. By Phillip C. Saunders et al., chapter by Andrew Erickson and Michael S. Chase, “Informatization and the Chinese People’s Liberation Army Navy,” 267, 271.

61. See Yasuyuki Sugiura, “The Joint Operation Structure of the Chinese People’s Liberation Army with Focus on the Reorganization of the Chain of Command and Control under the Xi Jinping Administration,” *NIDS Journal of Defense and Security*, 19 no. 1 (December 2017); Dennis J. Blasko, “PLA Weaknesses and Xi’s Concerns about PLA Capabilities,” testimony to the U.S.-China Economic and Security Review Commission, February 7, 2019; and Cortez A. Cooper III, “PLA Military Modernization: Drivers, Force Restructuring, and Implications,” Testimony the U.S.China Economic and Security Review Commission, February 15, 2018, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT488/RAND_CT488.pdf. Regarding investments in AI and autonomy, see Elsa B. Kania, “‘AI Weapons’ In China’s Military Innovation,” *Global China*, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf; Else B. Kania, “杀手锏 and 跨越发展: Trump Cards and Leapfrogging,” thestrategybridge.org, September 6, 2017, https://thestrategybridge.org/the-bridge/2017/9/5/-and-trump-cards-and-leapfrogging; and Elsa, B. Kania, “Chinese Sub Commanders May Get AI Help for Decision-Making,” Defense One, February 12, 2018, https://www.defenseone.com/ideas/2018/02/chinese-sub-commanders-may-get-ai-help-decision-making/145906/?oref=d-river.

62. Yu Qifeng, “Pòjiě “wǔ gè bù huì” nántí yào cóng yuántóu rùshǒu” [“To Crack the ‘Five Incapables’ Problem Start with the Source”], 81.cn, October 13, 2015, http://www.81.cn/jfjbmap/content/2015-10/13/content_125880.htm, which states, “Yīxiē zhǐ huī yuán líkāile jīguān jiù bù huì pànduàn xíngshì, bù huì lǐ jiě shàngjí yìtú, bù huì dìng xià zuo zhàn juéxīn, bù huì bǐ i bīng bù zhèn, bù huì chǐ zhì tú fā qíngkuàng” [“Some commanders will not judge the situation, understand their superiors ’intentions, make up their minds to fight, not deploy their troops, or deal with emergencies when they leave the organization”]; cited in Blasko, “PLA Weaknesses and Xi’s Concerns,” 7.

63. See: Blasko, “PLA Weaknesses and Xi’s Concerns;” Cooper, “PLA Military Modernization;” Michael S. Chase, Jeffrey Engstrom, Tai Ming Cheung, Kristen Gunness, Scott W. Harold, Susan Puska, and Samuel K. Berkowitz, “China’s Incomplete Military Transformation Assessing the Weaknesses of the People’s Liberation Army (PLA),” RAND Corporation, 2015, https://www.rand.org/pubs/research_reports/RR893.html; and Mark R. Cozad, “PLA Joint Training and Implications for Future Expeditionary Capabilities,” RAND Corporation, 2016, https://www.rand.org/pubs/testimonies/CT451.html.

64. For more on these reforms, see Costello and McReynolds, “China’s Strategic Support Force;” Phillip C. Saunders, Arthur S. Ding, Andrew Scobell, Andrew N. D. Yang, and Joel Wuthnow, eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (Washington: National Defense University Press, 2019), 5–15.

65. For more on the centralization of Russia’s command and control, see *Russia Military Power*, Defense Intelligence Agency, 2017, 25–28, https://www.dia.mil/portals/27/documents/news/military%20power%20publications/russia%20military%20power%20report%202017.pdf.

66. *Russia Military Power*, 25–28.

67. For more, see Roger McDermott, “Russian Military Introduces New Automated Command-and-Control Systems,” *Eurasia Daily Monitor*, 16 no. 86 (June 11, 2019), https://jamestown.org/program/russian-military-introduces-new-automated-command-and-control-systems/; and Roger McDermott, “Moscow Showcases Breakthrough in Automated Command and Control,” *Eurasia Daily Monitor*, 16 no. 164 (November 20, 2019), https://jamestown.org/program/moscow-showcases-breakthrough-in-automated-command-and-control/.

68. See Keir Giles, “Assessing Russia’s Reorganized and Rearmed Military,” Carnegie Endowment for International Peace, 2017, https://carnegieendowment.org/2017/05/03/assessing-russia-s-reorganized-and-rearmed-military-pub-69853.

69. See Lester W. Grau and Charles K. Bartles, “The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces,” Foreign Military Studies Office, 2016, 51.

70. Department of Defense, *National Defense Strategy*, 7.

71. Lt. Col. Brus E. Vidal, "AFCENT Executes Command and Control of AFCENT from Shaw AFB US," U.S. Air Force, October 7, 2019, https://www.af.mil/News/Article-Display/Article/1982367/afcent-executes-command-and-control-of-afcent-from-shaw-afb-us/.

72. For more on how DoD has held information operations at arm's length, see Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, July 25, 2018, 7–9, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830. For more on the legal considerations, see Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, November 27, 2012, III-1 through III-3, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

73. Brad Lendon, Ivan Watson, and Ben Westcott, "'Leave immediately': US Navy plane warned over South China Sea," CNN, August 23, 2018; Jim Sciutto, "Behind the scenes: A secret Navy flight over China's military buildup," CNN, May 26, 2015.

74. Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment*, 7–9; Joint Chiefs of Staff, *Information Operations*, III-1 through III-3; and "Conference Report: National Defense Authorization Act For Fiscal Year 2020," U.S. House of Representatives, December 9, 2019, 546–552, https://www.congress.gov/116/crpt/hrpt333/CRPT-116hrpt333.pdf.

75. Grau and Bartles, "The Russian Way of War," 51.

76. The U.S. Navy gradually improved its night-fighting capability by improving its information and command capabilities. See Trent Hone, *Learning War: the Evolution of Fighting Doctrine in the U.S. Navy 1898–1945* (Annapolis: Naval Institute Press, 2018) 208–249.

77. Adam Raymond, "'We Own the Night': The Rise And Fall Of The US Military's Night-Vision Dominance," Task and Purpose, July 11, 2017, https://taskandpurpose.com/gear-tech/night-rise-fall-us-militarys-night-vision-dominance.

78. See, for example, Bryan Clark and Dan Patt, "JADC2 Needs To Change Course: More C2, Less Comms," Breaking Defense, April 13, 2020, https://breakingdefense.com/2020/04/jadc2-needs-to-change-course-more-c2-less-comms/.

79. For China, see *China Military Power: Modernizing a Force to Fight and Win*, Defense Intelligence Agency, 2019, 27, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf; Sam Goldsmith, "U.S. Conventional Access Strategy: Denying China a Conventional First-Strike Capability," *Naval War College Review*, 72 no. 2 (Spring 2019), 5–7. For Russia, see Defense Intelligence Agency, *Russia Military Power*, 26.

80. For China, see Goldsmith, "U.S. Conventional Access Strategy." For Russia, see Dave Johnson, "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds," Lawrence Livermore National Laboratory, 2019, 73–74.

81. Jan Van Tol, "AirSea Battle, A Point-of-Departure Operational Concept," Center for Strategic and Budgetary Assessments, 2010, 56–59, https://csbaonline.org/uploads/documents/2010.05.18-AirSea-Battle.pdf.

82. Donald E. Vandergriff, *Adopting Mission Command: Developing Leaders for a Superior Command Culture* (Annapolis: Naval Institute Press, 2019), 3.

83. David R. DiOrio, "Operation Unified Response – The 2010 Haiti Earthquake," in "Campaigning," *The Journal of the Joint Forces Staff College*, Fall 2016, 52, https://jfsc.ndu.edu/Portals/72/Documents/JCWS/campaigning/Fall%202016%20Campaigning.pdf.

84. David S. Alberts and Richard E. Hayes describe six forms of decentralized command, from most to least centralized: 1. Cyclic. 2. Interventionist. 3. Problem-Solving. 4. Problem-Bounding. 5. Selective Control. 6. Control-Free. See David S. Alberts and Richard E. Hayes, *Power to the Edge: Command . . . Control . . . in the Information Age* (Washington: DoD Command and Control Research Program, 2003), 20; B. A. Friedman and Oliva A. Garard, "Technology-Enabled Mission Command," War on the Rocks, April 9, 2020, https://warontherocks.com/2020/04/technology-enabled-mission-command-keeping-up-with-the-john-paul-joneses/; and B.A. Friedman and Oliva A. Garard, "Clarifying Command: Keeping Up with the (John Paul) Joneses," War on the Rocks, April 7, 2020, https://warontherocks.com/2020/04/clarifying-command-keeping-up-with-the-john-paul-joneses/.

85. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States,* Joint Publication 1-0, (25 March 2013 Incorporating Change 1, 12 July 2017), I-18, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf. For evidence of the lack of mission command in U.S. armed forces, see Eitan Shamir, *Transforming Command: The Pursuit of Mission Command in the U.S., British, and Israeli Armies* (Stanford, CA: Stanford University Press, 2011); Vandergriff, *Adopting Mission Command*; and Donald Vandergriff and Stephen Webber, eds., *Mission Command: The Who, What, Where, When and Why* (CreateSpace, 2017).

86. Vandergriff, *Adopting Mission Command*, 10.

87. For more on this, see Christopher J. Lamb and Evan Munsing, "Secret Weapon: High-value Target Teams as an Organizational Innovation," National Defense University Press, 2011, 4, https://inss.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-4.pdf; Jim Thomas and Chris Dougherty, "Beyond the Ramparts The Future of U.S. Special Operations Forces," Center for Strategic and Budgetary Assessments, 2013, https://csbaonline.org/uploads/documents/SOF-Report-CSBA-Final.pdf.

88. Bryan Clark, Whitney Morgan McNamara, and Timothy A. Walton, "Winning The Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum," Center for Strategic and Budgetary Assessments, 2019, 42–44, https://csbaonline.org/uploads/documents/Winning_the_Invisible_War_WEB.pdf.

89. Sydney J. Freedberg, "'Algorithmic Warfare:' DSD Work Unleashes AI On Intel Data," Breaking Defense, April 28, 2017, https://breakingdefense.com/2017/04/dsd-work-unleashes-ai-on-intel-data-algorithmic-warfare/.

90. Rear Admiral (Retired) Mark Montgomery, CNAS Workshop.

91. Timothy M. Bonds, Myron Hura, Thomas Young, "Standing up a More Capable Joint Task Force Headquarters," RAND Corporation, 2011, https://www.rand.org/pubs/research_briefs/RB9625.html.

92. See Jennifer McArdle, "Victory Over and Across Domains, Training For Tomorrow's Battlefields," Center for Strategic and Budgetary Assessments, January 25, 2019, https://csbaonline.org/uploads/documents/Victory_Over_and_Across_Domains_Web.pdf.

93. Shane Bilsborough, "More Space Wargames, Please," War on the Rocks, November 17, 2020, https://warontherocks.com/2020/11/more-space-wargames-please/.

94. For more on how France used honeypots against Russian cyber operations, see: Sean Gallagher, "Macron Campaign Team Used Honeypot Accounts to Fake out Fancy Bear," Ars Technica, May 10, 2017, https://arstechnica.com/information-technology/2017/05/macron-campaign-team-used-honeypot-accounts-to-fake-out-fancy-bear/.

95. See Rachel S. Cohen, "Moving MDC2 from Research to Reality," *Air Force Magazine*, April 15, 2019, https://www.airforcemag.com/article/moving-mdc2-from-research-to-reality/; Valerie Insinna, "What's the end game for the US Air Force's command and control overhaul?" C4ISRNet, May 21, 2019, https://www.c4isrnet.com/air/2019/05/21/whats-the-end-game-for-the-us-air-forces-command-and-control-overhaul/; Eliahu Niewood, Greg Grant, and Tyler Lewis, "A New Battle Command Architecture for Multi-Domain Operations," MITRE Center for Technology and National Security, December 2019, https://www.mitre.org/sites/default/files/publications/Joint-All-Domain-Command-Control.pdf; Paul Birch, Ray Reeves, and Ray Dewees, "Build ABMS From Bottom-up, For The Joint Force," Breaking Defense, May 13, 2020, https://breakingdefense.com/2020/05/build-abms-from-bottom-up-for-the-joint-force/; and Valerie Insinna, "The Air Force tested its Advanced Battle Management System. Here's what worked, and what didn't," C4ISRNet, January 22, 2020, https://www.c4isrnet.com/air/2020/01/22/the-us-air-force-tested-its-advanced-battle-management-system-heres-what-worked-and-what-didnt/.

96. For more on DMO, see Kevin Eyer and Steve McJessy, "Operationalizing Distributed Maritime Operations," Cimsec, March 5, 2019, http://cimsec.org/operationalizing-distributed-maritime-operations/39831.

97. For more on CEC, see Eyer and McJessy, "Operationalizing Distributed Maritime Operations;" "CEC: Cooperative Engagement for Fleet Defense," *Defense Industry Daily*, May 10, 2019, https://www.defenseindustrydaily.com/cec-coooperative-enagagement-for-fleet-defense-updated-03120/.

98. For more on this threat, see Hinck, "Evaluating the Russian Threat to Undersea Cables;" David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *The New York Times*, October 25, 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html; Matsakis, "What Would Really Happen If Russia Attacked Undersea Internet Cables;" and Michael Birnbaum, "Russian submarines are prowling around vital undersea cables. It's making NATO nervous," *The Washington Post*, December 22, 2017, https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html.

99. Elsa Kania, "AlphaGo and Beyond: The Chinese Military Looks to Future 'Intelligentized' Warfare," Lawfare blog, June 5, 2017, https://www.lawfareblog.com/alphago-and-beyond-chinese-military-looks-future-intelligentized-warfare; and "'Intelligentization' and a Chinese Vision of Future War," Mad Scientist Laboratory blog, December 19, 2019, https://madsciblog.tradoc.army.mil/199-intelligentization-and-a-chinese-vision-of-future-war/.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.

As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, CNAS maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

© 2021 by the Center for a New American Security.

All rights reserved.

Center for a
New American
Security