IDA | Research Summary

Cyberspace's Human Dimension

The Department of Defense (DoD) has made progress on building a significant U.S. cyber capability since the release of its strategy for operating in cyberspace in July 2011. But the current cyber workforce reflects limitations of embedding a combat force's mission in a structure dominated by intelligence and information. IDA researchers have been exploring cyberspace as an organizing concept for training and equipping cyber forces for years. A look back at several IDA projects reveals the continuing challenges that surround the human dimension of cyberspace.

Building a force for cyberspace: Responding rapidly to the need for effective cyber operations, DoD initially associated cyber forces with existing structures for intelligence and information systems. That approach produced significant new cyber operations capabilities. Still, additional gains can be made. There is a need for a clear mission identity across DoD, more clarity in military department responsibilities for force building, and more rapid growth in capabilities. The solution may be to balance the future career force so it is fed and sustained by communications, information, and intelligence career fields. Addressing cyber targets requires extensive intelligence preparation and continuous network analysis to navigate to the cyber target, penetrate defenses, create the desired effect, and assess the results. Further, cyber operations can change this artificial domain in hard-to-predict ways, requiring network analysis in real time. These and other factors demand closely integrated, multi-disciplined, experienced cyber combat crews in tailored units.

Balancing supply and demand of skilled workers: Ever since the military departments collectively began to build the U.S. Cyber Command's Cyber Mission Force (CMF), DoD has struggled with the demand for

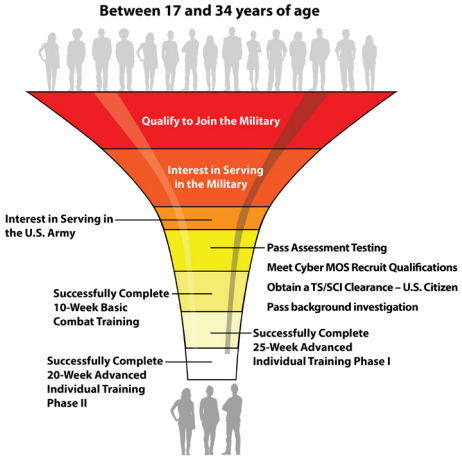
(continued)

March 2021
NS D-21550

skilled cyber workers exceeding the supply. This problem cannot be defined either too broadly or too narrowly. The just-right solution is one capable of evolving as skills and technology continue to advance. An approach based only on expanding the workforce pool may not lead to a satisfactory solution. DoD needs a thorough understanding of the cyber landscape before viable solutions can be explored meaningfully.

Choosing the right force mix: On one project, IDA researchers analyzed the CMF mission to determine which roles should be considered military essential, inherently governmental, or commercial activities. Choosing the wrong total force mix for the CMF can put the mission at risk or create inefficiencies that consume scarce resources. Researchers found that a more civilian-intensive force mix could save the DoD approximately $130 million annually. DoD could improve its ability to assess the optimal total force mix by (1) developing a legal framework for determining CMF work roles that require direct participation in cyberspace hostilities and (2) comparing position descriptions with work to be performed to develop accurate information on the true nature of the positions.

Linking attributes of recruits with performance in cyber roles: For another project, IDA looked at the challenge of identifying and training U.S. Army enlisted personnel for the cyberspace workforce. If the Army can identify recruits from a shallow pool of candidates with the right attributes and potential, it can increase the number who pass lengthy and expensive advanced training. Hackers and cyber warriors are what the Army should be seeking. The Army is investigating the links between aptitude, knowledge and skill, maturity, personality traits, motivation, and successful performance in cyber operations roles of new recruits and enlisted personnel already in the force. However, additional research is needed to understand the predictive value of attributes identified to performance in cyber operations roles.



Of the large pool of recruits who meet minimum military qualifications, only those recruits who pass assessment tests, obtain high-level security clearance, pass a background check, and successfully complete 55 weeks of training will become Army cyberspace operations specialists.

Meeting national and domestic goals: Another topic IDA examined was cyber career fields in the Air National Guard (ANG). The ANG has been working for some time on the national goal of ensuring its cyber squadrons are ready for mobilization to the CMF while exploring ways to meet the domestic goal of providing greater cyber support to state, local, tribal, and territorial entities. IDA identified challenges and opportunities to achieving these goals by analyzing employment trends for cyber professionals at the national level; examining ANG-specific career fields, missions, recruiting, and retention in cyber; and exploring the ANG's potential to assist in various domestic cyber efforts. IDA recommended that the ANG determine a national-level vision for its future roles and responsibilities in cyberspace and devise a way to balance domestic efforts with CMF mobilizations.

Modernizing cybersecurity's test and evaluation workforce: IDA recommended the U.S. Air Force 46th Test Squadron implement a spiral improvement program to meet the increasing demand for support from the Air Force's cybersecurity test and evaluation workforce. IDA researchers developed a modernization roadmap to accomplish near-, mid-, and far-term objectives that augment the workforce and improve its infrastrucure and processes.

As Director of the Information Technology and Systems Division of the IDA Systems and Analyses Center, **Margaret Myers** (mmyers@ida.org) leads a team of IDA researchers who address cybersecurity challenges as well as other national and global issues in the realm of information technology.

This summary is based on *IDA Research Notes*, "Challenges in Cyberspace: The Human Dimension," by L. Welch, G. Cox, T. Barth, S. Horowitz, E. McDaniel, J. Warshafsky, and W. Rhoads, November 2018. The work was supported by IDA's Independent Research Program.