

Messages from the top

"The goal of the program is to train and educate Army Reserve Soldiers to be elite cyber security professionals through classroom work and field experience. Each of these schools have been chosen for their excellence in cyber security research, teaching and their experience in helping the public and private sectors address cyber security issues."

*LTG Jeffrey Talley
Chief, Army Reserve
Commanding General, Army Reserve Command*

"The recent establishment of the Cyber Center of Excellence and Cyber Branch (Career Field 17), and the evolution of Army Cyber Command, are important milestones that will help us build, Train, develop, and sustain a highly talented and qualified cyber workforce."

*Hon. John McHugh
Secretary, U.S. Army
From the FY15 Secretary of the Army Top Priorities*

Phase I Partners

Universities:

University of Colorado Colorado Springs
Drexel University
George Mason University
Norwich University
University of Texas at San Antonio
University of Washington Tacoma

Employers:

AECOM Management Services
CALIBRE Systems, Inc.
Chevron Corporation
DynCorp International
EMC Corporation
Federal Bureau of Investigation
Microsoft
Professional Project Services
Rackspace US, Inc.
T-Mobile US, Inc.
Verizon



Cyber P3

Office of the Chief, Army Reserve

Facebook:

www.facebook.com/PrivatePublicPartnership

LinkedIn:

[www.linkedin.com/groups/
USAR-Private-Public-Partnership-1617837](http://www.linkedin.com/groups/USAR-Private-Public-Partnership-1617837)

Twitter:

www.twitter.com/USAR_P3O

Web:

www.usar.army.mil/PrivatePublicPartnership

Cyber Private Public Partnership

Office of the Chief, Army Reserve



Building the Future U.S. Army Reserve Cyber Force



Generating Readiness Through Partnerships

Mission Statement

The U.S. Army Reserve (USAR) Cyber program is designed to enhance our Soldiers' development and retention, while supporting individual, leader, and unit readiness in Cyber Security/ Defense across the USAR force.

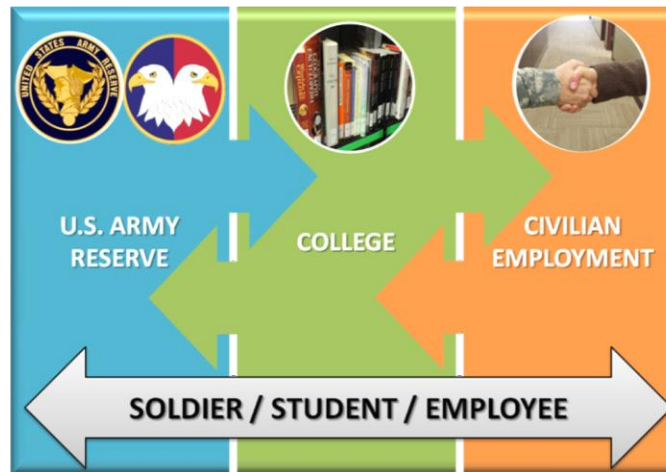
This program is designed to identify, understand, and fill a strategic opportunity for the USAR to provide expandable, tailored, and holistic solutions to the federal government, Department of Defense (DoD), and the public and private sectors.



Endstate

USAR cyber force Soldiers are educated through the Army Education System and college-level academic institutions. They develop critical thinking and technical skills, in order to react to dynamic cyber defense situations.

Two main components must function together to fluidly meet the USAR cyber force requirements. The first is stable employment with industry and/or government. The second aspect is the alignment of civilian and military cyber-related academic programs. A successful process maintains and enhances cyber skills.



Protecting the Nation - Cyber

The United States relies on information systems and data for almost every level of national power. The U.S. critical infrastructure and military operations are at risk from advanced persistent threats (nation-states, non-state actors, terrorists, and criminal networks).

The nature of cyber defense was formerly focused on "passive defense," which was reliant on redundancies and firewalls. The defense industry has now transitioned to "active defense," which emphasizes critical thinking skills and cyber professionals. The demand for these individuals and units far outpaces the cyber Soldier and unit inventory.

The USAR cyber Soldier is unique in that he/she bridges the gap between the military and civilian employment fields.

Lines of Effort

- 1. Form national and regional academic networks with universities that boast nationally recognized Cyber Security programs that will be customized to meet the Army requirements. To date there are signed Memorandums of Understanding (MOUs) with six universities, and additional academic institutions have been identified to participate in Phase II over the next year.*
- 2. Form national and regional employment networks to support employment of USAR Cyber Soldiers. Networks are designed for entry level through master Cyber Security professionals.*
- 3. Form community outreach programs in Cyber Security to reach and support development of middle and high school Students as well as college students.*

