U.S. Army Cyber School
Distinctive Unit Insignia

Symbolism: Black signifies the hidden nature of cyberspace operations and the importance of privacy and security. Silver (Gray) embodies the technological emphasis and the balance between offensive and defensive capabilities. Gold is symbolic of success and emphasizes domination in the cyber domain. The lightning bolts indicate the swift nature of electronic warfare. The sword represents offensive missions, while the shield is indicative of defense. The keyhole alludes to exploitation missions and is in the center of the shield to represent every defense having a weakness.

Background: The distinctive unit insignia was approved on 19 November 2015.

U.S. Army Cyber School Shoulder Sleeve Insignia

Symbolism: The black and white colors on the shield reflect the importance of digital data communications to the cyber mission. The crossed lightning bolts represent the convergence of the Electronic Warfare and Cyber Schools under one torch. The torch represents the Cyber Training Battalion’s primary mission as an educational institution.

Background: The shoulder sleeve insignia was approved on 19 November 2015.

633 Barnes Avenue
Building 25601
Fort Gordon, GA 30905
https://cyberschool.army.mil/
Message from the Commandant

Cyber Team,

It has been an extremely busy but exciting first 9 months of my tenure as your Commandant. I see progress every day in all of our lines of effort – Build the School, Build the Branch, Train the Force, and Establish the Culture – and each one of you are critical to those ends. I am heartened by the intensity of your focus to build Cyber into a dynamic and capable branch. I remain privileged to serve with you and I thank you for your service to the Army. Here at the Cyber School, we are excited to announce several key events on the horizon.

On the 10 November 2016, the Army’s Human Resources Command (HRC) published a series of Notices of Future Change (NoFC) that effective 1 October 2018, the Electronic Warfare (EW)/Career Field 29 will be subsumed into the Cyber Corps. This action supports the published Cyber Center of Excellence strategic plan for the merger of Cyber and Electronic Warfare. This proposal meets the CSA’s intent of mitigating capability gaps between Cyber, Electronic Warfare, and Signal by providing a single institutional responsibility for all the aforementioned capabilities to support national, strategic, operational, and tactical Army Cyber missions. With this change, the Cyber Corps will nearly double in size, bringing with it an immense requirement for training. We will not wait until 2018 to begin this task, however. We will deliver training through a number of methods including home station training, TDY and PME channels. I have already made one trip to Fort Sill to visit the EW College and plan to make regular visits to lend my support to the process of integration. As the Cyber Corps evolves to provide more options for commanders at the corps and below, the integration of EW Soldiers and officers will be critical.

This March, the Cyber School and Fort Gordon will welcome the very first 17C Soldiers into Advanced Individual Training. These young Soldiers will have completed basic training and the 24-week Joint Cyber Analysis Course in Pensacola, Florida before arriving at Fort Gordon for an additional 20 weeks of training, including a common technical core, defensive and offensive methodologies and a culminating exercise. This training promises to turn out highly skilled cyber Soldiers who are prepared to make an immediate impact in the Cyber Corps. In a recent visit to Pensacola, CSM Rinehart and I saw first-hand the energy these Soldiers will bring to the complex problems and capable enemy we face. These Soldiers will be trained at Fort Gordon by some of the best and brightest cyber NCOs who are tasked with not only instilling Army Values and discipline, but training the intricacies of cyberspace and conducting operations within it. I have no doubt that we will provide the highest level of training to those Soldiers and you can look forward to seeing them in your formation by late summer.

Finally, I want to thank the Cyber Center of Excellence, MG Morrison and his predecessor, MG Fogarty, for all their support in establishing a temporary SCIF to conduct training and support the Cyber School’s growth over the next few years. In an era of shrinking budgets and competing priorities, they enabled the construction of a 27,000 square foot facility to bridge the gap before the larger, Cyber University plan is implemented in 2021.

As we close out another holiday season, I’d like for everyone to know that I am committed to the mission in front of us but also how we care for our families at home. Families are the ones that often carry the burden when you are away at training or deployed. It is important to thank them for their support and personal sacrifice that allows us to be Soldiers and Civilians on the Army team. I ask that each of you continue to respect and learn from each other as our diversity in backgrounds, training and other areas makes us the dynamic force that we are.

Dominate the Domain!
Message from the Cyber Corps CSM

The Cyber School has been busy on your behalf. We will start our first iteration of Phase II, AIT 17C10 in the month of March. Following completion of the Joint Cyber Analysis Course at Pensacola, FL our initial entry 17C10s and reclassifying 17Cs will proceed to Fort Gordon, GA to begin the second phase of their AIT. In the past, troops completed training in Florida and proceeded to their first unit of assignment; the 780th MI Brigade or the Cyber Protection Brigade. In the past, they would then begin the necessary training to certify on a work role to work on one of the teams available in those brigades. Beginning in March 2017, 17C JCAC graduates will begin a second phase 5 ½ month training curriculum in the Cyber School to qualify them in all but three enlisted work roles on all types of teams. This will allow them to proceed upon graduation to either one of the cyber Brigades and begin work after certifying in Joint Qualification Requirements (JQR) for the work role they are placed within. This approach will save the Department dollars and resources each year, enable a ready work force upon assignment, and lessen the training requirements upon arrival to their first unit of assignment.

The Cyber School is also in the second pilot phase of a Title 10 Operator course to support Army missions. This is a five week course that presents new graduates prepared to begin JQR on mission sets currently being executed from the Joint Mission Operations Center, Fort Meade, MD or GA. This course was put together by operational force NCOs, Warrant Officers, and Cyber School cadre, taught in the U.S. Army Cyber School. Incorporating operational Soldiers into course development and instruction assists the school course managers in maintaining relevant, current curriculum within the schoolhouse.

The Cyber School trained 161 students in FY16 and is projected to train 561 students in FY17. Student loads will continue to grow each year through 2019. This increase in student load will incorporate our National Guard and Reserve component Soldiers, as well as sister services vying for seats. We are scheduled to run seven iterations of Phase II AIT in FY17. We also continue to run 17C ALC and SLC. The Cyber School will run three ALC courses and two SLC courses in FY17. I don’t need to mention the necessity of attending PME when available. This will require NCOs to remain physically fit, mentally sharp, and ready to meet the challenges of a changing Army. Your SSD requirements remain foremost to ensure you are prepared to attend PME when seats are available.

Finally, I want to take a moment and discuss the teaching approach we are taking at the Cyber School with all curriculum. We have embraced the adult learning model and incorporated the Adaptive Soldier Leader Training and Education methodology. ASLTE focuses on a framework that allows evaluation of 21st Century Soldier Competencies rather than teaching a set of steps to accomplish. This methodology is baked into all programs of instruction and instead of teaching students steps to take to accomplish tasks, it starts with the desired outcomes, perhaps a short demonstration, and expects the learner to take the lead in achieving those outcomes with a highly technical cadre providing facilitation. There are multiple paths to success and each pathway has merit. This method of instruction allows learner centric skills to be applied to the process and the student takes an active role in achieving the desired outcome. The act of memorizing a list of tasks to achieve a goal does not work well in an environment where multiple avenues exist to reach the goal. Each avenue brings its own unique challenges and should be allowed as a possible solution. The ultimate goal is the desired outcome. It has changed the way we deliver our courseware and certainly produces a better trained troop capable of meeting the demands of cyber-space operations.

Thank you for all you do to make our branch the best in the Army.

Defend, Attack, Exploit!

WILLIAM M. RINEHART

CSM, USA

Cyber & E.W. Corps
Office Chief of Cyber (OCC)

OCC — Officer Division

United States Army Recruiting Command continues the Warrant Officer Accessions Board process from 28 November to 02 December. We are expecting some great results from this board and look forward to working with all of the 170A (Cyber Operations Technician), and the 290A (Electronic Warfare Technician) Warrant Officers who are selected. There are a lot of truly talented NCOs out there who wanted to take a leap into the Warrant Officer Branch and become Technical Experts. I want to stress this for everyone who submitted a packet, the highest preference is always given to the NCOs in 17, 25, and 35 series with Cyber mission force experience. However, we always stress the importance that all NCOs, from all career fields, and sister services are eligible to apply, if you meet the minimum requirements as outlined on the USAREC warrant officer recruiting.

OCC — NG/RESERVE Division

The Reserve Component plays a key role in bolstering the nation's defensive and offensive capabilities as the Army develops increased Cyber capabilities throughout the force. Both the Army Reserve and the Army National Guard have Cyber units designed to conduct military cyber operations, defend the DODIN networks and actively defeat adversary activity. Citizen Soldiers bring a wealth of experience, education and knowledge to the force and Officers, Warrant Officers and Enlisted leaders have increased opportunities to significantly impact the Cyberspace workforce as Cyber Warriors. There are significant opportunities for Reserve Soldiers to participate in Cyber operations and increase the critical capabilities the Nation needs. As the Reserve Component continues to grow resources and force structure to meet the Nation's requirements, Cyber service opportunities have expanded across the country. In the upcoming months, the USAR and ARNG will be accepting additional transfer and reclassification packets for service in the Cyber career field. Officers, Warrant Officers and Enlisted Soldiers that possess a sincere desire to serve in the Cyber career field, have significant Cyber experience and display strong Information Technology backgrounds should contact their respective Career Counselors and Career Management Officers for more information.

<table>
<thead>
<tr>
<th>OCC Director</th>
<th>COL Chris Wade</th>
<th>706-791-5119</th>
<th><a href="mailto:chris.a.wade3.mil@mail.mil">chris.a.wade3.mil@mail.mil</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>OCC Deputy Director</td>
<td>Mr. Shawn Bova</td>
<td>706-791-5129</td>
<td><a href="mailto:shawn.d.bova.civ@mail.mil">shawn.d.bova.civ@mail.mil</a></td>
</tr>
<tr>
<td>Proponent SGM</td>
<td>SGM James Krog</td>
<td>706-791-6891</td>
<td><a href="mailto:james.m.krog.mil@mail.mil">james.m.krog.mil@mail.mil</a></td>
</tr>
<tr>
<td>National Guard/Reserve Liaison</td>
<td>LTC Montrese Love</td>
<td>706-791-8902</td>
<td><a href="mailto:montrese.r.love.mil@mail.mil">montrese.r.love.mil@mail.mil</a></td>
</tr>
<tr>
<td>Force Integration Specialist</td>
<td>Mr. Andre Golden</td>
<td>706-791-4406</td>
<td><a href="mailto:andre.a.golden.civ@mail.mil">andre.a.golden.civ@mail.mil</a></td>
</tr>
<tr>
<td>Force Management Officer</td>
<td>MAJ Lauren Maloney</td>
<td>706-791-5141</td>
<td><a href="mailto:lauren.r.maloney.mil@mail.mil">lauren.r.maloney.mil@mail.mil</a></td>
</tr>
<tr>
<td>Officer Division Chief</td>
<td>Mr. Phillip Williams</td>
<td>706-791-5142</td>
<td><a href="mailto:philip.e.williams.civ@mail.mil">philip.e.williams.civ@mail.mil</a></td>
</tr>
<tr>
<td>Career Manager 170A/290A</td>
<td>CW5 David Koscinch</td>
<td>706-791-4939</td>
<td><a href="mailto:david.a.koscinch.mil@mail.mil">david.a.koscinch.mil@mail.mil</a></td>
</tr>
<tr>
<td>Force Integration Specialist</td>
<td>Mr. Larry Pugh</td>
<td>706-791-5147</td>
<td><a href="mailto:larry.c.pugh.civ@mail.mil">larry.c.pugh.civ@mail.mil</a></td>
</tr>
<tr>
<td>Enlisted Division Chief</td>
<td>Mr. John Plotts</td>
<td>706-791-5112</td>
<td><a href="mailto:john.r.plotts.civ@mail.mil">john.r.plotts.civ@mail.mil</a></td>
</tr>
<tr>
<td>Senior Career Mgmt NCO</td>
<td>MSG Julius Williams</td>
<td>706-791-6887</td>
<td><a href="mailto:julius.n.williams.mil@mail.mil">julius.n.williams.mil@mail.mil</a></td>
</tr>
<tr>
<td>Career Manager 17C</td>
<td>SFC Newtina Mitchell</td>
<td>706-791-6218</td>
<td><a href="mailto:newtina.f.mitchell.mil@mail.mil">newtina.f.mitchell.mil@mail.mil</a></td>
</tr>
<tr>
<td>Career Manager 29E</td>
<td>SFC Antraun Glover</td>
<td>706-791-6887</td>
<td><a href="mailto:antraun.t.glover.mil@mail.mil">antraun.t.glover.mil@mail.mil</a></td>
</tr>
<tr>
<td>Career Manager 29E</td>
<td>SSG Wesly Linton</td>
<td>706-791-4401</td>
<td><a href="mailto:wesley.m.linton.mil@mail.mil">wesley.m.linton.mil@mail.mil</a></td>
</tr>
<tr>
<td>Historian</td>
<td>Mr. Scott Anderson</td>
<td>706-791-6877</td>
<td><a href="mailto:scott.r.anderson67.civ@mail.mil">scott.r.anderson67.civ@mail.mil</a></td>
</tr>
</tbody>
</table>
The Technical Training and Education Directorate continues to make great strides as we continue to bring new courses on line and refine courses that have already been made available.

Over the past quarter the inaugural Cyber Basic Officer Leader Course and Common Technical Core Courses graduated their first student cohorts. These students will enter the force with a very solid technical foundation that will allow them to make immediate contributions to Offensive or Defensive Cyber formations. We also graduated the first cohort of the Advanced Leaders Course and Senior Leaders course which helped to prepare cyber leaders to take their place along other NCO MOS’s that form the backbone of the United States Army.

Army Leaders Cyberspace Operations Course (ALCOC) instructors traveled to Fort Riley, KS to train the 1st BDE of the 1st Armored Division as it prepares for an upcoming National Training Center Rotation. This course prepared 1st BDE 1st AD to integrate effects produced via cyberspace into its operational planning.

The FA29 and 290A courses incorporated a new module into their curriculums that tested the ability of students to learn how to operate and operationalize open source and commercial off the shelf technologies.

We expect the next quarter to be even busier and better than this one was as we continue our efforts to train the force. Dominate the Domain!!!

CTED — Cyber Leader College

Joint Advanced Cyber Warfare Course – Georgia (JACWC-G):

Another successful iteration of JACWC-G just wrapped up, with 44 newly minted graduates representing a spectrum of Cyber Warfare specialties. The two-week course, conducted in the NSA-Georgia facility, is designed to provide an orientation of the U.S. Cyber Command, the global cryptologic platform, the Intelligence Community, the USG cyber community of interest, and major partners from local industry in the conduct of cyber warfare, mitigation of cyber threats, operations, planning, and analysis of desired effects. The student body consisted of NCOs attending the Army Advanced Leaders Course, Junior Army Officers attending the Cyber Operations Officer Course, and a variety of senior leaders from the Cyber Protection Brigade and the 782nd MI Battalion.

At the conclusion of the course, the students presented their research papers and discussed various aspects and implications of cyber operations. The papers spanned topics from current trends in cyberspace, operating in congested and contested domains, the importance of investing in Science Technology Engineering Mathematics (STEM) academic programs, and talent management in a competitive field. The course culminated with a key note presentation from CSM Rinehart who is the Cyber Corps Command Sergeant Major. The ending key note included vital insight about the development and the way ahead for USCYBERCOM. The course enabled the graduates to create sustainable professional relationships, and gain perspective of the larger context of cyberspace operations which will assist them in the future execution of operations in cyber space.
On 21 OCT 2016, the Army's second 17C Advanced Leader's Course graduated with 17 students. The Advanced Leader's Course provided the 17C Noncommissioned Officers with the skills to grow them into the professional and technical leader needed to maintain, sustain and direct their unit in accordance with regulations and their capabilities. These NCO's leave the academy equipped with a refresher of basic and advanced Soldier skills; conducting training in areas of, drill and ceremony, proper wear of the uniform, Physical Readiness Training, company and platoon drills, in-ranks inspections, and receive technical training. This course provided these Noncommissioned Officers with the Army's foundational building blocks of what it means to be a Noncommissioned Officer, providing the force with a fully competent and capable Army leader upon arrival back to their respective units.

The 17C Students learned the critical requirement for the cyber planners to build out adversary views and describe the operational environment in Cyberspace in terms of operational variables. The course focused on Cyber Teams across the Military Force, familiarizing each student of the effectiveness across each team and how Offensive Cyber Operation planners conduct access-based planning and equipped each individual with the understanding of capabilities-based targeting.

While here at the Advanced Leader Course, they not only accomplished outstanding achievements for themselves and the academy, but for Fort Gordon and the greater Augusta Community as well. Class 17C 502-16 contributed a combined total of 136 hours of community services to Fort Gordon and the CRSA supporting the Augusta Partnership for Children aiding the organization’s diaper supply, helping to provide new Mother's in the local CSRA with free cases of diapers.

**17 Series Training Pipeline Update**

With the advent of the updated USCYBERCOM J7 training pipeline and the approval of the DCITA Cyber Protection Team Core (CPT-C) methodologies class, the Cyber School added the one week CPT-C class to all MOS qualifying courses. In a demonstration of the joint courseware model, DCITA will continue to own and manage the CPT-C courseware, with an agreement for the Cyber School to instruct this material. CPT-C is scheduled directly after Cyber Common Technical Core (CCTC) to allow Cyber Mission Force units to send Soldiers to one 10 week block of training. In addition to adding CPT-C, the AIT and OOC pipelines now reflect a two-week programming module that will enable Soldiers to brush up on programming-related Joint Cyber Analysis Course (JCAC) knowledge, skills, and abilities prior to CCTC. Finally, 17X students wishing to validate the CCNA and CISSP modules must possess a current CCNA or CISSP certification at the time they report to the Cyber Training Battalion; this will enable them to request approval of a self-development plan during that time. The updated curriculum is available from the CTED page on the cyberschool.army.mil website.
The first quarter of fiscal year 17 promises new opportunities and challenges for the EW College. Some of the events happening or slated to occur are the activation of C CO, conducting the first company CREW specialist course classes, the integration of the Electronic Warfare Planning and Management Tool (EWPMT), and the updating of course ware from the results of two critical task site selection boards.

**Activation of C CO:**
The EW College FY17 TDA includes the addition new positions, two of which are First Sergeant and Company Commander of Crow Company CTB. These positions form the nucleus of a headquarters section for C CO at Ft. Sill, OK which will be the third company of the Cyber Training Battalion at Ft. Gordon, GA. The activation ceremony was on 19 January 2017 at Rinehart Gym FSOK. CPT Jackson Wittkamper assumed command and 1SG Darnell Folsom assumed responsibility for C Company CTB.

**Company CREW Specialist Course (CCSC) - ASI 1K:**
CREW Master Gunner Course (CMGC) was moved from the ICoE at Ft. Huachuca, AZ to the EW College at Ft. Sill, OK and renamed the Company CREW Specialist Course (CCSC). Besides getting a new home and name the CCSC syllabus was revamped to meet the current and futures needs of Soldiers at Company/Troop/Battery level.

**Electronic Warfare Planning and Management Tool (EWPMT):**
The EW College is in the process of building a EWPMT, capability drop one lab. EWPMT is inclusive Cyber Electromagnetic Activities (CEMA) planning software on a closed system. Future capability drop will be an open system connected to US Army mission command systems further enhancing EW Soldier’s ability to plan CEMA. EWPMT improves the EW Soldier’s ability to plan and execute CEMA in support of the maneuver commander’s mission.

**29E2-3 and 290A WOBC/AC CTSSB:**
The Critical Task Site Selection Boards (CTSSB) for both the 29E2-3, 290A Warrant Officer Basic, and Advanced Courses were completed recently. The results from these boards are used to improve the course material. The CTSSB recommendations stressed innovative problem solving methods to prepare the graduates to meet the needs of providing CEMA planning support and integration to maneuver commanders in an ever changing electromagnetic environment.