



01

OPERATIONALIZING CYBER TO PREVAIL IN THE COMPETITION OF WILLS

BY COLONEL TIM HUENING, U.S. ARMY AND
COLONEL JOHN ATKINSON, U.S. MARINE CORPS

“The conduct of war is fundamentally a dynamic process of human competition requiring both the knowledge of science and the creativity of art but driven ultimately by the power of human will.”⁰¹ – Marine Corps Doctrinal Publication

“Fundamentally, war will remain a contest of wills.”⁰² – U.S. Army Operating Concept

In the wake of a decade plus of war, the nation is attempting to shift its focus to the Asia-Pacific and renew its commitment to a strategy of engagement to prevent war.⁰³ At the same time, the United States must maintain the capacity and ability to respond to crisis and prevail in war. For its part, the Joint Force must have the capabilities, attributes and skills to develop and conduct globally integrated operations.⁰⁴ The planning of these operations must leverage the synergy of a truly joint force in order to generate unified action.⁰⁵ Moreover, history and recent experience teach us that the Joint Force must improve its ability to visualize, understand, and describe the operational environment in order to direct and conduct integrated operations and campaigns. There is no doubt that in a disorderly complex world, the nation will demand more from its instruments of national power, especially its military, irrespective of shrinking budgets and end strengths. In fact, fiscal constraints and force reductions alone substantiate the need for a more efficient, effective and integrated joint force.

There are a number of service and joint efforts underway that will posture the Joint Force and enable it to better link and arrange actions and activities to

protect U.S. interests and achieve national objectives. If successful, these efforts will offer senior civilian leadership a broader array of acceptable approaches to effectively deliver favorable outcomes that contribute to the attainment of strategic objectives. Two efforts with potential synergistic overlap are the Strategic Landpower Task Force and the United States Cyber Command’s initiative to ‘operationalize’ Cyber.

The SLTF is a U.S. Army, U.S. Marine Corps and U.S. Special Operations Command tri-party effort envisioned to provide an operational description of how Strategic Landpower can contribute to the Joint Force’s ability to more effectively plan and conduct military operations. The SLP initiative is guided by what is commonly referred to as the ‘Clash of Wills’ white paper. This white paper is a seminal document endorsed by the Chief of Staff of the Army, the Commander USSOCOM, and the Commandant of the Marine Corps. The SLTF was initially chartered to, amongst other things, investigate the contemporary strategic nature and qualities of landpower; learn appropriate lessons from the recent past to frame the critical aspects of landpower; integrate a common understanding of achieving

physical objectives that influence human behavior in the formulation/execution of strategy, operational plans and tactical actions; and expand the social sciences dialogue regarding the physical science of warfare's influence on human behavior. Over time, the SLP initiative evolved into a holistic intellectual pursuit transcending landpower. The initiative currently aims to make the Joint Force and DoD more effective instruments of national power.

With this refined, yet more comprehensive approach, the SLTF seeks to re-emphasize the centrality of humans in war and warfare, and examine how the Joint Force thinks about, plans, and executes campaigns. As a first principle, the SLTF postulates that everything the Joint Force thinks and does must be founded on an appreciation of the human aspects of military operations. As a result, two inter-related Joint Concepts, the Joint Concept for Human Aspects of Military Operations⁰⁶ and the Joint Force Integrated Campaigning⁰⁷ spiraled out of SLTF thinking. If properly implemented and embraced, human-centric thinking and a dynamic approach to joint campaigning will allow the Joint Force to plan, direct, monitor and assess integrated operations that shape human decision-making and behavior and deliver favorable operational outcomes.

To this end, the SLTF seeks to identify and collaborate with other joint staff and service efforts that endeavor to better posture the Joint Force. Accordingly, the ongoing efforts to "operationalize" Cyber are of particular interest. This paper examines the confluence of Cyberspace and joint operations within the context of influencing human activity to achieve national objectives. It is intended to be an opening salvo in what the SLTF believes will be a rigorous, forthright, and collaborative examination of what is meant by, and more importantly what is required to, "operationalize Cyber."

Simply stated, without an appreciation for the HAMO, and lacking an operational approach to seamlessly link Cyber capabilities with other domains and functions, the Joint Force will fail to properly "operationalize" Cyber. The corollary, that the Joint Force will never achieve unified action or integrated campaigns without Cyber is also true.

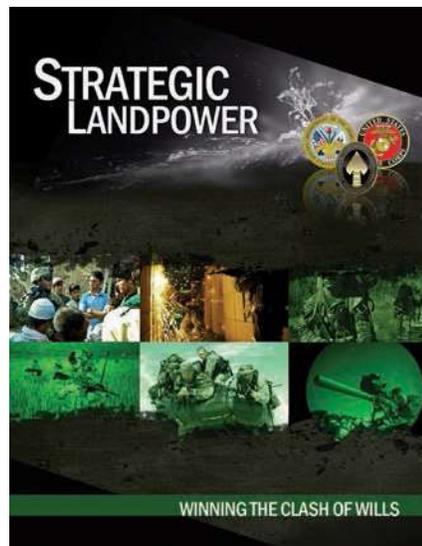
ON TECHNOLOGY AND THE PHYSICAL ASPECTS OF WAR

*"Technology is an enabler. Technology is that aspect of warfare that changes. The human element — war always being a contest of will — is an aspect of the eternal nature of war."*⁰⁸ — Dr. Lani Cass, National Defense University.

A focus of examination for SLP has been the dynamic relationship between human and technological considerations in war and warfare. This examination is informed by reflecting on the nation's post Cold War experience and the Department of Defense's embrace of the ideas offered by the Revolution of Military Affairs. The RMA constitutes an early assessment of the dynamic relationship between the human and technological nature of war the effects of which greatly shaped the U.S. military in the years leading up to 9/11.⁰⁹ In the wake of Desert Shield and Desert Storm, and the overwhelming application and display of American high-tech military might, in keeping with RMA, many of the nation's leaders were convinced that technology had not only changed the character of modern warfare, but also offered solutions to overcome the chaos, uncertainty and other primordial elements of war's immutable nature.¹⁰ Along these lines, Lt. Gen. H.R. McMaster recently lamented that advocates of what he called 'the orthodoxy of the RMA' predicted that advances in surveillance, communications and information technologies, when combined with precision-strike weapons, would

overwhelm any opponent and deliver fast, cheap and efficient victories.¹¹ Apostles of the orthodoxy believed that technology enabled the American military to overcome or bypass the human dimension in war, distilling conflict down to a mathematical equation vice a dynamic clash of wills. Recent experience in Iraq and Afghanistan, specifically the failure to understand the human aspects of the operational environment, are tragic reminders, bought and paid for with the blood of American Soldiers, Sailors, Airmen and Marines, that Thucydides, Sun Tzu, and Clausewitz were not wrong about the nature of war.

Nonetheless, the RMA drove DoD thinking, processes and policies for decades. Post Cold War budgets and programs were, and continue to be, implemented in a manner that belie a focus on the physical aspects of warfare, and a belief that wars can in fact be won easily and cleanly by way of technical military superiority.¹² Typical investment across the traditional domains — air, land, maritime, and space appear to reflect this thinking. Likewise, operational art has devolved into linear thinking, math-like processes and the rote application of physical capabilities against physical objectives. In fact, this situation caused some to declare that operational art died.¹³ With a few notable exceptions, service and joint doctrine and processes followed suit. The more complex, messy and intangible human aspects of war were set aside, and physical effects were seen as the path-way to operational outcomes.¹⁴ This reliance on technology and processes, when combined with other shortfalls in Strategic Art, has typically resulted in insufficient strategic guidance, a misalignment of ends, ways, and means, wholly military solutions, fleeting military successes and a consistent failure to deliver favorable political outcomes.¹⁵



02

01
Uniformed and civilian cyber and military intelligence specialists monitor Army networks in the Cyber Mission Unit's Cyber Operations Center at Fort Gordon, Ga.
U.S. ARMY PHOTO BY MICHAEL L. LEWIS

02
The Strategic Land Power Task Force's white paper commonly referred to as the "Clash of Wills." DoD PHOTO

Lop-sided match ups and victories like Desert Shield and Desert Storm engendered a belief that war had become a clash of technologies. Ironically, while the military outcomes of Desert Shield and Desert Storm were indeed impressive, they obfuscated the shortcomings of American strategy, the misguided discipleship of the RMA and other related initiatives, like Effects Based Operations, that came after. What was lost in the wake of Desert Shield and Desert Storm was the realization that focusing purely on physical targets in order to attain military objectives in the end failed to deliver conditions for sustained political outcomes. The reliance on technology and focus on the physical aspects of warfare within a limited operational context exemplifies a situation where military operations and warfare were confused with strategic objectives and war.

Furthermore, the thinking and by-products of the RMA, when juxtaposed to the Clausewitzian understanding of war, uncovers the broader and more insidious problem. That is, that American RMA operational and strategic thinking and approaches do not reflect a fundamental understanding that war is at its essence a human endeavor, a clash of wills driven by human passions like hatred, enmity, and fear, a competition that emanates from, and terminates in, the minds of men.¹⁶ It is humans that give war and the operating environment operational context. However, it is an understanding of, and a focus on, humans that is both required and lacking across all domains.

This flawed mindset and approach has adversely influenced the formulation of strategy and DoD's thinking and approach to war and warfare. Moreover RMA thinking has impacted how the services pursue their Title X responsibilities to organize, train and equip resulting in Joint Force shortfalls. Despite a National Security Strategy emphasis on engagement and understanding, the military industrial complex is resourced to generate

technical solutions to future challenges. This is troubling as recent and ongoing conflicts reinforce the need to understand the relationship between technology and the human, cultural, and political continuities of armed conflict.¹⁷ Such an understanding is necessary across all domains. This is a cautionary tale for the nascent and necessarily technical Cyber force as it seeks to "operationalize." There is evidence the leadership of U.S. Cyber Command and the service components recognize the danger of only considering the technical and physical aspects of Cyber.

OPERATIONALIZING CYBER

*The moral is to the materiel as three is to one.*¹⁸ — Napoleon Bonaparte

Shortly after taking command of USCYBERCOM in 2014, Adm. Michael S. Rogers identified "properly operationalizing Cyberspace"¹⁹ as USCYBERCOM's biggest challenge. He further articulated, that 'defending networks' is the 'niche' role and means by which the sub-unified Cyber Command will function at the operational level of war.²⁰ The admiral's recognition of the need to "operationalize" Cyber is a positive development, and one that is of interest to operational artists and commanders throughout the wider Joint Force. In fact it is not an overstatement to say that it is impossible to fully employ today's Joint Force without leveraging Cyberspace.²¹ It is

the integration of land, maritime, air, space, and Cyberspace operations that achieves campaign objectives.²²

The possibilities and perils of the Cyber domain are generally understood by military professionals at the rudimentary level. Unfortunately Cyber planning, capabilities development and operational employment are often left to technical experts. This techno-centric expert work is not fully known, understood or overseen by operational planners and commanders. A recent article penned by Brett Williams warned that, "Commanders cannot continue to run the risk of inappropriately delegating key operational decisions because they and their staffs lack an understanding of the (Cyber) domain."²³ Therefore, despite Adm. Roger's effort, the "operationalizing" of Cyber is not merely the purview of USCYBERCOM, service Cyber components or technical experts traditionally assigned to those formations. "Operationalizing" Cyber is a national security imperative that demands the interest, involvement and intellectual effort of the entire Joint Force — especially those who are charged with visualizing, describing and directing integrated joint operations and campaigns. "Operationalizing" Cyber cannot be limited to technological solutions, a singular warfighting function (command and control) or physical operations. What prevents us from taking this approach today is a lack of shared Cyberspace knowledge and an agreed upon operational approach that links



01

Joint service members from the U.S. Navy, Air Force and Army analyze a scenario during exercise Cyber Flag. U.S. AIR FORCE
PHOTO BY SENIOR AIRMAN MATTHEW LANCASTER)

01

Cyberspace missions and actions, and places Cyber activity in the larger context of joint operations. This will prevent the Joint Force from leveraging the capabilities necessary to compete and prevail in the emergent global operating environment subsequently preventing integrated operations and limiting joint force effectiveness.²⁴

The Cyber challenge is similar to the JC-IC and JC-HAMO challenge. The technology focused Cyber force appears to have already strayed from a human-centric understanding of war and military operations and is centered on the technical and physical missions of protecting and defending the nation's networks and infrastructure. Adm. Rogers highlighted the inadequacies of a defensive approach recently testifying a "purely defensive, reactive strategy will be both late to need and incredibly resource-intensive."²⁵ Senator John McCain echoed the admiral's concerns and added, "The failure to develop a meaningful Cyber-deterrence strategy has increased the resolve of our adversaries and will continue to do so at a growing risk to our national security."²⁶ In light of this testimony, it is apparent that USCYBERCOM must take a more proactive, effective, affordable and balanced approach to operations. This would of course include concentrating technical capability on offensive and defensive operations to achieve physical and psychological outcomes that influence human behavior.

Nonetheless, Defense Industry advertisements are an indicator of the persistent power of a false RMA perspective and a defensive approach to Cyber. A recent Northrop Grumman ad extolled the virtue of ubiquitous and dominant technological defense of networks and related physical infrastructure.²⁷ The ad describes a clash of technology with a singular focus on 'things'. There is no mention of humans, human behavior and human decision-making or human will. This is similar to ads seeking investment from the joint and service proponents of other domains – all promote the virtue of technology, the promise of certainty and dominance, and an unwavering focus on physical things, effects and objectives.

Of equal concern, the Cyber force and Cyber domain have become intellectually, organizationally and

IN THE END, IT MUST BE THE HUMAN BEHIND THE KEYBOARD THAT IS THE FOCUS OF ANY DECISIVE CYBER ACTION.

procedurally isolated from the inter-domain and Joint Force planning. This is the result of a reductionist domain-centric approach to joint planning by the broader joint force, that invariably leads to 'stove-pipe' versus integrated solutions. This renders the Joint Force a disjointed force, rather than an integrated Joint Force. In the face of adversaries who operate seamlessly across domains, disjointedness and reductionism will fail to produce unified action or desired operational outcomes.

This domain-centric isolation of Cyber is also driven by the composition of the personnel who comprise the Cyber organizations, most of whom are selected from the communications/signal, information technology and intelligence career fields. Technical expertise is vital for successful Cyber employment. However, experience gained during recent and ongoing conflicts suggest there are limits to the ability of technology to influence human behavior, effect cultural change, and drive political outcomes. The value of Cyber tools resides in their ability to contribute to an integrated campaign within the context of the continuities of armed conflict.²⁸

There is no doubt that networks need to be defended. However, in the context of joint military operations, these activities must be seen as continuing actions conducted to enable unified action simultaneously and in depth across all domains. In the end, it must be the human behind the keyboard that is the focus of any decisive Cyber action, and the action will only be decisive if it is informed by, meaningfully linked to and arranged with other more traditional actions and activities within an integrated joint operation or campaign.

JC-HAMO & CYBER

"The cultural, social, economic, religious and historical considerations that comprise the human dimension of war

*must inform wartime planning as well as our preparation for future armed conflict."*²⁹ — MG H.R. McMaster USA

Lessons learned from the last decade of war reinforce the need to understand social, cultural, physical, informational and psychological issues to influence actors and shape behavior. This understanding not only informs our activities but helps the Joint Force link and arrange military activities to achieve objectives that lead to desired strategic outcomes. The Joint Force is currently reassessing its ability to understand and account for these human aspects of military operations (HAMO) through the development of the JC-HAMO.

The Joint Force must leverage Cyber induced physical and cognitive outcomes more effectively to win the clash of wills. Cyber is one of many operational tools Joint Force planners and commanders must integrate into joint planning, operations, and campaigns. The Cyber Force, like the broader Joint Force, must re-emphasize human behavior outcomes to be effective. It is the integration of land, maritime, air, space and Cyberspace operations, developed in the context of HAMO that will influence human behavior to achieve campaign objectives.³⁰ In this context, efforts to operationalize Cyber and JC-HAMO are inextricably linked, and when understood and considered together provide an important consideration for those examining how the Joint Force should plan and execute campaigns.

JC-IC AND CYBER

*"It is essential to relate what is strategically desirable to what is tactically possible with the forces at your disposal. To this end, it is necessary to decide the development of operations before the initial blow is delivered."*³¹ — Bernard Montgomery

With a human-centric understanding and approach to warfare, including Cyber operations, the Joint Force can