Cultivating Technology Innovation for Cyberspace Operations

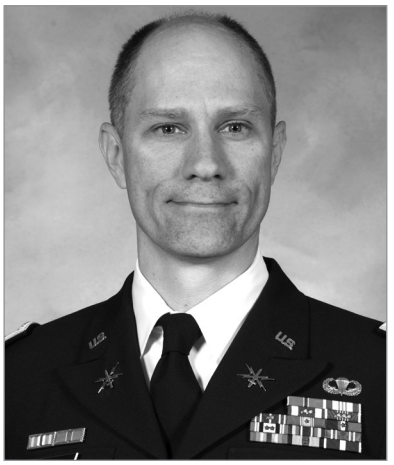
Colonel Stoney Trent, Ph.D.

"Pursuit of innovation need not require big bets on uncertain futures.... [Organizations] can succeed ... by harnessing the past in powerful ways" [1].

Our Nation and our allies are fighting a Cyber Cold War against multiple capable adversaries. [2] Like the original Cold War, we have lost ground in the first decade by failing to acknowledge the breadth and sophistication of our adversaries' actions. While recent hacks of financial and political institutions have drawn significant attention, some of the most disturbing intrusions have been directed at military and nuclear industries. Sadly, these cyber-attacks have been met with general inaction. Widespread Russian cyber-attacks in Ukraine [3] set the conditions for an invasion that was generally described as a separatist movement. [4] The most recent National Security Strategy emphasizes the gravity of China and Russia's information operations. [5] Unfortunately, disinformation sown about and through cyberspace attacks has resulted in domestic squabbling that has limited our ability to govern effectively, let alone mount an effective response.

Fortunately, the United States (US) and its allies have great potential to prevail again. A great legacy of the US is its ability to rebound from initial losses. As with the first Cold War, it is imperative that the government leverages the best attributes of its industrial base to enable its military to adapt and defeat emerging threats. For example, in response to growing cyber threats, the Defense Department (DoD) established U.S. Cyber Command (USCYBERCOM) in 2009 to defeat threats in and through cyberspace. [6] The Cyber Mission Force (CMF), as illustrated in Figure 1, will eventually consist of approximately 6,200 active-duty personnel organized into 133 cyber teams. [7]

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply



Colonel Stoney Trent is a Cognitive Engineer and Army Cyber Warfare Officer, currently serving as the Chief of Operations and Plans for the Joint Artificial Intelligence Center under the Department of Defense Chief Information Officer. Previously, he served as the Chief of Experimentation and Director of the Cyber Immersion Laboratory at U.S. Cyber Command. He has 23 years of experience in operations and intelligence assignments in tactical, operational, and strategic echelons. His research has focused on team cognition and automation support for mission command, intelligence, and cyberspace operations. He is an Army War College graduate who served as Cyber Fellow at the National Security Agency.

An additional 2,740 Reservists and National Guardsmen will augment these teams and provide another 36 teams when mobilized. [8] The Army's portion of the CMF is 62 teams, including 11 National Guard and 10 Reserve cyber protection teams. [9] Active duty Army cyber teams are based in the National Capital Region, Georgia, Texas, and Hawaii. Army National Guard and Reserve units operate from 30 States, South Korea, and Germany. As with previous conflicts, innovation in operations, training, and technology will ensure these forces can overmatch adversaries.

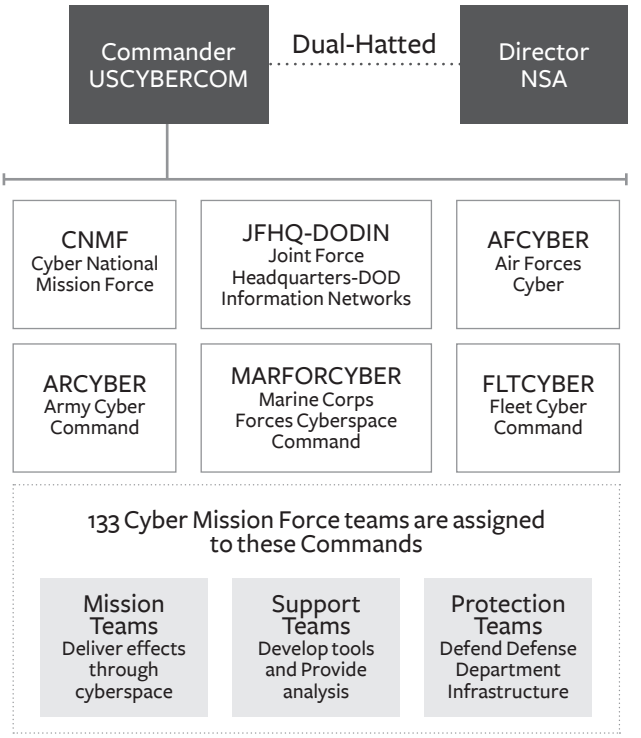


Figure 1. The Cyber Mission Force [9]

Innovation is adopting, adapting, or developing a new device, system, policy, program, process, product, or service. [11] Innovation permits the Army to stay ahead of determined enemies and accomplish the mission. [12] The Army has formally acknowledged that the pace of change in the current operating environment demands more innovation [13], but leaders must implement strategies and philosophies. Even the best leaders will fail to achieve a vision without the proper culture and resources. This report summarizes characteristics of previous innovation activities and offers recommendations for how the Army could cultivate technology (devices and systems) innovations for cyberspace operations.

What encourages innovation?

A cornerstone of American success has been its proclivity for innovation. Historians, sociologists, and management scientists have studied innovation activities in the US and have documented environmental, organizational, and individual commonalities in both public and private sector innovations. The preponderance of research on past innovative environments began in the 1990s with studies of regions such as Silicon Valley.

Silicon Valley is an innovative ecosystem that has been cultivated over the past century. Before the 1960s, the Santa Clara Valley was an agrarian region known as the "Valley of Heart's Delight" because of its vast orchards and pleasant climate. [14] It was also the home to Stanford University, a private institution, which had been developing wireless communication technologies for the Navy since the early 1900s. [15] During and after World War II, Frederick Terman, the dean at Stanford's College of Engineering, not only encouraged increased defense spending at Stanford but also emphasized partnerships with local corporations. These partnerships, through which the university shared laboratory facilities and talent with new companies, created a cycle of successful ventures and increased defense-related investment. Amongst the thousands of startups that have emerged in Silicon Valley are Hewlett-Packard, Apple, SanDisk, Facebook, Netflix, and fifty-six other Fortune 1000 companies. [16]

Unlike other innovation districts such as Hartford (precision manufacturing in late 1800s), Detroit (assembly line automotive construction in early 1900s), or Minneapolis-St Paul (medical technologies in 1950s), Silicon Valley has ridden consecutive waves of technology development, such as radio communications (1930s), aerospace (1950s), electronics (1970s), computing (1990s), and internet applications (2010s). [17] A confluence of features fueled this evolution. Foremost were loosely constrained resources in the form of substantial and sustained government research [18], and a world-class private university with close ties to local industry. The region has favorable weather, scenery, and immigration rules that entice talented people to live there. Entrepreneurial corporate and academic cultures encouraged risk-taking and information-sharing. Local government was supportive of technology-related development. [19] Aggressive venture capitalists were entrepreneurs themselves and were knowledgeable and involved with start-up activities. [20] Over time, the region's dense social

networks and open labor markets allowed for talented people to move between companies as startups came, grew, or went. Many other regions have attempted to replicate Silicon Valley's success with mixed results.

AnnaLee Saxenian has extensively compared Boston, MA to Silicon Valley. [21] She noted that prominent universities, a history of defense spending, attractive city infrastructure, and a desire to encourage technology development had placed Boston on an equal footing with Silicon Valley by the early 1980s. However, Silicon Valley companies grew by $25B between 1986 and 1990, while Boston companies, which included Raytheon, Boston Scientific, and Digital Equipment Corporation (acquired by Compaq in 1998), grew by only $1B. Many of the historic strengths of New England business dampened growth in the 80s and 90s. The region was dominated by highly self-sufficient companies with hierarchical organizations, vertical information flow, and centralized decision-making. Manufacturers clung to proprietary architectures and emphasized secrecy over collaboration with other companies. Vertically integrated companies (i.e., companies that handle design, manufacture, test, marketing, and support) allowed for controlled profits but hindered adaptation. Business associations focused on lobbying for legislation and tax cuts rather than industry cooperation and standard setting.

Furthermore, venture capitalists were financial professionals, rather than technologists and entrepreneurs, so they provided little more than resources and profit expectations for their ventures. Interestingly, when many Silicon Valley companies adopted New England business models in the late 70s and early 80s, they lost ground to Japanese industry. A return to principles of cooperation and collective innovation in the 80s and 90s restored their dominance.

Other regions that have attempted to recreate Silicon Valley include New Jersey, Texas, and New York. In southern New Jersey, RCA and Bell Labs attempted to set up partnerships with Princeton. RCA Sarnoff Lab exchanged researchers with the university, while Bell Labs created its own program, called the Institute of Science and Technology, to grow research talent in-house. Bell sought investments from other regional corporations as well as a partnership with Princeton. Texas companies desiring a source of engineering expertise established the Graduate Research Center of the Southwest. Southern Methodist University created the Foundation for Science and Engineering and even hired Frederick Terman as the president. The Microelectronics and Computer Cooperative and the Semiconductor Manufacturing and Technology Institutes were established in Austin. Sadly, none of these organizations were able to integrate their regional economies, which were comprised of vertically integrated companies. [22] New York created a Center for Industrial Innovation, which was centered on Rensselaer Polytechnic Institute (RPI). Unfortunately, the Albany-Troy region lacked a strong industrial base to capture innovations, so RPI ended up exporting its best ideas and graduates to other places. [23] Each of these efforts lacked a critical mass of defense spending and

failed to foster an ecosystem of interdependent startups like that in Silicon Valley.

Margaret O'Mara offers another contrast case in her detailed analysis of the Georgia Institute of Technology and Atlanta. [24] Georgia Tech is a state-funded university that was originally intended to improve industrialization in the South. As a public university, it is subject to the whims of state legislators for its financing and thus has limited incentive to encourage city economic development. This resulted in most development to support technology activities being in remote suburbs, which were disconnected from the main campus. City planners were focused on retail capacity and entertainment facilities, rather than high-tech development. Georgia Tech also did not benefit much from post-WWII defense spending. "In order to stay solvent, the school dared not stray far from its original mission - to serve the state's interests rather than greater and more intangible academic ends". [25] Atlanta also suffered from a history of racial intolerance and socioeconomic division that consumed political activities for decades during which major advancements were being made elsewhere. Ultimately, Georgia Tech lacked "the size, capacity, or powerful leadership to become the center of another Silicon Valley". [26]

Although the available historical analyses focus on the growth of innovation districts in the twentieth century, they are still instructive. Each of the previously discussed regions has undeniably matured since 2000; however, it is helpful to understand how and why they advanced at variable paces. In each case, the regional economy, culture, infrastructure, and policies were important local contributions to innovation. In effect, these factors can be thought of as the soil of innovative ecosystems.

Scientists investigating urban growth have noted interesting patterns that emphasize the importance of physical proximity. An analysis of a variety of urban development measures determined that innovation and creativity, as measured by patents and research and development jobs, follow a positive power law with scaling exponents between 1.15 and 1.27. [27] For example, cities that were 10x larger than other cities had 18x more inventors, and cities that were 50x larger produced 143x more patents. This exponential increase in innovation is related to social networks and access to ideas, resources, and expertise in more populated urban settings. Transaction costs are lower in more densely packed cities. Local hiring is more comfortable, and experts find it easier to move between organizations. Serendipitous exchanges are more likely as experts from various industries interact socially. Of note, the degree of success captured from this scaling is reduced in districts that suffer from too much control of information. [28] This appears to explain why populous cities across Asia have failed to recognize innovative successes commensurate with their size. Additionally, prosperous regions benefit from organizations prepared to sow and nurture the seeds of innovation.

Individualistic societies, such as the US, tend to emphasize the role of individual experts in innovative outcomes. However, recent research challenges the notion that lone geniuses are

the prototypical innovators. Andrew Hargadon advances a network perspective that suggests innovators are not necessarily smarter, but rather more connected than others. [29] This has important implications for how organizations enable innovation. While specialized talent is important, information sharing may be more so. Hargadon's analysis of technology innovations from Edison's Menlo Park to Ford's factory floor and Jobs' garage suggests that most innovations are recombinations that combine existing objects, concepts, and people in ways that spark technological revolutions. Such brokering involves spanning industries, moving ideas and building new communities. "Hiring smart people, building flat organizations, and cross-functional teams, and engaging in brainstorming and rapid prototyping are not enough to make organizations innovative". [30]

Innovative organizations and ecosystems include a core of specialists as well as a cadre of generalists responsible for spanning and brokering. Spanners are not liaisons, but rather people with (or willing to develop) first-hand experience in multiple domains. Lawyers in Silicon Valley have historically played such a role. [31] Lawyers have exposure, access, and trust amongst many companies and serve as connective tissue in and between industries. They can mediate crucial flows of resources and information and facilitate the consolidation and legitimization of ideas and organizations. McKinsey and Company, a global management consulting firm, not only brokers information between industries but also maintains its own "Rapid Response Team," which is responsible for connecting internal experts for projects. [32] Spanners maintain weak links to spark ideas and connect experts who subsequently build strong links to capture them. Workspaces encourage or discourage these linkages.

More attention is being paid to how workgroups are impacted by their workspaces. Innovation workplaces require a balance between order and chaos. [33] Open office plans afford no privacy, and closed offices discourage coordination. Cross-fertilization and interdisciplinary work require ample space to exchange ideas, while private spaces are needed for seclusion and reflection. Telework reduces overhead and offers individual flexibility but reduces opportunities for employees to intermingle. Because intermingling is critical for recombination, it is no surprise that successful, high tech organizations still invest in workspaces that promote face-to-face interactions. [34] Ultimately, workplaces must be flexible and tailored to the current work needs of the workgroup. "Cookie-cutter settings will produce cookie-cutter ideas." [35] MIT's Building 20, now replaced by the Stata Center, was a World War II-era temporary structure that afforded great flexibility during its fifty-year existence, cultivating efforts as diverse as the first hackers, Noam Chomsky's linguistics department, and Bose Acoustics and Digital Equipment Corporation. [36] Microsoft's Redmond Lab, or Building 99, is similarly built to be reconfigured with little effort. [37] Such flexibility is critical in light of the finite lifespan (approximately twenty years) of innovation districts, spaces, or groups. [38]

Organizational behavior research has identified a wide variety of factors that are common amongst innovation activities. A meta-analysis of 46 studies conducted between 1960

and 1988 found that specialization, managerial attitude toward change, slack resources, and communication were associated with innovation. [39] A more recent meta-analysis of 133 studies of public sector innovation between 1990 and 2013 revealed that slack resources, leadership styles, incentives with clear goals, low-risk aversion, and employee autonomy were common across innovative activities. [40] A survey of Australian Public Service Commission employees showed that experimentation, corrective action for low-performers, feedback loops, and motivation to make improvements enhanced the likelihood of innovative activities. [41] An analysis of over 96,000 responses to a Canadian workplace survey between 1999-2006 found that highly qualified personnel, motivated employees with consistent opportunities to innovate, and innovation as a persistent strategic priority contribute to innovation. [42] A Smithsonian Institute study determined that charismatic leaders who were supportive of individual researcher freedom and interdisciplinary teamwork were common amongst US places of innovation. [43] Examples of individual autonomy can be found at Google and 3M, where they direct their engineers to allocate fifteen to twenty percent of their time to pursue projects of their interest. [44] Employees are only required to provide regular updates to their supervisors on their initiatives. These studies provide compelling insights into individual and organizational contributions to innovations. Table 1 summarizes them alongside the previously discussed environmental characteristics to suggest ways for the Army to encourage innovation.

Environmental	Organizational	Individual
Inter-organizational relationships	Slack resources	Specialization/Highly qualified personnel
External pressures	Feedback loops	Employee autonomy
High density employment pools	Experimentation	Charismatic, supportive leader
Appealing locale (weather, outdoor activities, scenery)	Communication	Motivation for improvement
Successful regional economy (schools, businesses, public transportation)	Incentives with clear goals	Corrective action for low performers
Favorable immigration rules	Interdisciplinary work	
Top-tier research universities	Low risk aversion	
Open culture and labor markets	Mix and collaborative and private spaced	
Finite lifespan (~20 years)	Flexible workspaces	

Table 1 . Characteristics of Innovative Activities

How is the Army postured for technology innovation?

Although regional characteristics are important for technology innovations, the Army has limited input over the location of its installations and major activities (basing decisions are made by Congress, but at the request of the DoD). Because of decades of base realignments and closures, most military research and development for cyberspace capabilities occurs in regions that lack the environmental elements that have been associated with technology innovation. (Figure 2 identifies the current locations of the most significant military cyberspace research and development activities.) It is unsurprising that the Army has struggled to hire highly qualified scientists and engineers in these locations. Doctoral scientists and engineers in the Army's Research, Development and Engineering Centers have comprised between two and five percent of their workforces for decades. [45] As of 2007, Army Research Laboratory (ARL) had improved their doctoral workforce from twenty-five to thirty-five percent over the preceding decade, but that was far below the fifty percent for Navy Research Laboratory (both are in or near Washington, D.C.).

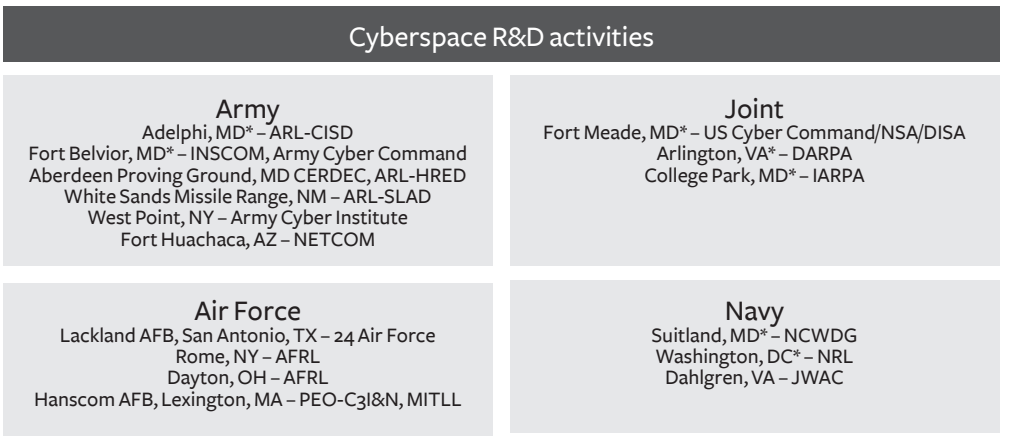


Figure 2. Current cyberspace R&D activities and locations

A notable exceptional region is the National Capital Region (NCR). Due to the preponderance of government research activities located within fifty miles of Washington, D.C., the NCR has emerged as a new technology innovation district. With extensive federal installations as well as government-leased facilities throughout the Capital Area, there continues to be significant room for further growth. Elsewhere, the Defense Department has made poor use of military installations that are located within innovative districts. Moffett Air Field in Silicon Valley, Fort Devens near Boston, and Fort Hamilton in New York City could be software development and data science hubs but have been left fallow.

The Army has decided to move its Cyber Headquarters away from the NCR to Fort Gordon, GA. Several good reasons for this move include geographic distribution of national security capabilities, the presence of an existing military schoolhouse (the Army Signal Center), and the presence of a national cryptologic center (NSA/CSS Georgia). [46] Additionally, inexpensive housing, power, workspace, and cooling contributed to the decision. [47] It is likely that the colocation of training and operational organizations will encourage innovative practices in both. The seclusion of Fort Gordon may also help protect operational innovations from adversaries. Unfortunately, Augusta, GA lacks most of the characteristics that have attracted technologists to other innovation regions. Limited public infrastructure and services, sparse employment options, a humid subtropical climate, a lack of a private research university, and distance from urban centers will likely delay the emergence of innovative technologists in Augusta-Richmond County. Furthermore, technology innovations face other self-imposed constraints.

Organizations and processes stifle technology innovation in the Army. Congressionally mandated acquisition processes are implemented in a way that diffuses responsibility across large bureaucracies. For example, a cyberspace need is supposed to be identified by operational commanders (Army Cyber Command), documented by a capability manager (Cyber Center of Excellence), validated by a force manager (Army Capabilities Integration Center, G-8, and/or J-8), funded through a 5-year budget cycle overseen by a resource manager (G-8), researched by a program officer (Army Research Laboratory and Communications Engineering Research Development and Engineering Center), developed and delivered by program manager (Program Executive Office), tested by a test engineer (Army Test and Evaluation Center), and used by cyber team members. [48] This baton passing crosses up to ten general offices, with most of the staff work and decision-making performed by people with little technical knowledge and who will never be impacted by their decisions. This convoluted and inefficient process ensures that any technology "solution" is poorly fit, or obsolete, if/when it is delivered.

Army scientists and engineers are hardworking and well-meaning, but the Army is failing them. Due to the location of Army research activities, very few scientists and engineers have access to the operators and analysts who will have to use the technologies under development. Many research program officers have limited knowledge of the daily tasks and work conditions of cyber teams. They must rely on wordy, and poorly described, requirement documents to provide critical information about users' needs. This problem is worse for the thousands of contracted scientists who rely on the program officer for guidance. High-level research guidance gets implemented across many organizations with little coordination among stakeholders. Figure 3 illustrates the assortment of Army organizations that are conducting research and development for cyberspace capabilities. In fact, Figure 3 fails to fully capture the diffusion of cyber research within these organizations, as individual research-

ers pursue cyber and non-cyber projects. The current construct limits the pooling of highly qualified personnel and resources necessary to create slack, or flexibility, for innovation. It also makes directing and collaborating with operational units, USCYBERCOM, other Service Departments, industry, and foreign partners exceedingly difficult.

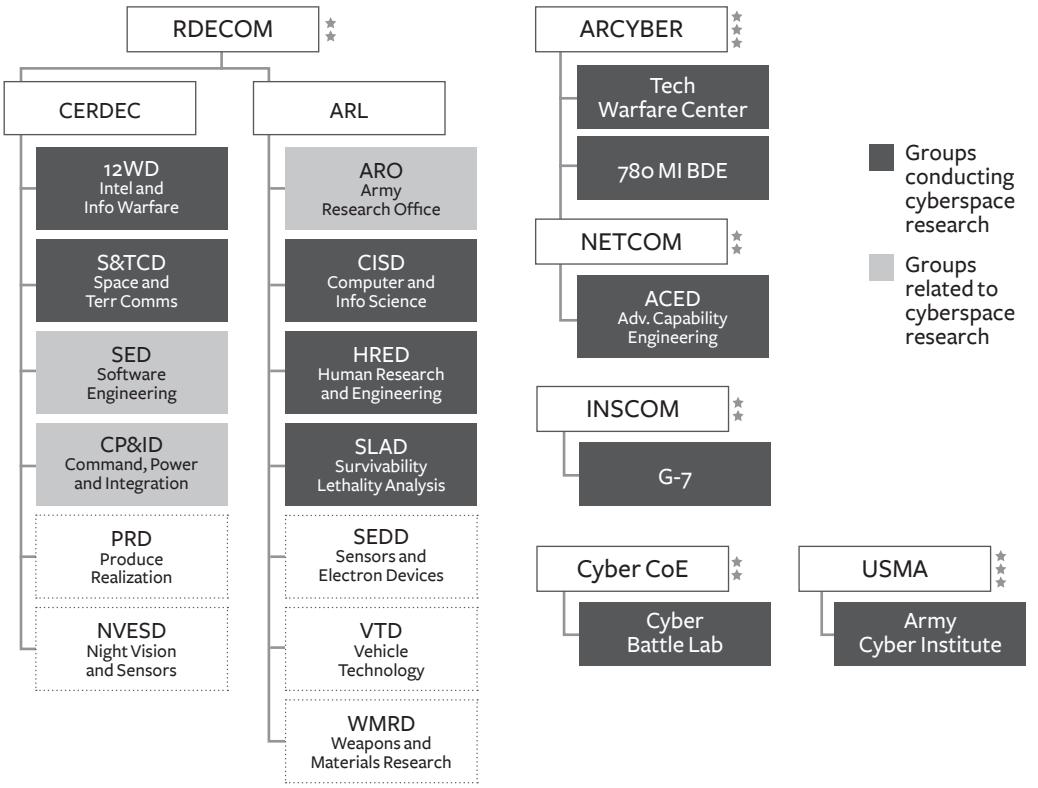


Figure 3. Cyberspace R&D within the Army [49]

The Army has long desired more STEM talent; however, it has not fully utilized its existing talents. Assignments rarely consider academic credentials and very few personnel authorizations explicitly identify advanced degree pre-requisites. Outside of the United States Military Academy, officers are responsible for generalist staff or command roles that require no STEM expertise. As a result, officers with a Ph.D. find few opportunities outside of USMA to maintain currency and provide benefit to the Army for their graduate educations.

In 2011, former Defense Secretary Robert Gates encouraged new Army Lieutenants to seek out broadening assignments that were "off the beaten path, if not a career dead end," and stated that the Army should encourage the effort. [50] He was arguing for breadth and a collaborative disposition to complement depth of skill. Successful innovative corporations

foster just such a balance. [51]In 2012, the Defense Science Board recommended that the Service Departments make opportunities for troops to serve in laboratories and research program offices. [52] In 2013, the Army Science Board recommended re-establishing a military scientist and engineer career path that would direct and strengthen Army research and development. [53] The Army Research Development and Engineering Command (RDECOM), with the concurrence of its higher headquarters, the Army Materiel Command, attempted to implement this recommendation, but the pilot stalled out due to lethargic human resource processes. [54] In particular, no career incentives existed to justify individuals accepting the risk of such assignments. Additionally, assignment officers lacked the mandate to identify and adequately utilize advanced STEM skills. Unfortunately, the Army's human resource system is designed to reward successful completion of well-established roles and discourage/disadvantage innovative, new roles. Officers following Secretary Gates's recommendation will not last long in the inventory.

The recently established cyber warfare branch offers promise for niche specialists if they are not blunted by the human resource system. Army Pamphlet 600-3 now describes a career path for cyber warfare Soldiers that suggests gainful employment for the growing force. However, like cyberspace itself, personnel requirements will change more rapidly than the current human resource system can support. For example, in 2009 the DoD hastily developed a plan for the size and composition of the CMF. This plan sacrificed commanders and staff for team-level structure, forcing units like the Cyber National Mission Force and the Cyber Protection Brigade to employ a variety of workarounds to satisfy critical command and staff roles. This situation has persisted through 2018.

Although the Cyber Center of Excellence has diligently worked to update force structure documentation, it is hard to see how it will keep up with emerging operating concepts. Under the current system, validating a new requirement takes at least twelve to twenty-four months. Once a requirement is validated, assignment cycles limit the speed at which new requirements are filled. This sclerotic process results in lost opportunities and expertise as blunted innovators seek more supportive sources of employment. Although much of the current cyber branch is under initial service obligations, the insatiable demand for software developers, cyber operators, analysts, and data scientists across the Service Departments, the intelligence community, and commercial sectors will make retention difficult in the near future. Focus groups and sensing sessions will be insufficient to retain innovative experts in the force. Without an agile personnel system that can offset the private-sector advantages, our cyber workforce will become a routinized harbor for mediocrity, incapable of defeating more agile adversaries.

Recommendations for improvement

The Army recently established the Army Futures Command to dramatically improve the way in which capabilities are delivered to the force. [55] This new Command is not a startup, but rather a merger of multiple large bureaucracies, each with its own infrastructure, heritage, and culture. As strategic integration unfolds for this Command, some proofs of concept that demonstrate the value of the new organization will be important. The sense of urgency and relatively low cost of cyberspace capabilities suggest that cyberspace capability reform would be an ideal first step. The following four recommendations fully support the intent of this new Command and can be implemented now.

Establish a Cyberspace Operations Research and Development (R&D) Group – To reduce the diffusion of responsibility and create slack resources for innovation, the Army should consolidate R&D of cyberspace capabilities as illustrated in Figure 4. The director of this group should be an academically qualified (STEM Ph.D.) cyber Colonel, with the responsibility and resources for ensuring that R&D is operationally aligned and responsive to environmental changes. The director would report to the Commander, RDECOM, and coordinate with cyber brigade commanders and the Cyber Capability Manager to exchange information about the trajectory of science and technology.

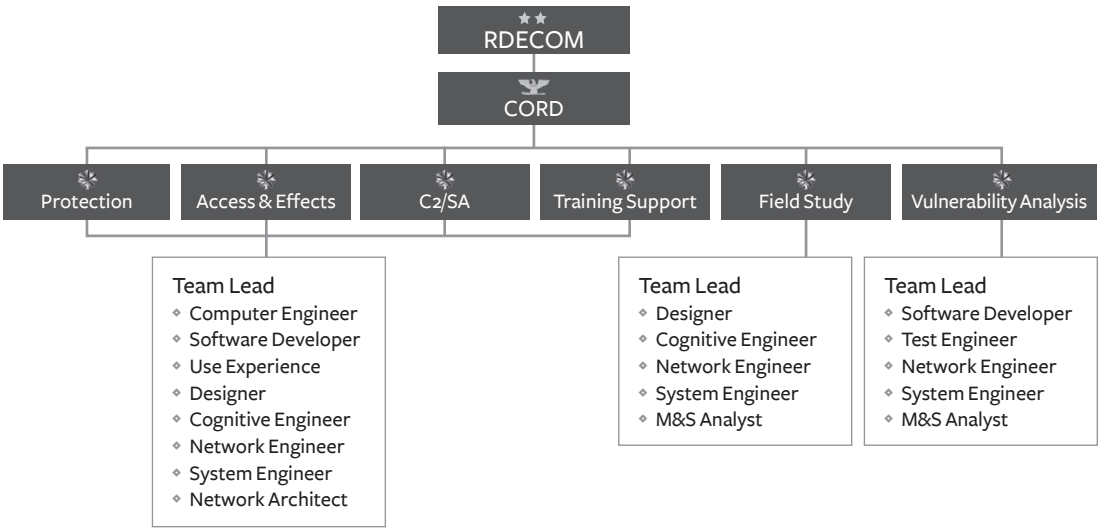


Figure 4. Army Cyberspace Operations Research and Development Group

This group should be organized into interdisciplinary research teams, each led by academically qualified cyber officers and aligned with operational requirements (performance of this organization should be measured based on operational feedback from users). Government civilians would provide continuity for this organization by serving as research

staff, project leads, and deputies. Following Title 5 of the U.S. Code and DoD policy, the Army could hire Highly Qualified Experts for up to five years to serve as technical directors in this organization. [56] These technical directors would provide sustainable exchanges of eminent experts from industry and academia. Because of its critical mass of technical expertise, this organization would represent cyber equities in the cross-functional teams within the Army Futures Command.

This organization should be principally located at Fort Meade and Adelphi, MD to provide it with direct access to cyber teams and the preponderance of cyber research expertise located within the NCR. To sustain appropriately skilled leaders, mid-career officers should be afforded Advanced Civil Schooling with utilization tours in this organization. In this way, select cyber officers could progress from cyber team members to cyber research leaders to cyber staff officers and return to cyber research leadership roles throughout their career. Such a program and organizational construct could be extended to other capability areas (e.g., intelligence, communications, and armaments) as well. Ultimately, the DoD would benefit from each of the Service Departments establishing a similar organization.

Improve Collaboration – The Army needs better formal and informal coordination to enable innovation. Innovation is a process in which the phased application of expertise is important. [57] Highly qualified scientists and engineers are critical for research phases, whereas legal, contracting and doctrine expertise are critical for implementation. In large organizations, it is difficult to locate appropriate expertise, and senior leaders have little visibility on how expertise is being applied to large-scale, complex problems. Research in cognitive psychology suggests that Transactive Memory Systems are essential for high performing organizations.

Transactive Memory Systems distribute knowledge and skills across people and tools to achieve high efficiencies. Transactive Memory theory emerged from studies of intimate couples where knowledge was efficiently federated between the two individuals [58] (it is more efficient for a couple to ask each other for information than for both people to know the same things). Accurate transactive memory has been observed to be a significant predictor of team performance. [59] In new product teams, transactive memory has positive impacts on team stability, familiarity, interpersonal trust, team learning, and effectiveness. [60] Support for transactive memory should include automation as well as human boundary spanners. A transactive memory support tool would analyze computer work to infer skills amongst workers. These data along with self- and colleague-reported information about skills could generate navigable knowledge graphs to help with expertise location. A dedicated knowledge management team should maintain not only this support tool but also foster inter-divisional collaborations. These informal methods will enable the actions and decisions from more formal venues.

The Army should establish or request three cyber capability councils–Army, Joint, and Combined–to plan and collaborate with other relevant organizations. The Army's cyber capability council should be chaired by an SES or Brigadier General on the Army Cyber Command Staff and should include the following roles:

- Director, Cyberspace Operations R&D Group
- Commanders, Cyber Brigades
- Cyber Capability Manager
- Director, Army Cyber Institute
- Director, Cyber Battle Laboratory
- INSCOM G-7

The Joint Cyber Capability Council should be chaired by a Senior Executive in U.S. Cyber Command Capabilities Development Group and include all Service Cyber R&D leads and the Defense Advanced Research Projects Agency Information Innovation Office Director. U.S. Cyber Command is currently working with the Joint Staff to establish a Cyber Functional Capabilities Board (FCB) for the Joint Requirements Oversight Committee. This will be a critical coordinating body for large-scale requirements. However, most cyber capabilities will not meet the threshold for consideration by the Cyber FCB, so the Joint Cyber Capability Council should tend to the smaller scale requirements. The Combined Cyber Capability Council should be chaired by the Office of the Undersecretary of Defense for Research and Engineering, USD(RE), and include U.S. Cyber Command, the Service Cyber R&D leads and select foreign partner R&D groups (e.g., Defense Science and Technology Laboratory, Government Communications Headquarters, Australian Signals Directorate). These coordinating councils will help inform operational planning as well as avoid (or validate) redundancy and gaps in technology development.

Commit to a Campaign of Field Study and Experimentation – Field studies provide thorough descriptions of operational needs that far surpass the fidelity and consistency of After Action Reviews (AARs) and needs statements. Field studies also provide the insights necessary for the design and conduct of experiments and afford cyber teams a voice in the requirements process through the performance of their regularly assigned duties. Experimentation offers a way to democratize technology decisions, as cyber team members provide data on tool and team performance as participants. Because of the pace of change in cyber work, these complementary research activities must be a sustained campaign rather than a collection of discrete yearly projects. The research staff should be responsible for publishing unclassified findings whenever possible. In this way, academic and industry developers will be more knowledgeable of technology requirements.

USCYBERCOM has established the Cyber Immersion Laboratory, which is developing and assessing capabilities for the CMF. [61] To date, it has been minimally staffed and resourced, with nearly all of USCYBERCOM's research funding going to external performers. The Army Cyber Center of Excellence has relabeled the Signal Battle Lab to be the Cyber Battle Lab and has been building the capability to conduct experiments to inform the cyber requirements process. These labs require a sustained budget and sufficient, appropriately skilled staff to be successful. ARL, particularly the Human Research and Engineering Directorate, should be leading or participating in this campaign to ensure that human factors are preeminent in the design of new technologies. In addition to lab staff and infrastructure, successful experimentation requires practitioners to participate.

Now that the CMF is fully operational, cyber teams should be apportioned to these laboratories as an experimentation force. Cyber battalions should designate a Chief Technology Officer who would be responsible for managing the teams' participation in field studies, experiments, and technology-oriented focus groups. In this way, the CMF can formally involve all cyber teams in a manner that accommodates collaborative planning and resourcing. Multi-domain experiments should be facilitated by including cyber teams in command post exercises and combat training center rotations. Instrumenting cyber teams to provide tool and team performance data from training and real-world operations will improve our understanding of what works and why. Ultimately, data from experiments and real-world operations will inform models that can be used to evaluate strategic and operational planning as well as technology development decisions.

Leverage existing and spawn new innovation districts – The military has been exploring ways to improve access to the knowledge, skills, and technologies in our mature innovation districts. The Defense Innovation Unit (DIU) is one example that has been focused on Silicon Valley and Boston. Other regions, such as the NCR, Pittsburgh, Seattle, Austin, and Denver are emerging as technology hubs. The Army's Futures Command has selected Austin has its headquarters to afford efficient access to that region's expertise. Despite improvements in coordination technologies, proximity and personal interactions will continue to reap the most from our existing innovative regions.

Unfortunately, the current innovation ecosystems are failing to satisfy the Nation's needs for cyber operators, software developers, and data scientists. Incremental increases to investments in established regions will recognize diminishing returns as costs of living increase. Innovation districts must be grown to dramatically increase the breadth and depth of intellectual capital, which is crucial for success in future conflicts. Because regional change is slow, wise investments in fertile locales are warranted.

Three regions offer great promise for new innovation districts–South Bend, IN, Nashville, TN, and St Louis, MO. Each region has a world-class private research university (University of Notre Dame, Vanderbilt University, and Washington University, respectively) without a federally funded or university-affiliated research center. They are in, or near, attractive cities with strong growth potential and an ability to capitalize on technologies that are developed there. They offer low costs of living and are within a two-hour flight of the preponderance of cyber teams. If these universities and their local communities are willing to partner to foster cyber or data science-related business development, the Undersecretary of Defense for Research and Engineering should establish University Affiliated Research Centers at each. These centers will accommodate broader involvement from each university and underpin the growth of more innovative ecosystems.

SUMMARY

The Cyber Cold War is raging, and the United States has the most to lose. Although the CMF is now fully operational, it will require continual technology advancements to stay ahead of our adversaries. Unfortunately, much of the Army's R&D enterprise is not well-postured to leverage our Nation's strengths, nor is it proximal to operational practitioners. A consolidated, operationally-oriented cyberspace R&D group could afford the organizational and individual enablers of innovation while helping the Army to better utilize the talent and resources that it already has. Collaborative technologies and organizational design in the Futures Command can help the Army leverage its size with improved interconnectedness.

Improving technology innovation is critical and will not come without cost and effort. Much work is needed to set environmental conditions and organizational design to support individual initiatives. Fortunately, the DoD currently stands to benefit from increased defense spending in FY19. The Secretary of Defense fully understands the need for dramatic improvement, and fifteen years of Army acquisition failures have created the crisis necessary for change. The Secretary and Chief of Staff of the Army have initiated a generational opportunity to improve innovation. This confluence of conditions is as supportive as it is ephemeral. Without immediate, bold action, the Army will miss its best opportunity to seize the initiative in the current Cyber Cold War. Decades of studies indicate the importance of a culture of experimentation. While our adversaries are experimenting, we must not dither.

DISCLAIMER

This paper reflects the views the authors. It does not necessarily represent the official policy or position of Department of Defense, U.S. Army War College or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission or broadcast.

ACKNOWLEDGMENT

I would like to thank Dr. Eric Hintz, with the Smithsonian Museum of American History, for his work on the History of Innovation Centers in the United States, which inspired much of the thought in this report. Additionally, General Paul Nakasone, Lieutenant General Stephen Fogarty, Lieutenant General (Retired) Edward Cardon, Colonel James Raftery, Lieutenant Colonel James Doty III, Giorgio Bertoli and other Army colleagues provided invaluable consultation.

NOTES

1. Andrew Hargadon, *How Breakthroughs Happen: The Surprising Truth About How Companies Innovate* (HBR Press, 2003), xii.

2. Stoney Trent, "Amid a Cyber Cold War, is the Cyber Mission Force Prepared?", Bulletin of Atomic Scientists, October 30, 2017, https://thebulletin.org/amid-cyber-cold-war-cyber-mission-force-preparedl1233.

3. Andy Greenberg, "How an entire nation became a test lab for cyberwar", *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

4. Damien Sharkov, "Putin claims Russia 'Forced to defend' Ukraine separatists", *Newsweek*, October 12, 2016, Accessed at: http://www.newsweek.com/putin-claims-russia-forced-defend-ukraine-separatists-509281.

5. National Security Strategy, United States of America, December 2017, Washington, DC.

6. Secretary of Defense (2009). Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations. Washington, D.C. , June 23, 2009.

7. Stoney Trent, "Amid a Cyber Cold War, is the Cyber Mission Force Prepared?", Bulletin of Atomic Scientists, October 30, 2017, https://thebulletin.org/amid-cyber-cold-war-cyber-mission-force-preparedl1233.

8. S. Zuehlke, Status Update to RFPB Report "DoD Cyber Approach: Use of the National Guard and Reserves in Cyber Mission Force". Reserve Forces Policy Board, Department of Defense. Washington, D.C., January 27, 2017.

9. U.S. Army Cyber School, "Cyber Career Field / Branch 17 Overview," January 4, 2018.

10. Stoney Trent, "Amid a Cyber Cold War, is the Cyber Mission Force Prepared?", Bulletin of Atomic Scientists, October 30, 2017, https://thebulletin.org/amid-cyber-cold-war-cyber-mission-force-preparedl1233

11. adapted from Richard Daft, "A dual-core model of organizational innovation", *Academy of Management Journal* 21, 1978, 193–210.

12. Department of the Army, "The U.S. Army Operating Concept: Win in a Complex World," Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, October 31, 2014.

13. Department of the Army, "Army Innovation Strategy", Office of Business Transformation, 2017.

14. Margaret Pugh O'Mara, *Cities of Knowledge: Cold War Science and the Search for the Next Silicon Valley* (Princeton, 2005), 101.

15. Martin Kenney, ed., *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region*, ed. Martin Kenney. Stanford (Stanford University Press, 2000).

16. https://www.geolounge.com/fortune-1000-companies-list-for-2016/.

17. Margaret Pugh O'Mara. "Don't Try This at Home: You Can't Build a New Silicon Valley Just Anywhere." *Foreign Policy* 181, September/October 2010.

18. Stuart W. Leslie, "The Biggest 'Angel' of Them All: The Military and the Making of Silicon Valley," in Kenney, *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region*, (Stanford University Press, 2000), 48–67.

19. Stuart Leslie and Robert H. Kargon. "Selling Silicon Valley: Frederick Terman's Model for Regional Advantage." *The Business History Review* 70, Winter 1996.

20. AnnaLee Saxenian, *Regional Advantage: Culture and Competition in Silicon Valley and Route 128* (Harvard, 1994).

21. Ibid.

22. Stuart Leslie and Robert H. Kargon, "Selling Silicon Valley: Frederick Terman's Model for Regional Advantage." *The Business History Review* 70, Winter 1996.

23. Stuart Leslie, "Regional Disadvantage: Replicating Silicon Valley in New York's Capital Region", *Technology and Culture*, 42(2), April 2001, 236-264.

24. Margaret Pugh O'Mara, *Cities of Knowledge: Cold War Science and the Search for the Next Silicon Valley* (Princeton, 2005).

25. Ibid, 186.

26. Ibid, 222.

27. Luis Bettencourt, Jose Lobo, Dirk Helbing, Christian Kuhnert, and Geoffrey West, "Growth, innovation, scaling and the pace of life in cities", *In the Proceedings of the National Academy of Sciences*, 104(17), April 2007, 7301-7306.

28. Steve Johnson, *Where Good Ideas Come From: The Natural History of Innovation* (Riverhead, 2010).

29. Andrew Hargadon, *How Breakthroughs Happen: The Surprising Truth About How Companies Innovate* (HBR Press, 2003).

30. Ibid, 51.

31. Suchman, 71-91.

NOTES

32. Andrew Hargadon, *How Breakthroughs Happen: The Surprising Truth About How Companies Innovate* (HBR Press, 2003), 149.

33. Johnson, Steve. *Where Good Ideas Come From: The Natural History of Innovation* (Riverhead, 2010), 62.

34. Arthur Molella, "What makes an Innovative Lab or Workspace?" *American heritage of invention and technology*, Vol 25, Spring 2010, 28-37.

35. Ibid, 29.

36. Stewart Brand, *How Buildings Learn: What happens after they're built*, (Viking, 1994).

37. https://www.microsoft.com/en-us/research/lab/microsoft-research-redmond/

http://www.amusingplanet.com/2009/10/inside-microsofts-office-at-redmond.html.

38. Arthur Molella, "What makes an Innovative Lab or Workspace?" American heritage of invention and technology, Vol 25, Spring 2010, 28-37.

39. Fariborz Damanpour, "Organizational Innovation: A meta-analysis of effects of determinants and moderators", *Academy of Management Journal*. 34(3), September 1991, 555-590.

40. Hanna De Vries, Victor Bekkars, and Lars Tummers, "Innovation in the Public Sector: A systematic review and future research agenda", *Public Administration* 94, Issue 1, March 2016, 146-166.

41. Mehmet Demircioglu and David Audretsch, "Conditions for innovation in public sector organizations", Research Policy 46(9), 2017, 1681-1691.

42. James Chowhan, Fred Pries, and Sara Mann, "Persistent innovation and the role of human resource management practices, work organization, and strategy", Journal of Management and Organization, 23(3), 2017, 456-471.

43. Arthur Molella, "What makes an Innovative Lab or Workspace?" *American heritage of invention and technology*, Vol 25 (Spring 2010), 28-37.

44. Steve Johnson, *Where Good Ideas Come From: The Natural History of Innovation* (Riverhead, 2010), 93.

45. Gilbert Decker, et al., Improving Army Basic Research: Report of the Panel on Future Army Laboratories, RAND Corporation, Santa Monica CA, 2012.

46. Interview with LTG Edward Cardon, former Commander of Army Cyber Command, January 24, 2018.

47. Email from LTG Paul Nakasone, Commander of Army Cyber Command, April 9, 2018.

48. Department of the Army, "How the Army Runs: A senior leader reference handbook", U.S. Army War College, 28 August 2015, Carlisle PA.

49. Compiled from interviews and personal experiences of the author.

50. Secretary of Defense Robert M. Gates. Speech at West Point on February 25, 2011.

51. Morten Hansen, "IDEO CEO Tim Brown: T-shaped Stars: The Backbone of IDEOs Collaborative Culture", Chief Executive, (January 21, 2010), https://chiefexecutive.net/ideo-ceo-tim-brown-t-shaped-stars-the-backbone-of-ideoaes-collaborative-culture__trashed/.

52. Defense Science Board, Report of the Defense Science Board on Basic Research, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington DC, February 2012.

53. Department of the Army, "The Strategic Direction for Army Science and Technology", Army Science Board, Washington, DC, February 2013.

54. Director, U.S. Army Research, Development and Engineering Command, "Authorization for the Officer Scientist Engineering Program (OSEP) Pilot", April 2013.

55. Mark Esper, "General Orders No 2018-10: Establishment of the United States Army Futures Command", Headquarters, Department of the Army: Washington, DC, June 4, 2018.

56. Undersecretary of Defense for Personnel and Readiness, "Revised Policy Guidance – Hiring of Highly Qualified Experts (HQEs)", Washington, DC, March 26, 2010.

57. Fariborz Damanpour, Marguerite Schneider, "Phases of Adoption of Innovation in Organizations: Effects of Environment, Organization and Top Managers", *British Journal of Management*, 12(3), (September 2006), 215-236.

Lisa Daniel, Patrick Dawson, "The sociology of innovation and new biotechnologies," New Technology, Work and Employment, 26(1), February 25, 2011, 1-16.

NOTES

58. Daniel Wegner, Toni Giuliano, Paula Hertel, "Cognitive Interdependence in Close Relationships", In: Ickes W. (eds) *Compatible and Incompatible Relationships. Springer Series in Social Psychology.* (1985) Springer, New York, NY, 253-276.

59. JR Austin, "Transactive memory in organizational groups: the effects of content, consensus, specialization, and accuracy on group performance", Journal of Applied Psychology, 88(5), October 2003, 866-78.

60. AE Akgün, JC Byrne, H Keskin, and GS Lynn, "Transactive memory system in new product development teams", *IEEE Transactions on Engineering Management*, 53(1), February 2006, 95-111.

61. Stoney Trent, Robert Hoffman, Scott Lathrop, "Applied Research in Support of Cyberspace Operations: Difficult, but Critical", *The Cyber Defense Review*, May 2, 2016.