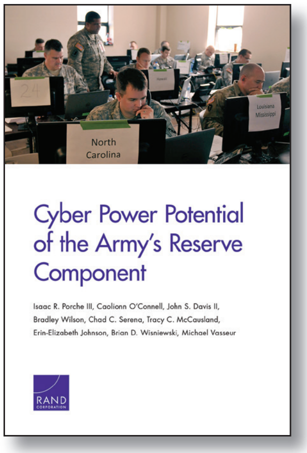
Cyber Power Potential of the Army's Reserve Component

Isaac R. Porche III, Caolionn O'Connell, John S. Davis II, Bradley Wilson, Chad C. Serena, Tracy C. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, Michael Vasseur

www.rand.org/t/RR1490



Cyber Power Potential of the Army's Reserve Component

Isaac R. Porche III, Caolionn O'Connell, John S. Davis II, Bradley Wilson, Chad C. Serena, Tracy C. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, Michael Vasseur

RAND CORPORATION

The military services are formalizing and bolstering their contribution to the nation's cyber force. This report identifies the number of Army reserve component (RC) personnel with cyber skills, to help identify ways in which these soldiers can be leveraged to conduct Army cyber operations. This report also describes the broader challenges and opportunities that the use of RC personnel presents.

RESEARCH QUESTIONS

- How can Army reserve component (RC) soldiers be leveraged to conduct cyber operations?
- Approximately how many Army RC personnel possess cyber skills, and which skills are most and least represented?
- What approaches should the Army use to recruit, train, and assign RC cyber personnel to support Army cyber operations?
- What broader challenges and opportunities does use of Army RC personnel for cyber operations present?

KEY FINDINGS

Untapped Cyber Potential Within the Army Reserve Component

- The level of cyber expertise that exists in the reserve component (RC) can be estimated with currently available data sources, including, potentially, novel uses of social media, such as LinkedIn profiles.
- The U.S. Department of Defense and the Army would benefit from a more detailed inventory of their cyber professionals, relative to what is provided by current data.
- Most (but not all) of the knowledge, skills, and abilities needed for cyber operations can be acquired via civilian-based training and experiences. Specifically, they can be acquired in part from popular certificate programs and civilian-sector on-the-job training.
- Sufficient operations tempo is vital to stay "cyber-sharp." Many guard and reserve soldiers are employed in leading-edge technology companies and have critical skills and experience in fielding the latest information technology systems, networks, and cybersecurity protocols. Arguably, their nonmilitary

continued on back

employment allows them to more easily maintain currency in their cyber skills, compared with some active component soldiers who are not engaged in cyber tasks on a frequent basis.

- There are personnel in the RC whose civilian cyber expertise is not being utilized in or applied to their Army careers. This possible untapped cyber potential is approximately 11,000 people who, at a minimum, have the propensity to learn the cyber skills needed for Army cyber operations.
- There are strong indications that many in the pool of untapped cyber potential have a desire to use their cyber-related skills in the Army. Many others who do not have cyber skills have a strong interest in acquiring them.

Recruiting More Cyber Personnel

- The Army will likely need more cybersecurity personnel in the future than it has today. This projected shortage is exacerbated by a rapidly growing demand for cybersecurity personnel in the private sector.
- The Army will need to continually adjust its strategies for recruiting, training, and qualifying cyber specialists. Potentially effective options for reserve recruiting include the use of expanded age ranges and generous compensation for sufficiently trained personnel in the private sector.
- The Army should use a cyber aptitude assessment tool, similar to what the Air Force, the National Security Agency, and other countries utilize, to aid recruiting for cyber personnel.

RAND ARROYO CENTER

RAND Arroyo Center is the Army's federally funded research and development center for studies and analyses. Its mission is to help Army leaders make decisions that are informed by objective, high-quality analysis. For more information visit Arroyo's website at **www.rand.org/ard**.