IT and Networks

Train, promote and lose: The battle for retention

By **Jan Kallberg**

Jul 9, 2018

If the armed forces seek to create a more significant force, recruitment and training of cyber support will only meet demand if retention is high. (Bill Roche/Army Cyber Command)

The United States is an engineering country where technical solutions are born, and solutions are thought up, in an innovation-friendly environment of academia and industry. There are gaps, but the United States is highly adaptive and able to face technological challenges due to its research capacity and industrial base.

The more substantial challenges are retention, maintaining an able workforce and transferring the willingness to serve to the next generation. The cost for the Department of Defense to recruit and train, or transition a mid-career officer, are high. Equally challenging is the time to replace an officer that decides to leave the armed forces. This is a simple math problem: If the armed forces seek to create a more significant force, recruitment and training will only meet demand if retention is high; otherwise, the inflow is only compensating the outflow from the service.

With the strengthening of the American economy, combined with a radically increased demand for information security competence in the civilian workforce, retention of cyber skills and cyberwarriors will be an ongoing concern. If you train, you need to be able to retain the personnel — otherwise it is a lost investment for the organization.

According to the RAND study “Millennial Perceptions of Security,” millennials and young people are less invested in national security issues, but care about their economic security. Millennials will be the predominant workforce in the next decade, slowly replaced by the post-millennials in the late-2020s. The retention of “Generation Instagram” is likely different than earlier generations.

Should we expect that “Generation Instagram” to leave their social media-upheld island in the digital world, return to the 20th century and embrace the bureaucracy and its industrial age apparatus?

A culture shift is needed. Conventional forces consistently prepare for war, while cyber forces are continuously engaged in cyberwar. Therefore, rotating cyber officers through assignments reduces readiness and increases risks. Allowing one individual to hold a position for five or more years will significantly improve operational readiness. Exempting the cyber force from mandatory positional and geographic moves will help build and maintain a more effective future force.

Also in need of change is the dated Defense Officer Personnel Management Act, which includes an embedded assumption that one partner makes a career and the other tags along with the rotations, trying to see what they can do at the post where they land. To retain these two smart individuals as a military family we have to design rotations and positions in a way that the spouses have career opportunities that match their abilities. Millennials and the younger generation want to influence their future.

Alexander Hamilton, writing in 1775, said "There is a certain enthusiasm in liberty, that makes human nature rise above itself, in acts of bravery and heroism." A rigid bureaucracy has limited workplace appeal for millennials; to release the enthusiasm, an organization that has a higher degree of freedom is more adaptive and mission-centered as the unit commanders are empowered.

Freedom is also a prerequisite for innovation, the freedom to fail an informed and rational attempt. Millennials are likely the next decade's cultural-change agents, not by intent but through catalyzing change, and from a cyber perspective, it might be necessary.

The rapid changing technical landscape, the increased velocity in engagements, the thick fog of uncertainty, all create a need for future cyberwarriors to stay current within an innovative, embracing, and enabling culture. At a large scale, it can be a strategic advantage compared to our potential adversaries that lack initiative, and have fear-driven cultures and repressive outlooks.

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.