







Here, there, and everywhere

The key to military competitive advantage is omnipresence

A report by Deloitte's Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Deloitte's Defense and National Security sector is focused on helping our clients address their most important opportunities and most difficult challenges. We support all of the military services and agencies in DHS, DOJ, and the intelligence community. The military services include Army, Navy, Air Force, Marine Corps, the Combatant Commands (for example, Special Operations Command), the Office of the Secretary of Defense (OSD) and the Deputy Chief Management Office (DCMO). The merger of DHS, DOJ, and Intel was a natural consolidation, as our clients all serve a similar cause: keeping the people of America safe. Our vision is to be recognized as the leading provider of world-class solutions to support the business and strategic priorities of the Defense and National Security sector.

CONTENTS

Introduction 2
Making your presence felt 3
How to be everywhere at once 4
Toward a unifying concept 8
(Off)setting the agenda 10
Crossing the Rubicon 12
Endnotes 13

Introduction

RESH from lopsided victories off the coasts of China and North Africa, the early 19th century British Navy sailed into a new era of naval dominance. Its newly commissioned steam-powered ships provided decisive military advantages, and the nation was giddy with possibility. The *Observer*, a British weekly newspaper, could barely contain itself when it declared in 1842 that, "Steam, even now, almost realizes the idea of military omnipotence and *military omnipresence*; it is everywhere, and there is no withstanding it."

One hundred years later, Werhner von Braun, a German engineer, suggested a different approach during a 1950 US Air Force-sponsored conference in Chicago. Von Braun had been secretly whisked away to the United States as part of an initiative to outpace the Soviet Union's rocket propulsion and space programs. He described for the rapt attendees the details of a rotating space station that would orbit the earth in less than two hours and cover the entire planet in about a day. Knowing his audience, he quickly launched into its military uses: "Our space station could be utilized as a very effective bomb carrier, and the nation who owns such a bomb-dropping space station . . . will have *military omnipresence*." 2

Today, the US Department of Defense (DoD) is looking for the next set of technological breakthroughs that can increase its military advantage over those of competing nations. Its goal is to prevent future wars by maintaining a military that can exercise its will anywhere in the world at any hour.³ Or, as past

presidents and defense leaders have put it, a military that can engage "at the time and place of our choosing." In other words, the DoD is looking to make military omnipresence a reality.

This strategy to regain our fighting edge has been called the Third Offset. But whether given this or some other name, one of its primary shortfalls is that it lacks a unifying concept. Many believe the present strategy is too focused on futurist technologies. And some scholars have argued that it seems to have "no clear purpose or urgency." While the First Offset was the strategic deployment of miniaturized nuclear weapons and the Second Offset was the enabling network for precision strikes, the Third Offset seems to lack the same clarity and focus.

Military, or operational, omnipresence is the answer to this dilemma. And unlike steam engines or rotating space stations, today's advances in technology make the supporting architectures for the concept possible. This is the orienting principle the Department of Defense needs in order to organize its current strategic efforts and regain its competitive advantage.

This study will make the case that operational omnipresence, considered by many to be the holy grail of military objectives, can today be achieved through the coordinated use of existing and imminent technologies and is the unifying concept that can usher the US military into another era of preeminence.

Making your presence felt

OR centuries, military planners have battled to overcome the obstacles presented by geography and information. Whether 19th-century muskets or 21st-century cyber weapons, the goal is the same: to be better positioned to take action against an adversarial nation quicker than it can respond. This not only requires the ability to gain a time-distance advantage, but also to collect, analyze, and integrate pertinent information in less time. The piecing together of this puzzle is the source of competitive military advantage.

The key to it all is *forward presence*, a concept that's been a US military preoccupation since at least World War II. Forward presence is the deploying or stationing of forces overseas to demonstrate national resolve, strengthen alliances, dissuade potential adversaries, and enhance the ability to respond quickly to contingencies.⁷ Ultimately, presence is the crux of US military strategy.

Recognizing this, in 1995 the US Air Force secretary and chief of staff co-authored a white paper calling

for global presence, which they defined as "the full range of potential activities from the physical interaction of military forces to the virtual interaction achieved with America's information-based capabilities." They envisioned that the combination of rapid deployment, precision munitions, and surveillance would make the military "more mobile, more lethal, and more *omnipresent* than ever before."

These Air Force leaders were on to something. Though their formulation was limited by the technology of the day, the primary insight still holds: increased presence is fundamentally a matter of networked interdependence. That is, omnipresence requires that not only must military forces and information-gathering systems rely on one another, but that each ship, plane, unit, weapon, and satellite must be capable of direct, intelligent interactions with one another. This is exceptionally difficult, which is why the supporting architecture that enables these connections is the basis of an enduring competitive advantage over other militaries.

How to be everywhere at once

MNIPRESENCE suggests being everywhere at once, and, of course, this is physically infeasible. Even attempts to establish more presence—by increasing the number of ships and planes, drones and unmanned vehicles, global deployments, and overseas bases—can fall far short. Moreover, pervasive physical presence is often precluded by its excessively high financial and political costs. But technological advances make other forms of presence possible. For example, cyberspace enables virtual presence in places where physical access isn't feasible. And satellite surveillance affords awareness of events occurring in inaccessible physical and virtual spaces, giving the perception of presence. Together, it's possible to reach some semblance of ubiquity.

Thus, operational omnipresence has three primary interconnected components: physical assets, virtual capabilities, and information. It is the culmination of where you are, where you can be quickly, and awareness of what is occurring everywhere else. Because the United States has global responsibilities, the sheer amount of national security interests it has around the world can make omnipresence difficult to achieve. But the model of interconnected presence, though difficult to establish, is proven.

Consider the omnipresence of the US banking industry. Its physical presence is substantial; there are nearly 100,000 brick-and-mortar banking offices and more than 500,000 ATMs.¹⁰ This means there is a bank or ATM for every 500 people in the United States. Virtually, banking services can be accessed at any time and from nearly any location

via telephone and software applications, including some banks that are based entirely in cyberspace. And banking information, from commercials and digital ad space to financial transaction data, is abundant and easily accessible. The combination of these different forms of presence make banking inescapable, but the architecture that facilitates the interactions between each of these elements makes banking omnipresent.

To make operational omnipresence a reality, physical, virtual, and perceived presence must first be established. And this requires surmounting the formidable challenges of time, distance, and information.

The tyranny of time, distance, and information

In international armed conflict, geography has long been a central consideration. The time and cost associated with moving large armies across vast expanses makes it one of the most complex challenges a nation can undertake. Sun Tzu, the 5th century BC Chinese military strategist, observed, "If you are situated at a great distance from the enemy, and the strength of the two armies is equal . . . the fighting will be to your disadvantage." Even more, "Geography attenuates a stronger military's advantages over a weaker regional foe fighting on its own ground." ¹²

This reality may be considered both a blessing and a curse for the United States. Fortunately, being sandwiched between two oceans means other nations must travel great distances to reach its lands. But it also means US forces must travel great distances to engage adversaries. To address this, the Department of Defense built a military that could overcome the disadvantage of distance and fight wars away from home—an approach that hinges on being present in places far away from its own shores.

This strategy is costly. Consequently, immense amounts of information about the opposing forces,

their capabilities, and their intentions are required to justify our military costs. Further, information about the environment and the conditions in which conflict may occur also shape military plans. Nations can't risk losing large chunks of their forces by sending their military into harm's way unprepared for the awaiting fight. Whereas militaries of the past had to operate with a relative lack of information, today's militaries must operate in an abundance of it. In the end, all other things being equal, the side with the information advantage has a distinct upper-hand; it is central to success.

Information, however, must not only be available, it must be accurate. Because information is exponentially more available and accessible today, it can be particularly difficult to ascertain what is most important and accurate, how best to integrate it, and the most efficient way to protect its integrity and continued availability.

To further complicate things, nations have long employed de-

ception to hinder the information-gathering and verification process. For example, military lore from World War II references a German airfield specifically constructed to deceive Allied forces; the planes, hangars, trucks, and oil tanks were all fake and made of wood. It was intended to provide false information to surveillance planes. But because of a multifaceted information-gathering campaign and intelligence analysis, the Allied forces knew the airfield was a decoy. In a bit of gamesmanship, once construction of the fake airfield was complete, an Allied plane circled it a couple of times before dropping one large wooden "bomb" on it.

The tyranny of time, distance, and information—the significant difficulties associated with operating

> across great distances and a major problem that operathree components of presperceived.

needing to be quick and sure-footed in doing so-is tional omnipresence must solve. It can do so via its ence: physical, virtual, and

Greater than the sum of its parts

For decades, whenever a crisis emerges, one of the first questions presidents have asked is, "Where are the carriers?"13 Aircraft carriers provide a mobile and potent physical presence, and no other nation even comes close to matching the quantity and quality of the US military's fleet. This is just one example of how important physical presence is to US military strategy.

Physical presence is the strategic positioning of mili-

tary forces around the world so that they are always in relative close proximity to contingencies. In addition to deploying ships and planes that provide physical presence, the US military maintains more than 150,000 servicemen and women on 800 bases in 70 different countries.14 This is the most expansive military footprint of any nation, holding more

Operational omnipresence has three primary interconnected components: physical assets, virtual capabilities, and information. It is the culmination of where you are, where you can be quickly, and awareness of what is occurring everywhere else.

than 95 percent of the world's foreign bases at a cost of more than \$150 billion annually.15 And the current presidential administration has articulated its goal to increase physical presence in a recent executive order that seeks more ships, planes, and personnel.16 Meanwhile, unmanned and autonomous vehicles and drones can greatly increase physical presence at a reduced cost.

But even with the incredible coverage provided by this level of forward presence, it can still fall short. Competitors fashion their militaries specifically to prevent or complicate the US military's physical presence-an evolving strategy often called "antiaccess, area denial." These nations' surveillance systems and weapons are programmed to identify and

In the end, all

other things be-

ing equal, the side

with the informa-

tion advantage

upper-hand; it is

central to success.

has a distinct

locate US forces and engage them at far-off distances. For example, the Chinese military has developed a long-range missile that is specifically designed to hit US aircraft carriers long before they can get close enough to launch aircraft.17 The world is simply too large, other nations' militaries too advanced, and costs too high for physical presence to provide operational omnipresence on its own.

Virtual presence can fill the gaps. Previous conceptions of virtual presence have limited it

to physically "being nearby," 18 or passive presence via technology.19 In fact, admirals and generals have lamented that in the eyes of US allies, such "[v]irtual presence is actual absence."20 But technological advances allow an expansion of the concept, transforming virtual presence into a proactive and consequential form of presence.

Virtual presence is where force can be applied quickly from a distance, from nanoseconds to hours, and includes cyber and electronic warfare, directed energy, and even hypersonic weapons. The expansion of the military's cyber force has improved its ability to take action against adversary nations by digital

means. Moving at the speed of light from thousands of miles away, cyber weapons can establish forward presence virtually without the cost and risk associated with physical presence. And it can have effects beyond the virtual space, impacting physical targets by modifying the software that controls them.

Similarly, directed-energy weapons focus high quantities of energy on a target to disable or destroy it and can reach their destination in nanoseconds. The US Navy and Air Force are currently testing new weapons that use microwave pulses or laser technology, and they're expected to be ready for operational use in the next few years. Also in development are hypersonic missiles that fly the equivalent of three marathons in one minute, making it

> geted nation to respond quickly enough. Other emerging capabilities, such as the electromagnetic rail gun that can launch nonexplosive projectiles at hypersonic speeds, are additional arrows in the virtual presence quiver. Together, gaps in physical presence can be filled virtually and done so faster than at any point in history.

> In a networked world, the ubiquity of digital connections means that virtual presence is absolutely essential to any notions of operational omni-

presence. It can complement physical presence by reaching into areas where physical access isn't possible or practical, such as deep into heavily fortified territories or networks where software, not hardware, is the target. Further, virtual presence leverages technical advances that make weapons moving at light and hypersonic speeds possible, resulting in approximate physical presence.

Yet, a large physical presence in all corners of the globe supplemented by virtual presence in digital networks and the fastest weapons on earth are still insufficient for operational omnipresence. Gaps will still exist. And competitor nations will likely

exceptionally difficult for a tar-

attempt to identify these gaps and develop an ability to operate there, out of reach from physical and virtual military forces. Russia, for example, is employing tactics that attempt to disrupt US virtual advantages through advanced electronic and cyber warfare. For operational omnipresence to be a reality, awareness of what's happening in these dead zones is paramount.

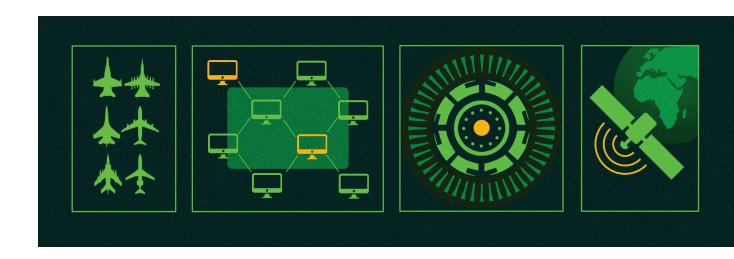
Perceived presence is the use of technology to collect information and monitor events occurring in places where physical and virtual presence aren't possible. Though it doesn't permit the application of force, the perception of being watched influences behavior.

Consider the panopticon, a conceptual structure devised by 17th century English social reformer and philosopher Jeremy Bentham.²² The building was designed so that prisoners could be observed from a single room without being able to tell whether they were actually being watched. It was a circular structure with a watchtower in the center and prisoners placed in cells around it. The windows into the watchtower were obscured by iron mesh or some other scheme to ensure guards could see out, but prisoners could not see in. In this way, prisoners knew they could be seen, but could never be sure if they were being observed. This uncertainty, Bentham posited, would cause prisoners to govern their own behavior, even when the watchtower was emp-

ty. Today, cyber and satellite constellation-enabled surveillance, coupled with traditional forms of intelligence gathering and the ubiquity of the press and personal devices, means that a global electronic version of the panopticon is possible. This is perceived presence.

Moreover, if you can be surveilled, you can be located. This is particularly important because if, for example, prisoners under the eye of a prison panopticon are never caught or punished when they violate rules, the scheme loses its effectiveness. So not only should behavior be observable, but there should be consequences when behavior violates norms. Today, for example, using perceived presence, the DoD could observe a nation's covert and illicit occupation of disputed islands in the open ocean. It would confirm it through satellite imagery and the collection of radar or infrared emanations. Revealing this information would expose the offending nation's actions and influence its future decisions. What was done in the dark is now under a spotlight. From that point forward, it would assume it's being watchedthis is a form of presence.

For perceived presence, consequences can come by means of public exposure of the norm-violating behavior or the threat of force by physical or virtual means. In this way, the perception of presence can begin to approximate the effects of actual presence.



Toward a unifying concept

ITH physical, virtual, and perceived presence established, operational omnipresence is possible. But for it to become real, previous offset strategies show that each element in each strategy should be networked and interdependent. Their clear and concise unifying concepts should be focused on the nation's efforts, bundling together several initiatives and pointing them toward the same goal. The establishment of such a concept is critical to the success of any offset strategy.

First offset

The First Offset was President Eisenhower's New Look national security policy during the 1950s. Its goal was clear: Use nuclear weapons to counter the size of adversaries' larger militaries. Eisenhower believed that trying to match Soviet and Chinese armies' man-for-man was an exercise in futility.²³ Moreover, he deemed the large loss of human life and the economic costs of waging traditional war to be an unacceptable burden to the nation.²⁴ To deter other countries, specifically the Soviet Union, he advocated for the widespread deployment of nuclear weapons and the ability to launch them deep into enemy territory.

Nuclear weapons, however, were large, cumbersome, and hard to deliver. And determining where to place them to ensure the best military advantage required intelligence about Soviet forces and capabilities. Technological advances were aimed at solving the associated time, distance, and information (tempo-geo-info) challenges. Nuclear weapons were

miniaturized and were placed on submarines covertly positioned around the world. Long-range jets that could carry these weapons thousands of miles were mass produced. Land-based ballistic missiles were built and were ready to launch at a moment's notice. New military and intelligence organizations were formed, and spy planes were designed to fly at extremely high altitudes and collect information on enemy forces.

With strategic nuclear weapon positioning as its unifying concept, the First Offset oriented technological advances to overcome the tempo-geo-info problem. Not coincidentally, it also took an incremental step toward operational omnipresence. The strategic positioning of nuclear-capable planes, ships, and missiles established forward presence and provided a global competitive advantage. The inexorable tie between increased presence and offset strategies became clear.

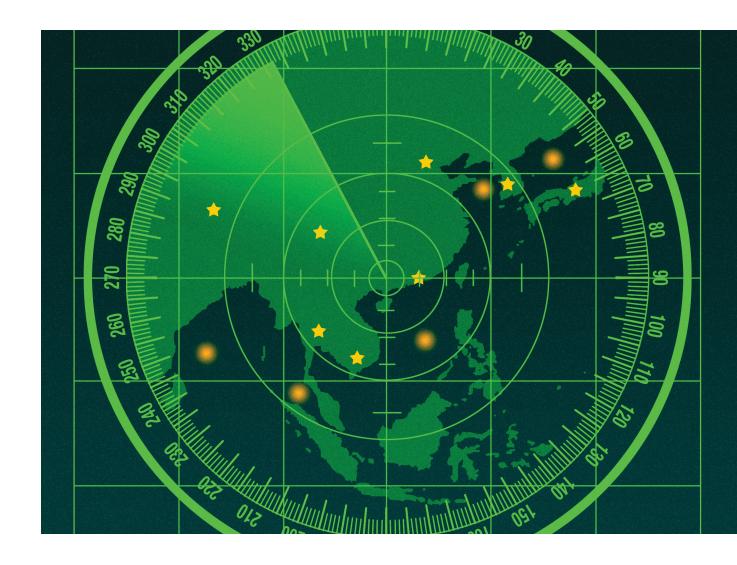
Second offset

The Second Offset stayed true to form. By the 1970s, the Soviet Union's advances in nuclear and propulsion technologies were eroding the United States' military edge. Further, the Soviets still maintained a larger military and a geographic advantage in its proximity to US allies in Europe. To combat this, US defense leaders devised a strategy that centered on near-zero-miss munitions. That is, they bet a military that could be extremely precise with a few missiles would be more lethal than one with lots of bombs that often miss. One good smart bomb is worth dozens of dumb ones.

The unifying concept of the Second Offset, then, was precision-guided munitions. Many of the innovations and technological advances occurring in government and in the commercial sector were then oriented to support this strategy. For this technology to work, a missile must know exactly where in the world it is and exactly where the target is. A global positioning system was developed to provide this capability, and weapons were built that could talk directly to it for locational data. A robust constellation of intelligence-gathering satellites were launched that provided detailed information on where targets were situated. Improvements in stealth technology allowed planes and ships to get closer to adversary territory and put their firepower

to use. The incredible amount of technology required to enable each of these elements worked only because they were working toward the same clear objective: precision strike.

Yet again, this offset strategy tackled the tempogeo-info challenge head-on. Stealth and precision munitions permitted closer approaches to adversaries and scoring direct hits on targets. More capable ships, planes, and other weapons made presence more efficient, accomplishing more with less of a physical footprint. And a vast information-gathering apparatus allowed military plans and operations to be more targeted and tailored. This was made possible by the information networks that supported every step of the process.



(Off)setting the agenda

FFSETTING the gains of other nations' militaries, then, is not just about more ships and planes. It's not just improved cyber, hypersonic, and directed-energy weapons. It's neither a vast surveillance network nor artificial intelligence. It is *all these things* in an interconnected, interdependent system that requires fundamental transformations of the interactions between technologies, organizations, and personnel. This structure is not easily replicable, even if other nations acquire some of its technological components. As such, it creates a viable and enduring offset to competitor nations.

Operational omnipresence is only realized when physical, virtual, and perceived presence are stitched together in an evolved architecture that fully leverages the advantages of each of its components. It requires technological advances to fully achieve each form of presence, but it also requires refashioned connections between them. Architectural innovation, defined as "the reconfiguration of an established system to link together existing components in new ways," requires a fresh evaluation of information streams and processes, unbound by an organization's tendency to do things as they always have. ²⁵ Put simply, operational omnipresence is a herculean task that requires advanced technologies and new ways of doing business.

As political strategist and Army officer Thomas Adams wrote over a decade ago:

"The effective use of such technologies will require rapid, effective, and close interaction between many different systems. This kind of new and subtle interaction will require radical changes in the architecture and integration of these interconnected and widespread [data collection and processing] systems. The actual achievement of solutions for the integration of such large, complex systems will be a long process involving extensive experimentation."²⁶

The heaviest lift is the necessity for near-real-time analysis of massive amounts of information. Technological advances mean that conflict can occur at machine-speed, and the information generated and gathered by the multitude of weapons, unmanned and autonomous systems, digital communications, and sensors can quickly overwhelm any ability to process and be responsive to it. The networked interdependence of every element of presence and the information required to support it "produce a data overload that will make it difficult or impossible" for humans to direct in a timely fashion.²⁷

General David Goldfein, the current chief of staff of the US Air Force, believes competitive advantage depends on "harnessing vast amounts of information, fusing it quickly into decision-quality information, and taking action by any available means anywhere in the world."²⁸ This means that information systems will need to bear more of the burden to review information, learn from it, and make immediate recommendations to decision makers—and, in some cases where the risk to life or the mission is at stake, take an action itself.

To enable this, operational omnipresence requires a common operating system, an architecture that supports real-time information exchanges between every component in the system of systems.29 Supercomputing power is necessary. Artificial intelligence across the system is critically important. Humanmachine pairing is vital. They are the means by which all of the data can be reviewed and analyzed, transforming presence from three sectored capabilities into a synthetic organism that can sense and respond to the environment around it with human direction.

Here is how it could work: When an aircraft carrier attempts to sail into waters within the range of a ballistic missile, satellite and spy plane collection

Operational

in an evolved

would detect the launcher's radars and communicate directly with the carrier. Virtual presence in the nation's command systems or launch software could delay the missile's ability to target the carrier. Should launch occur, collection of the missile's flight would be collected, analyzed in near-real-time, and communicated to all ships, planes, and defensive weapons in the area. Cognitive technologies would provide information to directed-energy platforms, rail guns, hypersonic missiles, and other countermeasures. At every point of the missile launch and flight, presence would be established and the interactive capabilities would provide a range of

options to ensure the carrier is never in danger of being hit. The systems to carry this out either exist or will imminently. But developing the architecture to support the required real-time, multiplatform information exchange is how operational omnipresence becomes possible.

Concurrently, organizational structures within the Department of Defense should change to accommodate the evolving role and salience of information processing. Experimentation toward this end has begun with the Joint Interagency Combined Space Operations Center (recently renamed the National Space Defense Center), a new organization designed to facilitate information sharing and fusion, experiment with new tactics in space-based surveillance and operations, and battle management across the different areas of presence.30 Other efforts, such as the Army's "multi-domain battle" and the Navy's electromagnetic maneuver warfare, are further evidence of the architectural changes occurring to facilitate increased presence.31 With these initiatives,

> the hierarchy of disparate systems elements-satellites, sensors, weapons, ships, planes, personnel, and cyber and other digital capabilities-is replaced by a flat, interactive system where direct interaction is possible between any two elements. This makes submarines launching cyberattacks, planes disabling satellites with directed energy, and portable networks taking autonomous actions to heal themselves and counterattack all within the art of the possible.

This is operational omnipresence. It is advanced warfighting that can only be accomplished by organizations that are willing and

able to evolve and create the capabilities necessary to make the conceptual, reality. It requires tailored innovations and a fundamental rethinking of processes. And because it is so difficult to do and requires systemic change, it cannot be easily copied. If mastered, the US armed forces' margin of advantage over competing nations will grow.

omnipresence is only realized when physical, virtual, and perceived presence are stitched together architecture that fully leverages the advantages of each of its components.

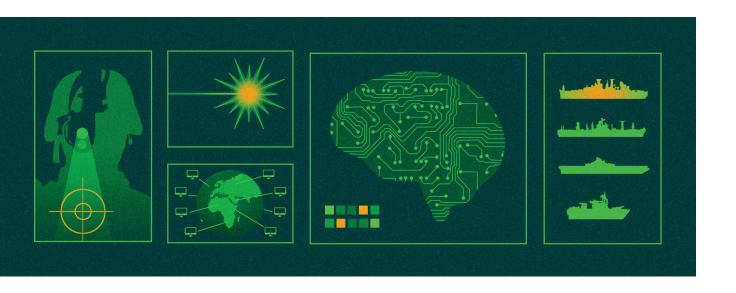
Crossing the Rubicon

N 49 BC, Julius Caesar led his army across the Rubicon River and invaded Italy, an action that could not be undone given the laws of the day. It's memorialized in the idiom "crossing the Rubicon," which has come to mean a revolutionary action from which one cannot successfully turn back. One of the US Navy's first modern electronic warfare weapons was given the prescient name RUBICON.³² It was capable of jamming communications, degrading data links, and even intercepting and spoofing older forms of cellular communication. In a single platform, there was physical, virtual, and perceived presence.

We have crossed the Rubicon. Technological advances and their military applications cannot be undone. Operational omnipresence seems to be the

logical next step in the progression of the changing character of warfare. The strategy to recover lost ground in our fighting edge over other nations needs this sort of unifying concept to ensure technological and architectural innovations are working toward the same goal. Without the vision of operational omnipresence to bind disparate efforts into a cohesive strategy, the US military runs the risk of a further eroding advantage.

The future of conflict, like its past, requires dominion over the time, distance, and information associated with operations. The Department of Defense is making progress in this regard, but it should continue adapting, innovating, and evolving until operational omnipresence is achieved.



ENDNOTES

- 1. Andreas Malm, "Steam: Nineteenth-century mechanization and the power of capital," *Ecology and Power: Struggles over Land and Material Resources in the Past, Present, and Future*, edited by A. Hornborg, B. Clark, and K. Hermele (New York: Routledge, 2012).
- 2. Werhner von Braun, "Multi-stage rockets and artificial satellites," *Space Medicine: The Human Factor in Flights beyond the Earth*, edited by John Marbarger (Urbana: University of Illinois Press, 1951).
- 3. Ian Livingston, "Technology and the Third Offset' foster innovation for the force of the future," *Brookings Institution*, December 9, 2016, https://www.brookings.edu/blog/order-from-chaos/2016/12/09/technology-and-the-third-offset-foster-innovation-for-the-force-of-the-future/.
- 4. See, for example, President Barack Obama (http://www.npr.org/2016/12/19/504998487/transcript-and-video-nprs-exit-interview-with-president-obama), President George Bush (http://www.presidency.ucsb.edu/ws/?pid=63645), Secretary of State Colin Powell (https://2001-2009.state.gov/secretary/former/powell/re-marks/2001/2864.htm), and General Vince Brooks in *The Iraq War and Its Consequences*.
- Remarks by Deputy Secretary of Defense Bob Work, Brussels, Belgium, April 28, 2016, https://www.defense.gov/ News/Speeches/Speech-View/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy.
- 6. Lawrence J. Korb and C. Evans, "The third offset strategy: A misleading slogan," *Bulletin of the Atomic Scientists* 73(2), pp. 92–95.
- 7. Department of Defense, "DOD dictionary of military and associated terms," Joint Publication 1-02, March 2017.
- 8. Sheila E. Widnall and Ronald R. Fogleman, "Global presence," Joint Forces Quarterly, spring 1995, pp. 94–99.
- 9. Ibid.
- 10. FDIC, "Brick-and-mortar banking remains prevalent in an increasingly virtual word." FDIC Quarterly 9(1), pp. 37–51.
- 11. Sun-Tzu, as in Samuel B. Griffith, The Art of War (Oxford: Clarendon Press, 1948).
- 12. James Holmes, "The tyranny of distance," *Foreign Policy*, January 18, 2016, http://foreignpolicy.com/2016/01/18/desert_storm_saddam_hussein/.
- 13. George W. Bush, remarks at the christening of the USS RONALD REAGAN, March 4, 2001, http://www.navy.mil/navco/pages/2002/gwbush010304.txt.
- 14. Bonnie Kristian, "Where in the world isn't the US military?," *US News and World Report*, May 4, 2016, https://www.usnews.com/opinion/articles/2016-05-04/obamas-secret-troop-deployments-cost-taxpayers.
- 15. David Vine, "The United States probably has more foreign military bases than any other people, nation, or empire in history," *Nation*, September 14, 2015, https://www.thenation.com/article/the-united-states-probably-has-more-foreign-military-bases-than-any-other-people-nation-or-empire-in-history/.
- 16. Jeremy Herb, "Trump order sets military buildup in motion," *Politico*, January 27, 2017, http://www.politico.com/story/2017/01/trump-rebuild-military-executive-action-234288.
- 17. US Naval Institute, Report: Chinese develop special kill weapon to destroy US aircraft carriers, 2009.
- 18. John M. Collins, "War-fighting fundamentals," *Military Strategy: Principles, Practices, and Historical Perspectives* (Washington, DC: Potomac Books, 2002).

- 19. David Kilcullen and Curtis Lee, "Marine Corps civil affairs," *Marine Corps Gazette* 101(1), pp. 35–41; Widnall and Fogleman, "Global presence."
- 20. See Michael Mullen, remarks at the National Defense University, August 16, 2005, http://www.navy.mil/navy-data/cno/mullen/speeches/mullen050816.txt; John Paxton, remarks at the annual Army expo, October 23, 2013, https://www.usnews.com/news/articles/2013/10/23/army-chief-chafes-at-new-reliance-on-technology.
- 21. For example, see Dave Majumdar, "How Russia's edge in electronic warfare could ground the US Air Force," *National Interest*, April 26, 2016, http://nationalinterest.org/blog/the-buzz/how-russias-edge-electronic-warfare-could-ground-the-us-air-15932.
- 22. Michael Foucault, Power/Knowledge, edited by Colin Gordon (Brighton: Harvester Press, 1980).
- 23. Donald Alan Carter, "Eisenhower versus the generals," The Journal of Military History 71(4), pp. 1169–1199.
- 24. Ibid.
- 25. Rebecca Henderson and Kim Clark, "Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms," *Administrative Science Quarterly* 35(1), pp. 9–30. See also Joe Mariani and Ted Johnson, "The blueprint for a better military: How architectural innovation deliver strategic competitive advantages," Deloitte, February 2017, https://www2.deloitte.com/us/en/pages/public-sector/articles/blueprint-for-a-better-military.html.
- 26. Thomas K. Adams, "Future warfare and the decline of human decision making," Parameters 41(4), pp 5-19.
- 27. Ibid.
- 28. David Goldfein, "War in the information age," Defense One, November 16, 2016, http://www.defenseone.com/ideas/2016/11/war-information-age/133193/?oref=DefenseOneTCO.
- 29. Ibid.
- 30. Department of Defense, "New joint interagency combined space operations center to be established," NR-352-15, September 11, 2015, https://www.defense.gov/News/News-Releases/News-Release-View/Article/616969/new-joint-interagency-combined-space-operations-center-to-be-established.
- 31. Sydney J. Freedberg, Jr., "Air Force leading way to 3rd Offset: Bob work," Breaking Defense, September 16, 2016, http://breakingdefense.com/2016/09/air-force-ops-centers-lead-way-to-3rd-offset-bob-work/.
- 32. Charles C. Boyd, *International Electronic Countermeasures Handbook*, 2004 edition (Norwood, Ma.: Horizon House, 2004).

ABOUT THE AUTHORS

Chuck Wald

Chuck Wald serves as vice chairman and senior advisor in the Federal practice of Deloitte Services LP. He is responsible for providing senior leadership in strategy and relationships with the US Department of Defense. Wald retired from the US Air Force as a four-star general and is a subject matter specialist in weapons procurement and deployment, counterterrorism, and international energy security policy.

Ted Johnson

Ted Johnson is the defense and national security research manager in Deloitte's Center for Government Insights within Deloitte Services LP. He is a retired commander in the United States Navy where he primarily focused on cyber policy and signals intelligence. During the course of Johnson's military career, he was a speechwriter for the chairman of the Joint Chiefs of Staff, a White House Fellow, a military professor at the Naval War College, and an aide-de-camp to the director of the National Security Agency. He holds bachelor's and master's degrees from Hampton University and Harvard University, respectively, and a doctorate of law and policy from Northeastern University.

ACKNOWLEDGEMENTS

The authors would like to thank **Bill Eggers** and **Joe Mariani** for their review and recommendations for this article.

CONTACT

Ted R. Johnson

Defense and national security research manager Deloitte Center for Government Insights Deloitte Services, LP +1 571 882 6623 tejohnson@deloitte.com



Deloitte. University Press



Follow @DU Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press

Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2017 Deloitte Development LLC. All rights reserved. Member of Deloitte Touche Tohmatsu Limited