

Opinion

The cyber bases of the future

By **Jan Kallberg**

Jun 11, 2018



National cyber defense units should be located in metropolitan areas where they can best take advantage of IT capabilities and infrastructure. (artisteer/Getty Images)

The cyber missions that support government and business cyber defenses need to be located where they can have an impact on the outcome. The Department of Defense owns a lot of real estate, but that doesn't mean that housing domestically defending cyber units in the existing installations are the optimal option.

The U.S. Army's Futures Command is going to seek a metropolitan area to attract innovation, momentum and access

advantage of remote controls and digital access, they still need trust, understanding and the ability to give practical guidance, support and information so they can cooperate under time pressures and uncertainty.

There are several spots in the United States that are hubs for financial data processing, IT infrastructure and communications with limited or nonexistent military presence and facilities. For example, St. Louis, Missouri, houses large data centers, data processing and IT infrastructure backbone. The Dallas/Fort Worth area, in the North Texas tech belt, has not only telecom and tech infrastructure, but several high-tech defense industries. And New York and Central New Jersey handle more financial transaction than anywhere else on this planet in combination with telecom infrastructure.

The rationale that put today's military installations where they are dates back in many cases to the Civil War era, and even the most recent cases are often from the pre-fax machine era.

The efficiency of creating large military installations with ranges that allow training and live-fire exercises makes financial and readiness sense for maneuver units and their support units. The BRAC (Base Realignment and Closure) mega-installations serve the needs of their combat units well with maintenance shops, vehicle storage, an army hospital, firing ranges, warehouses, plenty of terrains to train tactical and operational concepts. However, the military installation is not crucial for the cyber mission unless a cyber unit's focus is to defend the Department of Defense networks.



The cyber unit that will support the civilian entities can train at these BRACtowns, but there is another factor in play: time. The future support to the civilian society will include hands-on activities at the supported entity's IT infrastructure. Any reliable, rapid response ability requires that the response team can be at the premises within a few hours, not days.

A cyber unit that is housed in an office building in St. Charles, Missouri, on an office floor in Federal Plaza, Manhattan, or along the I-75 corridor in northern Texas is closer to the action when it happens. A cyber unit focused on protecting our retail supply chain and flow of perishables and food to the consumer might be better off working out of Bentonville, Arkansas — the world headquarters of Walmart — then maybe anywhere else. The cyber units of the future should be based where their ability to reach mission success is highest, no matter the locale.

When we speak of an innovative mindset, we have to be watchful of our path dependency and the lingering habit of doing things the way we always have done it. The BRACtown is likely not ideal for the future cyber defense teams. Downtown offers more mission support as national cyber units increasingly utilize private IT capabilities in defending critical infrastructure and government.

Jan Kallberg is a research scientist at the Army Cyber Institute at West Point and an assistant professor in the Department of Social Sciences at the United States Military Academy. The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute at West Point, the United States Military Academy or the Department of Defense.

Share:      