Power Projection in the Digital Age

The Only Winning Move is to Play

By Darren McDew

Logistics is the lifeblood of the Joint Force. It requires an effective distribution network as its heart, moving and sustaining the force at the right place and at the right time—all the time. U.S. Transportation Command (USTRANSCOM) delivers that decisive force, projecting American power globally through the robust Joint Deployment and Distribution Enterprise (JDDE) and leveraging the expertise of more than 140,000 professionals. No other nation in the world can compete with the United States in conventional warfare because we plan, secure, and distribute combat capability so well. As a result, many military planners are now value-programmed to believe that a soldier or bullet will always be where it needs to be, when it needs to be there—on demand.

Established in 1987 to enable wartime transportation, USTRANSCOM now manages the continuous delivery of cargo and personnel in conflict and in peace. With a worldwide mission and ever-changing requirements, USTRANSCOM's success hinges on far more than sufficient ports, planes, ships, and trains. In this digital age, USTRANSCOM is completely dependent on the cyber domain to oversee, plan, and synchronize operations across the entire JDDE. This digital dependence incurs risk.

Our adversaries are keenly aware of this uniquely American strength and are pursuing advantages to undermine it, namely by disrupting our ability to operate in and through cyberspace. As our adversaries evolve their capabilities to exploit the cyber domain, we in turn must change the way we think about operating in the digital space. However, unlike the 1983 movie "War Games," which concluded the only winning move in thermonuclear war is not to play, we cannot afford failure in cyberspace—we *have* to play.

The Changing Battlespace

On February 8, 1904, Japan launched a surprise attack on the Russian-held Port Arthur on the Korean Peninsula, a critical logistics asset to Russia as a warm water harbor for their Pacific fleet. Russia responded with deployments along both a 5,500 mile Trans-Siberian railway and an epic sea journey by their Baltic fleet. However, Russia simply could not muster the combat power to aggregate forces against Japan in a

General Darren W. McDew, USAF, is the Commander of U.S. Transportation Command, one of nine Unified Commands under the Department of Defense. USTRANSCOM is a global combatant command with functional responsibilities for air, land, and sea transportation for the Department of Defense, ultimately delivering national objectives on behalf of the President and Secretary of Defense.

realistic time period. The rail line was single-track and non-continuous, requiring the trans-loading of all cargo from railcars to ships and back to railcars to cross Lake Baikal. The Baltic fleet sailed more than 20,000 miles from Europe and around Africa to find themselves with depleted supplies and lacking support against a superior Japanese naval fleet. After fighting through the night, Russia's Baltic fleet ceased to exist. With challenged and constrained lines of communication, Russia could not mobilize or sustain its military, and Japan forced it to negotiate. Today, our lines of communication exist as much in cyberspace as they do across rail and sea.

disruption may transcend USTRANSCOM's ability to deny, deter, or defeat, placing the nation's strategic objectives at greater risk. Logistics readiness is wartime readiness, and that means we need to guarantee superiority in the cyber domain to survive and operate effectively in the more traditional domains.

Current events show just how disruptive the cyber threat can be—leaked personal information, compromised email registrations, hacked financial databases, and massive denials of service or access. Each event further pushes conflict outside more conventional designations like peace or war. We must be emboldened to transform how we wage war in this new context, and that starts by redefining the changing

Logistics readiness is wartime readiness, and that means we need to guarantee superiority in the cyber domain to survive and operate effectively in the more traditional domains.

History demonstrates the pivotal role logistics plays in the success of a military campaign and how irrelevant the best laid plans become when a force cannot rapidly deploy or sustain itself. If we consider the changing battlespace from a historical perspective, it becomes instantly apparent that we cannot afford a deployment failure and that we must appreciate the vulnerabilities created by operating in cyberspace.

For the United States, the lesson is demonstrative—without USTRANSCOM's engaged cyberspace presence, an adversary could disrupt or deny movement within our distribution network and compromise or corrupt sensitive information. Without a corresponding cybersecurity focus to complement our developing physical capabilities, adversaries will augment their conventional forces with robust and practiced digital disruption skills to target our softer delivery support systems. This

battlespace. Specifically, the growing impact of the cyber domain permeates across parochial understandings of air, land, maritime, and space. Blurring the lines between these domains results in a gray zone where hostile actors can operate with limited attribution and with relative impunity.

Further complicating the gray zone is adversarial engagements in the digital space. Commercial industry represents roughly 50 percent of USTRANSCOM's wartime transportation capability, and nearly 90 percent of our traffic flows on unclassified networks to and from our commercial providers. USTRANSCOM operates in this cyber gap between our military and industry networks, spanning the jurisdictions of the Department of Defense (DOD) and the Department of Homeland Security (DHS). If we do not address this communication seam that exists between DOD and DHS,

we leave U.S. military logistics susceptible to an inability to rapidly aggregate combat power. Much like Russia struggled a century ago in protecting the timely delivery of their capabilities, we will be at risk of cyberattack or a cyber-enabled strike against air, land, sea, or space movements.

Physical control of the global commons is no longer enough to assure our ability to project power through increasingly contested distribution networks. We require a robust cyber posture as the foundation to protect ourselves from an adversary capable of achieving strategic objectives without ever using kinetic force. An adversary no longer needs to attack physical lines of communication to blunt American power. Instead, the adversary only needs to deny our ability to move the force by attacking our virtual lines of communication or injecting doubt into the system, causing us to question our operations or the integrity of our deployment data. Understanding the changing nature of war, our challenge is maintaining mission assurance in a cyber-degraded environment. Today, our logistical network stretches from the factory to the foxhole, and the means of controlling that network exist almost exclusively in the cyber domain—from the operational commander initiating a supply action to the enterprise tracking that item from receipt of request through delivery.

This logistical thread ties the modern battlespace together, and an adversary's ability to untie these connections to counter American power significantly dampens our inherent advantages and limits our freedom of action. Military planners often falsely assume that we will not face a contested environment until we are attempting to enter a theater, encouraged by military language that speaks to anti-access and area denial, and not global counter-power projection. Planners routinely look for an adversary to affect us with an arsenal of advanced capability-denying weapons like integrated air defense systems, anti-ship missiles or mines, intermediate-range or inter-continental ballistic missiles, or other kinetic forces. However, this assumption fails to address the universal applicability of the cyber domain in transregional, multi-domain conflict, and the ways modern technologies could extend conflict to the homeland.

Gaining a better understanding of the impact that cyber could have on our operations requires these planners to imagine a 21st century, Russo–Japanese War, or comparable scenario, in which we struggle to project power beyond the homeland. In our case, it would be a scenario where ships never leave port and aircraft never leave the runway; one where the planned, overwhelming force simply never leaves our shores. To prevent what would most certainly result in strategic shock, USTRANSCOM defines the changing battlespace for counter-power projection as the "contested environment," where adversaries continuously dispute American power across all domains, linked by the cyber-enabled delivery chain. With that definition, we are able to imagine concepts previously unfathomable and remain at the cutting edge of strategic thought.

Often exclusively understood as a specific engagement area or warzone, the contested environment actually extends across the vast array of organizations that deliver a force, from the continental United States to the warfighter. Digital tools and technology inform every step in the deployment process, creating multiple levels of possible interference. Since services, agencies, and Combatant Commands all observe risk differently, DOD's challenge is to use this expanded definition of "contested environment" to inform assessments and prioritize resources. In USTRANSCOM, accomplishing national objectives means reevaluating assumptions and addressing the potential for a deteriorating asymmetric advantage in strategic mobility. Assessing strategic risk in contested environments enables governmental agencies to

highlight each other's needs and vulnerabilities. This cooperation, in turn, enables the mitigation and coordination required to project power globally, particularly across the cyber domain. More importantly, strategic risk assessments highlight the operational planning considerations required to prioritize and defend global mobility assets, networks, and cyber infrastructure.

Leading the Way

Malicious cyber actors increasingly pose the greatest asymmetric threat to American military supremacy. Without superiority in the cyber domain, it will not matter how dominant the Joint Force is; if we cannot project power, then it does not matter how much of it we have. The USTRANSCOM team recognizes the need to seize the cyber initiative to safeguard transportation operations across all other domains, and to ensure operations through our strategic ports, rail corridors, road networks, and distribution nodes. Many of our Joint Force customers do not realize that the bulk of the force moves on commercial carriers whose information systems are even more vulnerable to cyber threats than hardened military networks. Therefore, we must change the way we view the character of war to preserve American dominance, assure the mission, and preserve military options and decision space for the U.S. President in the 21st century.

It is fair to say that only a short time ago, USTRANSCOM was admiring the cyber problem. Today, USTRANSCOM is on the leading edge of facing the challenge by developing the programs, processes, and personnel to address digital disruption threats. Russia's strategic mistake in 1904 was a failure to plan for rapid deployment, and today this means securing cyberspace. The inherent task for USTRANSCOM is to broaden the scope of its analysis into an assessment of hazards and responsibilities by actively evaluating the most vulnerable aspects of our command and control, systems, and infrastructure. In today's connected world, this assessment infuses digital awareness as a core principle of mission success and highlights the need for a resilient cyber network. Ultimately, our job is to assess these vulnerabilities and provide multiple options for the Joint Force while creating multiple dilemmas for the adversary.

With an area of responsibility that transcends geographic boundaries, USTRANSCOM began its cyber journey by realizing that the cyber domain forms the connective tissue of our entire distribution network. We reached this understanding by educating our leadership and key teammates. We invited experts from government, industry, and academia to participate in a series of cybersecurity roundtables. These experts included heads of cybersecurity firms, Chief Information Officers, scholars, and talented hackers. With their assistance, we began to shape a vision of mission assurance in cyber-threatened and cyber-degraded environments. These cybersecurity roundtables are now biannual events, designed to continuously expand the Command's perspective and establish a foundation for actionable progress.

USTRANSCOM also conducted its first "thin line" cyber assessment in 2016 and outlined how to employ fundamental security strategies and develop the means to deny or respond to cyber events. The thin line is the operating space that separates our key cyber terrain and infrastructure from an adversary's ability to affect our operations—a cradle-to-grave look at where our mission incurs risk from cyber. This first thin-line assessment also tackled hard challenges, such as the Command's reliance on commercial providers across disparate virtual infrastructures. Taking this broad view allowed us to expose numerous seams between military and commercial networks, quantify our limited authorities, and appreciate

the implication of DOD cyber standards that do not necessarily extend to industry. As a result, we are institutionalizing and accelerating our ability to conduct similar assessments while moving forward to secure network data across applications, protecting our mission-critical information. While the task was initially daunting in scope, a holistic approach helped us capture both the breadth of effort required and the depth of organizational impact. It also reinforced the need to treat cyberspace operations as central to mission assurance. After mapping out our critical cyber infrastructure and corporate relationships, USTRANSCOM successfully partnered with organizations like Defense Digital Services (DDS), Stanford University's "Hacking for Defense," and DOD's Strategic Capabilities Office (SCO) to better inform our cybersecurity needs and help us develop innovative solutions to some of our most pressing challenges.

Today, USTRANSCOM is refining its Cyber Mission Assurance Strategy and actively pursuing initiatives to bolster mission critical capabilities. In conjunction with DOD, Combatant Commands, services, and interagency partners, we identified and analyzed key cyber terrain to assist with prioritizing support from our limited cyber forces. We enhanced security protocols and better defined relationships with our commercial providers and government partners. USTRANSCOM is also path-finding the next generation of cybersecurity, thinking through vital cyber considerations in war games and simulations. We are correcting outdated assumptions about permissive operations, and as a result, developing an all-inclusive enterprise view of critical cyber roles and tasks. Our goal is to position every mission partner across our organization to see themselves contributing in one or more cyber lines of effort, to deliver digital mission assurance and inform our situational awareness.

However, cybersecurity means more than addressing current network needs. We must also protect our data and continue to improve our capabilities as technology develops. With an eye to the future, USTRANSCOM is leading DOD by adopting a cloud-based infrastructure that enables better encryption, empowers trusted transactions, enhances data management, increases storage, and scales network demands to support our unique logistical requirements. We know we have to stay at the forefront of the Department's focus on multi-domain conflict, continuously infusing cyber resiliency into our distribution mindset. Working with our Joint and commercial partners, we are developing a more robust, decentralized, and agile cyber infrastructure that provides cyber security and preserves our ability to move and sustain superior forces.

What is Next

The future of cybersecurity has three strategic defensive focus areas, each meant to address and progress network survivability: resilience, deterrence, and technology. By focusing on these three survivability areas, USTRANSCOM can prevent the digital disruption of its distribution network and protect against a contemporary equivalent of the Russian failures deploying to Port Arthur. Resilience strategies are those that maximize our ability to detect hostile actions and control damage. This approach includes real-time network monitoring and response, either through a user-driven or automated function, allowing quicker recovery. In promoting a reactive role, we accept risk in unclassified data, but this is critical to our ability to remain interconnected with our commercial providers. Deterrence strategies limit access or minimize network exposure to deny an adversary access to our systems. Though deterrence strategies have the benefit of effectively closing opportunities to the adversary, they restrict our own organic operations because of restrictions on connectivity.

In blending resilience and deterrence strategies together, a more complete mission assurance cyber strategy understanding emerges—we can expect a certain level of interference from an adversary, but we still seek to limit that access. The path to accomplish this is through the third focus area, the advancement of our technological capabilities. The cyber domain is growing at an ever-increasing rate, shortening the time span from state-of-the-art to obsolete each day. To operate effectively within our distribution network, we must stay at the forefront of this dynamic cyber transformation, continuously seeking out new ways to secure our operations. This task starts by harnessing the power that resides within our own data. It is not sufficient to simply digitize our existing activities—we have to leverage the data.

That said, when discussing data, we have to make an important distinction. Data should not be treated as mere information. Rather, data is living material, shaped through critical insights and aligned with key parameters to inform tasks. In USTRANSCOM, our data revolve around connecting the user to the supplier and the distribution network. We recently began the first steps of mapping and pooling our data into a proverbial "lake" to initiate the creation of accessible, annotated, and useful knowledge. This business intelligence will work to improve and optimize the management of our enterprise, enabling and promoting computer-guided gains in efficiency, flexibility, and effectiveness. A robust neural net of algorithms will advance our data and create the potential for machine learning and artificial intelligence, to anticipate, predict, and proactively respond to our needs. As self-sustaining technology, our networks would detect deviations and intrusions while refining their own software and algorithms, improving performance in real-time while enabling immediate threat response.

The evolution of big data analytics is what makes it "smart." By compressing the time from analysis to action, we can eclipse the human advantage and an adversary's ability to disrupt operations in a contested environment. In the not-too-distant future, machine learning will allow us to process information, identify shortfalls, and enable corrective action before human ability can detect a threat. As USTRANSCOM builds its data lake, we are transforming our cyber vulnerabilities from limitations to knowledge. With this groundbreaking shift in how we process information, we are also expanding the potential for autonomous systems and vehicles. Autonomy provides an incredible capacity to leverage data-driven, global situational awareness to better disperse our network vulnerabilities and promote resilience. In this manner, autonomy is the action arm of smart data, and it represents the most significant present-day disruptor to commercial transportation capabilities and capacity. Autonomous vehicles have the power to streamline the number of pilots, sailors, and drivers we need, minimizing risk and cost while allowing us to capitalize on industry's technological gains.

Though deterrence strategies have the benefit of effectively closing opportunities to the adversary, they restrict our own organic operations because of restrictions on connectivity.

A Call to Arms

If we ignore the cyber domain's role in our ability to project power and perform critical supply and sustainment missions, the adversary gains an easily exploitable advantage. As a result, we can no longer assume away delivery and transportation challenges. With a cybersecurity focus, USTRANSCOM will continue to perform its mission and enable the fulfillment of national objectives: delivering an immediate force expeditiously and a decisive force when needed—anywhere, anytime, all the time.

Commanders need to advocate constantly for senior leader attention on contested environments and cyber mission assurance problemsets. If an organization is not engaged in addressing cyber domain challenges, it cannot expect to dominate its competition.

However, USTRANSCOM's efforts are not enough—we cannot address cybersecurity in isolation. Leaders across industry and government will ultimately decide how to address the cyber threat as it continues to evolve and affect operations in yet undetermined ways. Commanders need to advocate constantly for senior leader attention on contested environments and cyber mission assurance problemsets. If an organization is not engaged in addressing cyber domain challenges, it cannot expect to dominate its competition. Prioritization is just one way to bring cyber to the forefront of an organization's focus.

Senior executive leaders should also pursue comprehensive workforce development and training to enable our cyber operators to remain relevant. We cannot expect to maintain an advantage in multi-domain operations or move a force with digital tools if we do not have the right talent with the appropriate training. Workforce development and human capital management take on new meaning and value in an era where military success no longer exclusively relies on how much combat power one brings to the fight. Instead, success may hinge on how quickly one detects and resolves cyber intrusions. As an organization, we need the same skilled information technology workers as the successful start-ups of our day, with whom we compete for talent. The other part of our challenge is hiring the right number and the right mix of military and civilian personnel. By leveraging the skill of our workforce with emerging tools and collaborative technologies, we can better allocate duties and work, and give our people the necessary time to think—to anticipate, adapt, and guide the agile responses a distribution network requires in contested environments.

Buoyed by executive leadership advocacy and explicit workforce development, we advance the dialogue where cyber security is a pillar of mission assurance. In this vein, we should seek to collectively set and enforce digital standards for the hardware and software involved in our distribution network and those we do business with—how and where we design, manufacture, maintain, install, and connect systems. For USTRANSCOM, that means investing in the infrastructure that supports and delivers our warfighters while protecting its ability to provide

options and solutions to complex delivery problems. We are in a battle to gather and process data at faster and faster rates, and to make informed decisions when confronted with these problems; this requires the intentional development of our cyber infrastructure. With a resilient and secure network, we will enable the Joint Force to develop and prepare for operations in contested environments, accept or mitigate strategic risk, synchronize operations, and deny an adversary from pursuing asymmetric advantages across all domains.

The Only Winning Move is to Play

Functional views of USTRANSCOM's Combatant Command role do not provide enough emphasis on the critical nature of our cyber networks and infrastructure, nor on the importance of the JDDE and Global Deployment Network within DOD. Our mission requirements transcend geographic Combatant Command areas of responsibility and necessitate the ability to project force wherever and whenever needed. By partnering with industry and innovative organizations to better understand our mobility requirements, USTRANSCOM can safeguard American power across contested domains. We need to imagine the art of the possible, exploring the latest capabilities to resolve our inefficiencies and educate our personnel. We need to continue to lead and foster relationships, to better understand the next tasks that will shape our digital future and raise the level of connection to our data. We need to promote a multi-domain endstate, not advocate for targeted advancements or stove-piped outcomes.

The more successful we are, the more our adversaries will attempt to contest our influence, having potentially catastrophic consequences. By pursuing cybersecurity as a means to ensure global power projection, the United States can preserve its superior advantage in conflict. These are not solely technical issues, nor are they owned by any single entity within the JDDE. These are strategic issues. Leaders at all levels must continue to address cyber-specific challenges and recognize the consequences of cybersecurity failures, both in our policy and in our operations. Together, we can create the unity of purpose and effort required to deliver solutions. As a result, our adversaries will have fewer opportunities to degrade our mission capability. Future attacks will be less likely to succeed, and if they do succeed in disrupting operations, we will effectively mitigate the impacts to our overall mission and to the Joint Force Commander's ability to execute.

To succeed in cyber, one must play the game. The ancient Chinese strategist and philosopher Sun Tzu famously noted, "To subdue the enemy without fighting is the acme of skill." The advent of advanced cyber capabilities and related gray zone activities make this concept appreciably more realistic and contemporary. Although the connectivity and transactional speed enabled by cyberspace have revolutionized the way we think about command and control, information sharing, and operations assessment, our growing dependence on digital tools creates tremendous vulnerability. Russia's defeat at Port Arthur more than century ago is a compelling example of the tyranny of distance and the consequences of allowing logistics to exist as an afterthought. The reality is that scores of similar examples permeate across history, highlighting the direct relationship between logistical shortcomings and strategic failure. Viewed through the lens of the changing digital battlespace, we depend on the cyber domain to project power. We simply cannot afford to ignore or downplay the threat. PRISM