



FACT SHEET

U.S. Army Cyber Command and Second Army
The Nation's Army in Cyberspace
www.arcyber.army.mil

THE FACTS: TRAINING FOR CYBER SOLDIERS

The Cyber branch is the Army's newest, and building the Army cyber force is the mission of the Army Cyber Center of Excellence (CCoE) and the Army Cyber School at Fort Gordon, Ga. The center is in its initial operating status as of this writing.



What are the Cyber Center of Excellence and the Cyber School?

As the Army's force modernization proponent for cyberspace operations, signal/communications networks and information services, and electronic warfare, the CCoE integrates and develops doctrine, organization, training, materiel, leadership, personnel and facilities, and coordinates with the Army

Intelligence Center of Excellence for institutional intelligence support to cyberspace operations. The CCoE ensures Army cyberspace, electronic warfare and signal operations capabilities evolve with joint force requirements and capabilities. The Cyber School lays the foundation for development of skilled cyber forces that are trained to joint standards to meet combatant commanders' current and future force requirements.

The CCoE's current workforce capitalizes on significant investments by the Army's Intelligence and Signal specialties, and includes officers, warrant officers and enlisted Soldiers with backgrounds and training in computer science, programming, network engineering, analysis and electronic warfare.

What training will be available for Cyber Soldiers?

As they transition into the Army Cyber branch (Career Management Field 17), most Soldiers working in the cyber domain will get additional training to further develop their technical expertise and broaden their operational experience.

ABOUT US: United States Army Cyber Command and Second Army directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

As of 15 March 2016

Those in the Cyber branch will continue to work closely with their Intelligence and Signal counterparts, as they have reinforcing missions.

Newcomers to the Cyber branch will also complete resident training at the Cyber School. The first training offered was the Basic Officers Leader Course, started in August 2015. The school's catalog is expected to expand in phases through 2017. A two-tiered, 14-week warrant officer training program is planned for May 2016, with an advanced course for those who already have significant experience in cyber fields and a basic course for those newer to the work. The first new enlisted cyber Soldiers entered the Army in October 2015 and began Advanced Individual Training in February 2016. Because cyber operates as a part of a joint force, the first 22-week phase of AIT will be the Navy Joint Cyber Analysis Course at Pensacola, Florida. The second 22-week phase will be at Fort Gordon.

All three groups -- officer, warrant officer and enlisted - will conclude their training by participating together in joint exercises, ensuring that they join the Department of Defense's Cyber Mission Force fully trained to U.S. Cyber Command joint standards and well prepared to support Army units at all levels.

How can you get more information on the CCoE and Cyber School?

For more information on the CCoE and the Cyber School, visit the CCoE website at <http://cybercoe.army.mil>.

How can you get more information on Cyber careers?

For more information on joining the Army to pursue a cyber career as an enlisted Soldier, visit the computer and technology page at goarmy.com. DoD Common Access Card holders looking for information on Army enlisted, officer and warrant officer cyber careers can go to the Cyber Branch Assignment Management page at the Army Human Resources Command website at <https://www.hrc.army.mil/>.



ABOUT US: United States Army Cyber Command and Second Army directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

As of 15 March 2016