Air National Guard Cyber Force

Julia Warshafsky

The Challenge: The Air National Guard has a capable foundational cyber force, but it still faces challenges to manning and sustaining its cyber career fields. Additionally, the scope of this force's roles for and authorized activities in domestic cyber efforts is not yet well-defined.

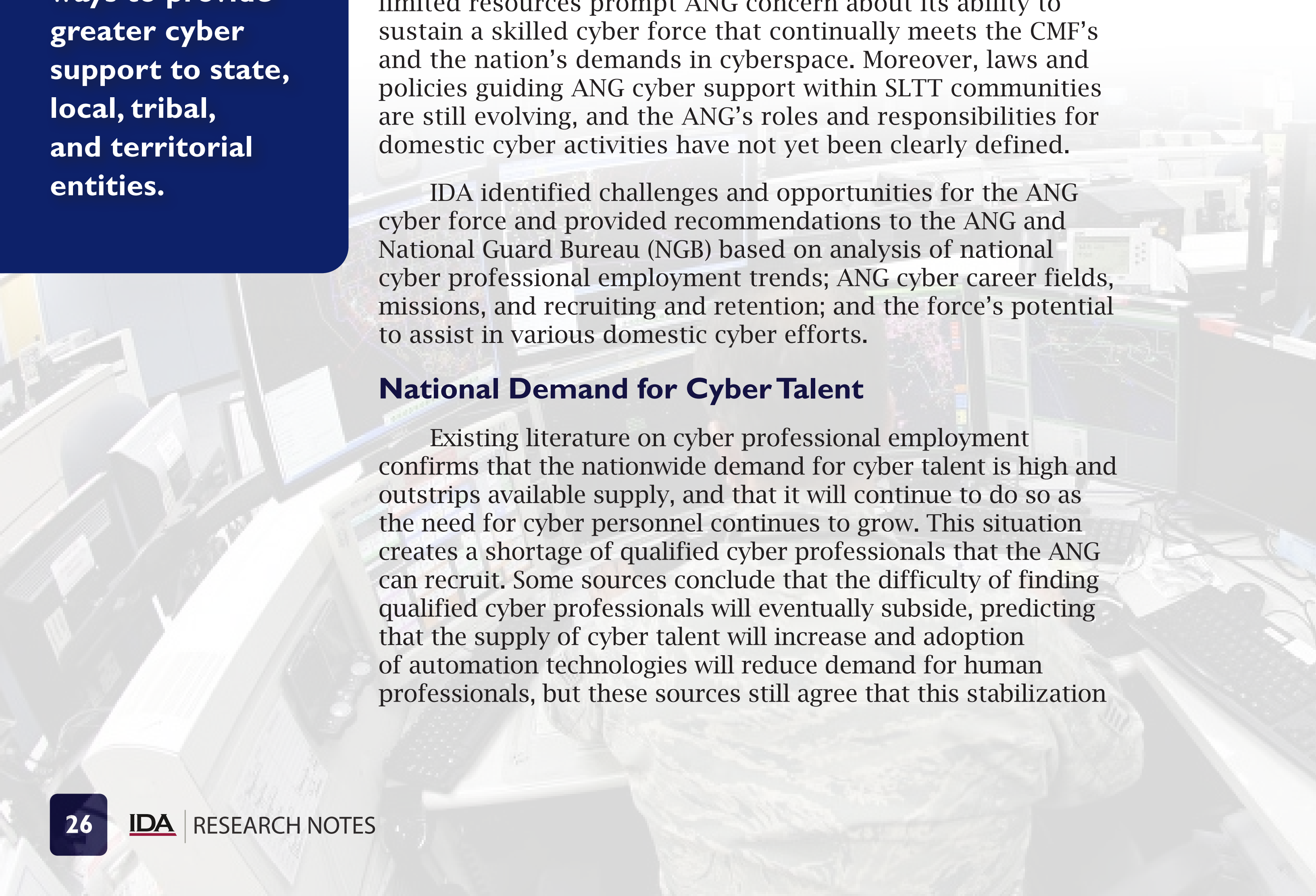
While working to man its cyber squadrons and ensure readiness for mobilizations to the Cyber Mission Force, the ANG has also been exploring ways to provide greater cyber support to state, local, tribal, and territorial entities.

In late 2014, the Air National Guard (ANG) began efforts to stand up 15 new cyberspace squadrons to support the Air Force component of the Cyber Mission Force (CMF) under U.S. Cyber Command. While working to man its cyber squadrons and ensure readiness for mobilizations to the CMF, the ANG has also been exploring ways to provide greater cyber support to state, local, tribal, and territorial (SLTT) entities. However, continuing shortages of cyber talent, declining propensity and eligibility for U.S. military service, stringent CMF and ANG cyber personnel eligibility requirements, and ANG Recruiting's limited resources prompt ANG concern about its ability to sustain a skilled cyber force that continually meets the CMF's and the nation's demands in cyberspace. Moreover, laws and policies guiding ANG cyber support within SLTT communities are still evolving, and the ANG's roles and responsibilities for domestic cyber activities have not yet been clearly defined.

IDA identified challenges and opportunities for the ANG cyber force and provided recommendations to the ANG and National Guard Bureau (NGB) based on analysis of national cyber professional employment trends; ANG cyber career fields, missions, and recruiting and retention; and the force's potential to assist in various domestic cyber efforts.

National Demand for Cyber Talent

Existing literature on cyber professional employment confirms that the nationwide demand for cyber talent is high and outstrips available supply, and that it will continue to do so as the need for cyber personnel continues to grow. This situation creates a shortage of qualified cyber professionals that the ANG can recruit. Some sources conclude that the difficulty of finding qualified cyber professionals will eventually subside, predicting that the supply of cyber talent will increase and adoption of automation technologies will reduce demand for human professionals, but these sources still agree that this stabilization



will not occur any time soon. (Libicki, Senty and Pollack 2014) (Vizard 2016)

We investigated the people who could potentially be *trained* to become ANG cyber personnel. Bureau of Labor Statistics data show that more than 5.6 million people, not including military members, federal employees outside the executive branch, or recent degree- or certificate-holders, are employed in computer, math, and engineering jobs nationwide. While there may be well more than 5 million people whose education and experience indicate that they could possibly be trained to become part-time cyber personnel to fill 1,065 ANG CMF positions, the potential supply pool quickly begins to shrink when the requirements for military service and, specifically, for military service in ANG cyber positions are taken into account.

Downward Trend in Military Service Propensity and Eligibility

The population of individuals who are both interested in and eligible for U.S. military service has been declining over the last two decades. Some of the factors for this are the declining veteran population (knowing someone who has been in the military is highly correlated with accession), false perceptions of the military, increasing propensity of high schoolers to attend college, and increasing disqualification for more than one reason (such as obesity, drug use, criminal activity, financial problems, certain tattoos and piercings, physical and medical conditions, and low scoring on the Armed Forces Qualification Test). At the same time that the pool of prospective recruits to the military is shrinking, the Services' need for greater numbers of specialized, technical talent has grown with the stand-up of the CMF and diversifying global cyber threats.

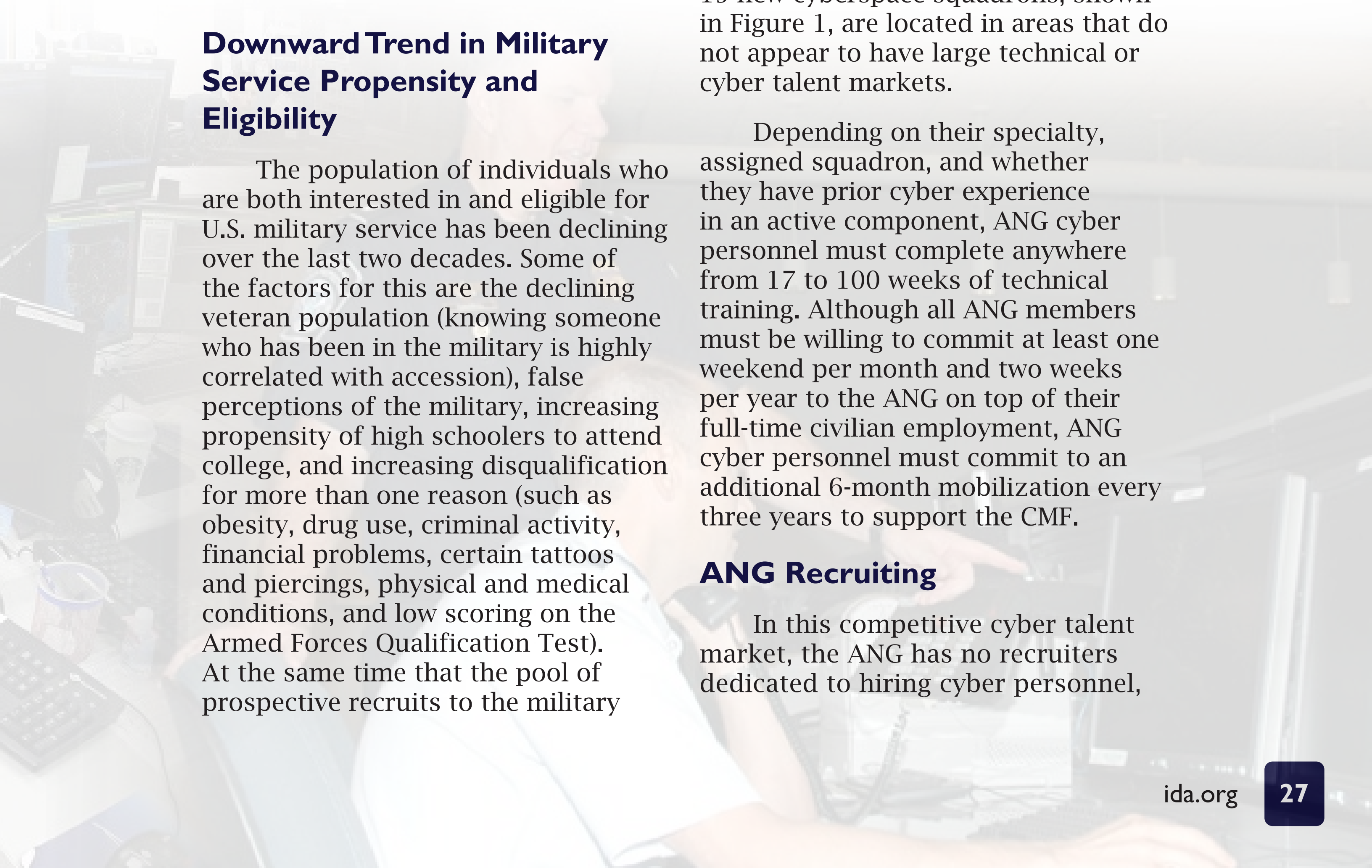
ANG Cyber Personnel Eligibility Requirements

Specific eligibility requirements for personnel to join an ANG cyber squadron further reduce the already limited pool of potential ANG recruits. ANG cyber personnel must complete basic military training if they have not previously served in the military, obtain a TS/SCI security clearance, and typically reside within a 50-mile radius of a squadron location. This last requirement poses additional challenges to sustaining a first-rate ANG cyber force, as some of the ANG's 15 new cyberspace squadrons, shown in Figure 1, are located in areas that do not appear to have large technical or cyber talent markets.

Depending on their specialty, assigned squadron, and whether they have prior cyber experience in an active component, ANG cyber personnel must complete anywhere from 17 to 100 weeks of technical training. Although all ANG members must be willing to commit at least one weekend per month and two weeks per year to the ANG on top of their full-time civilian employment, ANG cyber personnel must commit to an additional 6-month mobilization every three years to support the CMF.

ANG Recruiting

In this competitive cyber talent market, the ANG has no recruiters dedicated to hiring cyber personnel,



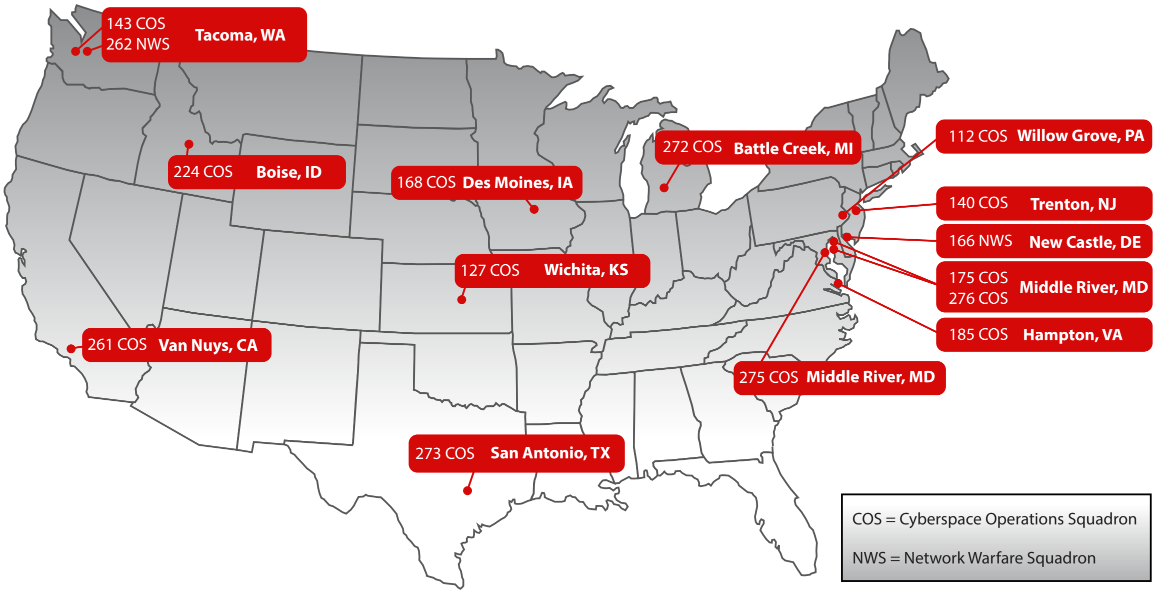


Figure 1. New Air National Guard Cyberspace Squadrons.

and ANG recruiters and staff lack adequate tools, technology, and resources to recruit specifically for cyber career fields, collect recruitment and retention data, and perform analyses of cyber workforce recruitment and retention. Because of the difficulty in finding non-prior service (NPS) personnel who can and are willing to meet the rigorous ANG cyber requirements, and the considerable time and cost involved in training NPS cyber recruits, the ANG fills its cyber positions largely by retraining current ANG members in other career fields or by recruiting personnel transferring from active duty who have had some level of cyber training. The active components are currently conducting pilot programs for the direct commissioning of recruits to cyber positions; however, similar pilot programs have not been authorized for the National Guard and Reserves.

Developing the ANG Domestic Cyber Roles

While originally developed to support Title 10 CMF missions, the ANG's cyber squadrons have also been working with their respective state governors, adjutants general, emergency management agencies, and public utilities to address state and local cybersecurity challenges. In the past few years, ANG cyber personnel have assisted in a number of state responses to domestic cyber incidents—such as those coinciding with the civil unrest in 2014 in Ferguson, Missouri, and in 2015 in Baltimore, Maryland—and have provided cyber protection capabilities such as vulnerability assessments to several state entities. Various reports over the last few years have called for the government to increase use of the National Guard for such efforts, citing the Guard's expanding cyber capabilities; ability to leverage private sector talent; tradition in building international, federal, and SLTT partnerships; and ability to operate under both state and federal authorities in three different duty statuses: State Active Duty, Title 32, and Title 10. However, laws and policies guiding ANG domestic cyber activities, in particular, are still evolving.

Cyber Incident Response

To date, the government has focused primarily on outlining the National Guard's role in cyber incident response, specifically in support of civil authorities during or after a cyber event, consistent with the National Guard's historical role in disaster response. National Guard capabilities for cyber incident response are being incorporated into DoD's policies for Defense Support of Civil Authorities and the National Cyber Incident Response Plan developed by the Department of Homeland Security. Directive-Type Memorandum 17-007, *Interim Policy and Guidance for Defense Support to Cyber Incident Response* (DSCIR), released in June 2017, is the latest guidance on responsibilities and use of the National Guard and other DoD Components for DSCIR activities.

Ongoing Cyber Protection

Less national-level focus has been devoted to how the National Guard could be used in an ongoing domestic cyber protection role. The May 2016 Deputy Secretary of Defense Policy Memorandum 16-002 offers the latest guidance on the National Guard's ability to coordinate with, train, advise, and assist mission partners in preventing, defending against, and recovering from cyber incidents. Although the memo is a step forward, it does not clearly establish the scope of the National Guard's authorized roles in advance of a domestic cyber incident or the specific actions the National Guard can undertake in cyberspace in Title 32 or State Active Duty status.

Recommendations

IDA recommends that the NGB and ANG focus on acquiring improved tools for workforce data collection and analysis and on examining the impact of both traditional and new incentives on the recruitment and retention of cyber personnel. We also recommend that the NGB and ANG create plans for National Guard engagement in accomplishing governors' cybersecurity goals, collaborate with stakeholders to implement command and control constructs in response to domestic cyber incidents, and conduct pilot projects to enhance National Guard domestic cyber protection efforts.

The National Guard and its stakeholders should determine the national-level vision for the Guard's future roles and responsibilities in cyberspace. Today, the National Guard has limited capacity for domestic cyber activities. If it is to be increasingly called upon for domestic cyber support, a construct allowing it to balance domestic efforts and CMF mobilizations will need to be developed.

References

115th Congress. 2017. Department of Defense Emergency Response Capabilities Database Enhancement Act of 2017, S. 307 and H.R. 1049.

Booz Allen Hamilton. 2015. *Cyber In-Security II: Closing the Federal Talent Gap.*

Burning Glass Technologies. 2015. "Job Market Intelligence: Cybersecurity Jobs, 2015."

Center for Strategic and International Studies. January 2017. *From Awareness to Action: A Cybersecurity Agenda for the 45th President.*

Commission on Enhancing National Cybersecurity. December 2016. "Report on Securing and Growing the Digital Economy." National Institute of Standards and Technology.

Council of Governors, Department of Homeland Security, and Department of Defense. 2014. "Joint Action Plan for State-Federal Unity of Effort on Cybersecurity." July.

Department of Defense. 2016. Deputy Secretary of Defense Policy Memorandum 16-002. "Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities." May.

Evans, Karen, and Franklin Reeder. 2010. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters,* CSIS Commission on Cybersecurity for the 44th Presidency, November 2010. Center for Strategic and International Studies.

Department of Defense. 2017. Directive-Type Memorandum 17-007. "Interim Policy and Guidance for Defense Support to Cyber Incident Response (DSCIR)." June.

Kosiak, Steven M. 2008. *Military Manpower for the Long Haul.* Center for Strategic and Budgetary Assessments.

Libicki, Martin C., David Senty, and Julia Pollack. 2014. *hacker5 Wanted: An Examination of the Cybersecurity Labor Market.* RAND Corporation.

Office of the Under Secretary of Defense, Personnel and Readiness. 2015. *Population Representation in the Military Services: Fiscal Year 2015 Summary Report.*

Orvis, Bruce R., Narayan Sastry, and Laurie L. McDonald. 1996. *Military Recruiting Outlook: Recent Trends in Enlistment Propensity and Conversion of Potential Enlisted Supply.* RAND.

Runey, Michael, and Charles Allen. 2015. "An All-Volunteer Force for Long-Term Success." *Military Review.*

Segal, David R., Jerald G. Bachman, Peter Freedman-Doan, and Patrick M. O'Malley. 1999. "Propensity to Serve in the U.S. Military: Temporal Trends and Subgroup Differences," *Armed Forces & Society.*

Soifer, Don, and Dan Goure. August 2016. "Six Principles for the National Guard's Cybersecurity Role Protecting the Grid." *In The National Interest.*

Vizard, Michael. 2016. "How Automation Will Affect Cybersecurity Jobs." *Dice Insights.*

Woodruff, Todd , Ryan Kelty, and David R. Segal. 2006. "Propensity to Serve and Motivation to Enlist among American Combat Soldiers." *Armed Forces & Society.*

Ms. Julia Warfshafsky is a Research Associate in IDA's Information Technology and Systems Division. She holds a Bachelor of Arts in political science and Spanish from the Pennsylvania State University, Schreyer Honors College.