Perspective on 2015 DoD Cyber Strategy

Addendum

Lara Schmidt

RAND Office of External Affairs

CT-439/1

February 2016

Document submitted on February 23, 2016 as an addendum to testimony presented before the House Armed Services Committee on September 29, 2015

For more information on this publication, visit www.rand.org/pubs/testimonies/CT439z1.html

Published by the RAND Corporation, Santa Monica, Calif.

QFR submitted by Shuster, Bill
House Committee on Armed Services
Outside Perspectives on the Department of Defense Cyber Strategy
Tuesday, September 29, 2015

Question for Dr. Lara Schmidt: In your written testimony, you addressed DoD shortfalls in both recruiting and retention of the cyber workforce. Oftentimes, financial incentives are cited as the potential solution to these shortcomings. I agree with your statement that retention is closely linked to job satisfaction, so my question is whether DoD's human capital management system is effective in placing the cyber workforce into positions that provide sufficient skill utilization and job satisfaction?

Answer: I have not conducted a formal analysis of the extent to which the Department of Defense's (DoD's) approach to cyber workforce management succeeds in placing civilians and service members into jobs for which they are qualified. Furthermore, I am unaware of any such assessment for workforce management approaches following the new initiatives DoD unveiled in 2015.[1] However, the work undertaken as part of the National Initiative for Cyberspace Education (NICE) *Cyberspace Workforce Framework,*[2] which identifies the required skills for many cyberspace jobs, is a necessary first step toward performing any "job analysis" to evaluate the extent to which personnel matched to jobs possess the required skills to work effectively. Both receiving the right training (initial and continuing) and progressing through different jobs that draw on *similar* skill sets are important to ensuring personnel are well matched to job requirements.

I am also unaware of any formal analyses of job satisfaction among DoD's civilian and military cyberspace cadres. Conventional wisdom asserts that DoD offers its personnel unique opportunities to serve the nation and conduct high-stakes, highly dynamic operations they would find no place else; as a result, conventional wisdom asserts that job satisfaction is high. While this assertion rings true for *some* DoD cyberspace jobs (e.g., military personnel conducting offensive and defensive operations), I question the wisdom of applying such logic to DoD cyberspace jobs that both (a) require staff to manage a high operational tempo and other stressors on family and personal time (e.g., frequent changes of duty location and/or organizations) and (b) are similar to jobs conducted in the private sector (i.e., lack the "only in DoD" allure). Therefore, an assessment of job satisfaction in the "IT-like" *DoD Information Network Operations (DoDIN Ops)* job

---

[1] Department of Defense, *Cyberspace Workforce Management*, Directive 8140.01, August 11, 2015.
[2] NICE, *National Cybersecurity Workforce Framework*, Washington, D.C.: Department of Commerce, 2013. The services have adopted this framework to varying extents.

categories may be illuminating, as it may not adhere to conventional wisdom. Commercial-sector IT job satisfaction has been linked to the existence of defined career paths that allow growth and progression not only through advancement into the management ranks, but also through technical tracks that allow personnel to continue to learn, engage with professional peer groups, and innovate to keep pace with rapidly changing technology.