Cyber Branch

1. Introduction

a. Purpose of the Cyber Branch. The Cyber Branch plans, integrates, synchronizes, and executes cyberspace and electromagnetic warfare operations. Cyberspace Operations (CO) are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. The interrelated missions of CO are defensive cyberspace operations (DCO), offensive cyberspace operations (OCO), and Department of Defense Information Network (DODIN) operations. Electromagnetic Warfare (EW) operations are military actions involving the use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) in order to support the commander's intent and concept of operations. EW includes electromagnetic attack, electromagnetic protect, and electromagnetic support. Cyber Officers conduct cyberspace and EW operations, with both lethal and nonlethal ends, to enable the commander's ability to mass effects and gain advantages in or through the cyberspace domain and EMS battlespace, and across other domains during multi-domain operations (MDO) in support of unified land operations (ULO) objectives. Cyber Officers also design, develop, and deliver relevant, timely, and effective software and hardware solutions to enable and enhance CO and EW effects at both echelons above corps (EAC) and echelons below corps (EBC). Cyber is the only branch specifically designed to engage adversaries directly within the cyberspace domain and the EMS battlespace through the employment of precision effects to deny, degrade, disrupt, destroy, or manipulate adversary capabilities while simultaneously ensuring the commander's freedom of maneuver across all domains. Cyber Officers must be U.S. citizens, with no other citizenships, who obtain and maintain a TOP SECRET clearance with access to Sensitive Compartmented Information (TS/SCI) in order to be awarded and retain a Cyber Branch AOC. A favorable special background investigation is also required. Additionally, Cyber Officers must be capable of passing a counterintelligence scope polygraph to serve in specific positions.

b. Proponent information. Commandant, U.S. Army Cyber School, Fort Gordon, GA 30905-5735. For more information, contact the Officer Division, Office of the Chief of Cyber at usarmy.gordon.cyber-coe.mbx.occ-officers@army.mil.

c. Functions. Cyber Officers are experts in projecting power in and through cyberspace and the EMS, and are proficient in all forms of decisive action: offense, defense, stability operations, and Defense Support of Civil Authorities (DSCA). Cyber Officers must fully understand maneuver operations to ensure synchronized, relevant, and integrated effects that enable success in ever-changing strategic, operational, and tactical environments. The Cyber Warfare Officer is the authority for the operations and employment of Cyber Mission Forces (CMF) and other CO elements, including planning, integrating, synchronizing, and/or executing DCO, OCO, or DODIN operations at all echelons. The Cyber Electromagnetic Warfare Officer (CEWO) is the commander's subject matter expert for planning, integrating, synchronizing, and/or executing cyberspace and EW operations at all echelons. The Cyber Capabilities Development Officer (CCDO) is the primary lead for providing cyberspace capabilities to support and enable CO and EW missions at all echelons. Cyber Officers serve primarily in Army, joint, interagency, and multinational (JIM) positions to fill a variety of key positions performing the following functions and tasks:

(1) Execute mission command of Cyber and EW units/elements in support of MDO and ULO.

(2) Integrate cyberspace and EW operations capabilities into MDO and ULO at all echelons.

(3) Develop doctrine, organizations, and equipment for CO and EW missions/units.

(4) Serve in staff positions and activities requiring general cyberspace and EW operations skills and expertise.

(5) Serve as instructors at pre-commissioning programs, service schools, and colleges.

(6) Design, develop, and deliver software and hardware solutions and related capabilities to enhance cyberspace and EW operations.

(7) Plan multi-faceted cyberspace and EW operations and campaigns against adversaries.

d. Branch eligibility. Officers who desire to transfer into the Cyber Branch should submit a request in accordance with: AR 614-100, chapter 4; U.S. Army Human Resources Command's most recent Voluntary Transfer Incentive Program (VTIP) MILPER message; and/or all policies and procedures for the applicable Component. Additionally, the applicant must meet the Cyber Branch requirements outlined in DA Pamphlet 611-21.

2. Officer Characteristics Required

a. The core competencies and essential capabilities of Cyber Officers. The Cyber Branch requires officers to become experts at building and leading mission-focused teams of Soldiers and the Department of the Army Civilians. They must be well-versed in all aspects of CO and EW, as well as, combined arms tactics, techniques, and procedures in order to support MDO and ULO at all echelons. They must be mentally and physically disciplined, possessing intrapersonal and interpersonal skills to enable them to perform as agile, adaptive, and innovative officers in all situations.

b. Characteristics required of all officers. Cyber Officers are selected for their leadership potential, technical aptitude, resilience, and ethics, accompanied by Cyber-focused passion and foundational preparation. They are trained and educated to effectively and efficiently perform duties as a leader, planner, and trainer of CO and EW, as well as, being a developer of associated software and hardware capabilities. They are adaptive, innovative, self-motivated, and able to operate without direct supervision. The Cyber Branch values inspirational leaders who possess relevant education, and who are logical, analytical, innovative, technologically adept problem solvers.

c. Unique knowledge and skills of a Cyber Officer. Cyber officers must possess the following knowledge and skills:

(1) Mastery of knowledge related to the cyberspace domain, the EMS battlespace, and the DODIN, including associated doctrine, policies, regulations, laws, and relevant technologies.

(2) Refined knowledge and skills in developing CO and EW capabilities and solutions.

(3) Strong leadership skills in CO and EW tactics, techniques, and procedures, as well as, knowledgeable of all types of maneuver and support operations.

(4) Understanding and ability to execute MDMP/JPP staff processes to employ cyberspace and EW actions and assets in support of MDO and ULO, including planning, coordinating, integrating, and assessing CO and EW capabilities to support the combatant commander.

(5) Able to leverage relevant Special Access Programs, special projects, and capability development efforts in order to plan, integrate, and synchronize current, emerging, and specialized Cyber and EW solutions into operations, as required.

(6) Communicate technical concepts clearly with accuracy and precision in terms that enable military commanders and civilian leaders to make decisions and assume necessary risks.

d. Unique attributes for Cyber Officers. The Cyber branch requires dynamic, competent, well-trained leaders at all levels who understand MDO and ULO in order to effectively plan, integrate, synchronize, and/or execute CO and EW. Cyber Officers must also be technologically adept, innovative, logical, analytical problem solvers and inspirational leaders, as well as, possess the following attributes:

(1) *Spatial intelligence and visualization.* Specific spatial intelligence attributes are required for Cyber Officers in order to visualize multi-dimensional environments and understand how to optimize CO and EW capabilities in support of strategic, operational, and tactical objectives. This includes understanding the nuances of the three cyberspace layers (physical, logical, and cyber-persona), as well as, all operational domains for effectively conducting CO and EW in support of MDO and ULO.

(2) *Diligence and attention to detail.* Cyber Officers must possess and demonstrate a high degree of diligence and attention to detail, as part of a highly technical and technological career field, to ensure timely and effective delivery of CO and EW capabilities and effects.

(3) *Expeditionary mindset.* Cyber Officers must be ready to provide CO and EW effects anywhere in the world, in either long or short duration, and an agile and adaptive manner. The application of CO and EW effects includes JIM assets that must be synchronized in MDO and ULO.

(4) *Multi-echelon and multi-domain collaboration*. Cyber Officers must be effective and efficient in multi-echelon and multi-domain collaboration in support of joint service cyber components. Planning, integrating, synchronizing, and executing cyberspace and EW operations often affect multiple services, agencies, and domains, which requires strong collaborative skills.

3. Cyber Branch Officer Development

a. Cyber officer development – areas of concentration. Cyber Officers receive initial and advanced training for AOCs 17A, 17B, and/or 17D. Cyber Officers should expect permeability between the 17-series AOCs in which they are qualified, depending on the availability of positions, personnel, and training. Additionally, successful service in key developmental positions for any 17-series AOC counts as key developmental credit for all 17-series Cyber Officers in the same rank/grade. For Cyber Officers serving in key developmental positions of the next higher rank/grade, that may also be used as key developmental credit in their current rank/grade. Prior to attending the 17B CEWO Qualification Course (formerly, EW Officer Qualification Course), Cyber Officers (starting at lieutenant) must first be qualified as AOC 17A. Cyber Officer who earn both AOCs 17A and 17B will have opportunities to leverage those skillsets throughout their careers, while those who earn AOC 17D will primarily serve in 17D assignments. Furthermore, Cyber Officers receiving assignments for Cyber Branch AOCs in which they are not yet qualified must attend the designated transition course/training pipeline to earn the AOC applicable for the duty position.

(1) Cyber Warfare Officer (17A). Duties include leading, directing, managing, planning, integrating, synchronizing, and/or executing CO at all Army and JIM echelons. The 17A is well-versed in tactics, techniques, and procedures for maneuvering in and through the cyberspace domain to deliver cyberspace actions, including: cyberspace defense; cyberspace intelligence, surveillance, and reconnaissance; cyberspace operational preparation of the environment; cyberspace attack; and cyberspace security. Cyber Warfare Officers utilize personnel, resources, and capabilities to engage and create effects against adversaries in and through cyberspace in order to preserve the ability to use friendly cyberspace capabilities; protect data, networks, net-centric capabilities, and other designated systems; and project power by the application of force in or through cyberspace. Cyber Warfare Officers deliver effects in and through cyberspace that manifest in cyberspace, or in one or more of the other domains, that are designed to deny, degrade, disrupt, destroy, or manipulate adversary activities or operations. The 17A plans, integrates, and synchronizes CO with other lethal and nonlethal actions to enable commanders to mass effects and gain advantages in the cyberspace domain, EMS battlespace, and across other domains during MDO in support of ULO. Cyber Warfare Officers command, lead, direct, and manage CMF teams and associated cyber units and organizations. The 17A also understands friendly and adversary cyberspace capabilities, objectives, organizations, and operations, as well as, the broader aspects of MDO and ULO.

(2) Cyber Electromagnetic Warfare Officer (17B). Duties include leading, directing, managing, planning, integrating, synchronizing, and/or executing CO and EW at all Army and JIM echelons. The 17B is well-versed in tactics, techniques, and procedures for performing CO and EW missions, including electromagnetic attack, electromagnetic protection, and electromagnetic support. CEWOs utilize personnel, resources, and capabilities to engage adversaries in and through the cyberspace domain and the EMS battlespace to affect or attack personnel, facilities, networks, or equipment; protect friendly personnel, facilities, networks, and equipment from cyberspace or electromagnetic attack, as well as, friendly or adversary use of the EMS that could impact friendly combat capabilities; and detect, intercept, identify, and locate or localize adversary electromagnetic vulnerabilities to enable future operations. Furthermore, the 17B plans, integrates, and synchronizes CO and EW with actions to enable commanders to mass effects and gain advantages in the cyberspace domain, EMS battlespace, and across other domains during MDO in support of ULO. CEWOs command, lead, direct, and manage Cyber and EW units and elements. The 17B also understands friendly and adversary cyberspace and EMS capabilities, objectives, organizations, and operations, as well as, the broader aspects of MDO and ULO.

(3) Cyber Capabilities Development Officer (17D). Duties include leading, directing, managing, planning, integrating, synchronizing, and/or executing capabilities development to support CO and EW missions, to include designing, developing, and delivering relevant, timely, and effective software, hardware, and other relevant solutions. The CCDO serves as a developer within a development element or associated organization at any echelons. The CCDO utilizes personnel, resources, and methods to enable and enhance CO and EW missions. The 17D also understands friendly and adversary cyberspace and EMS capabilities, objectives, organizations, and/or operations, as well as, the broader aspects of MDO and ULO in order to perform robust capabilities development efforts.

b. Lieutenant development. The professional development objective for this phase of an officer's career is to develop and utilize requisite Cyber Branch knowledge, skills, and behaviors. The focus for the Cyber lieutenant is primarily leading, planning, or executing CO or EW missions through the application of their technical and tactical acumen. Select lieutenants will focus on CO and EW capabilities developer roles.

(1) Education. After commissioning, Cyber lieutenants will attend Cyber Basic Officer Leader Course

(CyBOLC) for AOC 17A. Select lieutenants will attend the AOC 17B CEWO Qualification Course, following successful completion of 17A CyBOLC. Other select lieutenants will attend AOC 17D BOLC instead of AOC 17A CyBOLC. Cyber Officers directly appointed in the rank of lieutenant through the Cyber Direct Commissioning Program (CDCP) are required to attend the Army's Direct Commission Course, followed by the Cyber Direct Commission Officer Course, unless granted an exception to policy/waiver by the appropriate Army authority.

(2) PME course credit. Cyber Officers can apply for PME course credit based on previous leadership experience and past academic or training experience, per AR 350-1. The approval authority for course credit for the PME portion of BOLC (i.e. common core) is the Director of Training, TRADOC G-37, delegated from HQDA DCS G-3/5/7.

(3) Cyber Course Credit Program. Cyber Officers who acquire relevant CO or EW knowledge, skills, and behaviors through military courses or experience and/or civilian industry, education, or training may apply for course credit for portions of AOC qualification courses governed by the U.S. Army Cyber School. The Cyber Course Credit Program is managed by the U.S. Army Cyber School IAW AR 350-1 for the evaluation and awarding of constructive, equivalent, and operational credit. The approval authority for awarding 17A, 17B, and 17D AOC qualification course credit (not including PME credit) is the Commandant, U.S. Army Cyber School. Cyber course credit, if approved, will be documented in a memorandum signed by the Commandant, U.S. Army Cyber School, or authorized delegate. The approval memorandum serves as verification of course credit toward 17A, 17B, or 17D AOC qualification in lieu of DA Form 1059.

(4) Assignments. After BOLC (and the 17B CEWO Qualification Course, if applicable), Cyber lieutenants should expect to be assigned to CO or EW positions for at least 18 months in order to gain leadership experience and technical competence. Ideally, most lieutenants will serve on CO teams to hone their leadership and technical skills for development as future Cyber team leaders and company commanders. Select lieutenants will serve as EW Platoon Leaders or in CEMA sections, while other select lieutenants will serve as Cyber capabilities developers within development teams, crews, sections, sites, and/or units.

(a) Cyber lieutenants, upon completion of BOLC and requisite functional training, should be assigned to CO or EW positions, primarily within a Cyber Protection Team (CPT); National Mission Team (NMT); National Support Team (NST); Combat Mission Team (CMT); Combat Support Team (CST); Expeditionary Cyber Team (ECT); EW Platoon; CEMA Section; or Developer team/crew/section/site/unit. Cyber lieutenants may also develop expertise in technologies and technical skillsets used within the cyberspace domain and EMS battlespace through highly specialized training designed and/or designated by the U.S. Army Cyber Center of Excellence, U.S. Army Cyber Command, and/or U.S. Cyber Command.

(b) The goal of the branch is to assign lieutenants to the operational force as an initial assignment. Developmental assignments include but are not limited to:

Table 1: Developmental Positions for Lieutenants		
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Company XO Platoon Leader Assistant S3 Section Leader Cyber Planner Analytic Support Officer Battle Captain Aide de Camp Interactive Operator (CMF) Exploitation Analyst (CMF)	Company XO Platoon Leader Brigade/Regiment CEWO Cyber/EW Planner	Company XO Platoon Leader Developer

(5) Self-development. Lieutenants should focus on tactical and technical CO and EW fundamentals; CMF works role certifications; cyber-related industry certifications; leadership skills; logistics and basic administrative activities; fundamentals of training management; and other tactical and technical proficiency skills.

(6) Desired experience. Cyber lieutenants will serve in an operational Cyber unit and focus on developing small team or unit level leadership skills, as well as, understanding the essential elements of CO. Select lieutenants will serve as EW Platoon Leaders or in CEMA section positions while developing a firm understanding of the cyberspace domain and EMS battlespace. Lieutenants should continue to build their knowledge, skills, and behaviors in conducting various types of CO and EW missions.

c. Captain development. The professional development objective for a captain is to expand their expertise and lead small team/unit level cyberspace and EW operations. The primary focus of the Cyber captain is the development of tactical and technical leadership and management skills to conduct and synchronize cyberspace and EW operations in Army and JIM environments.

(1) Education.

(a) Cyber captains will attend the Cyber Captains Career Course (CCC) (for 17As and 17Bs) or the 17D CCC (for 17Ds). It is desirable for Cyber Officers to attend their designated Cyber CCC as soon as possible after promotion to captain, or after completing four years but prior to the seventh year of Active Federal Commissioned Service (AFCS).

(b) Cyber Officers directly appointed in the rank of captain through the CDCP are required to attend the Army's Direct Commission Course, followed by the Cyber Direct Commission Officer Course, unless granted an exception to policy/waiver by the appropriate Army authority. Cyber Officers directly appointed in the rank of captain through the CDCP are required to attend their designated Cyber CCC if receiving less than seven years of total constructive service credit at the time of appointment. Cyber Officers directly appointed in the rank of captain with seven or more years of credit are exempt from the CCC attendance requirement in order to optimize initial mission-focused assignments and individual promotion opportunities/timelines.

(c) Select Cyber captains may develop mastery of technologies and technical skillsets used within the cyberspace domain or EMS battlespace through highly-specialized training designed and/or designated by the U.S. Army Cyber Center of Excellence, U.S. Army Cyber Command, and/or U.S. Cyber Command.

(d) Cyber captains directed to fill AOC 17B assignments must complete the 17B CEWO Qualification Course (if not already 17B AOC-qualified) prior to reporting for their 17B assignment. When feasible, the 17B CEWO Qualification Course should be completed consecutively with the Cyber CCC.

(e) Company grade VTIP officers transitioning into the Cyber Branch must attend the Cyber Operations Officer Course (CyOOC) for AOC 17A or the designated transition course/training pipeline for AOC 17D, depending on which AOC for which they are selected. If designated for AOC 17B, VTIP officers must complete CyOOC for AOC 17A, followed by the 17B CEWO Qualification Course. For VTIP company grade officers who have not completed CCC for any branch prior to transfer, they will need to complete Cyber Branch CCC for either 17A or 17D, depending on their designated Cyber Branch AOC.

(2) PME course credit. Cyber Officers can apply for PME course credit based on previous leadership experience and academic or training experience, per AR 350–1. The approval authority for course credit for the PME portion of CCC is the Director of Training, TRADOC G-37, delegated from HQDA DCS G-3/5/7.

(3) Cyber Course Credit Program. Cyber Officers who acquire CO or EW knowledge, skills, and behaviors through military courses or experience and/or civilian industry, education, or training may apply for course credit for the portions of AOC qualification courses governed by the U.S. Army Cyber School, Fort Gordon, GA. The Cyber Course Credit Program is managed by the U.S. Army Cyber School IAW AR 350-1 for the evaluation of constructive, equivalent, and operational credit. The approval authority for awarding 17A, 17B, or 17D AOC qualification course credit (not including PME credit) is the Commandant, U.S. Army Cyber School. Cyber course credit, if approved, will be documented in a memorandum signed by the Commandant, U.S. Army Cyber School, or authorized delegate. The approval memorandum serves as verification of course credit toward 17A, 17B, or 17D AOC qualification in lieu of DA Form 1059.

(4) Assignments. Cyber captains will normally be assigned to key developmental positions prior to broadening assignments.

(a) Key developmental assignments. Key developmental positions provide a Cyber captain with the desired operational experience in small unit leadership, CO, and EW at this developmental phase. Key developmental assignments also provide credible experience in the core skillsets required of commanders, leaders, and staff officers. Cyber captains must serve in key developmental positions for a minimum of 18 months (optimally 24 months). Successful service in captain key developmental positions for any 17-series AOC counts as key developmental credit for all 17-series Cyber captains. Additionally, Cyber captains serving in key developmental positions for majors will receive key developmental credit in their current rank/grade. Success in the assignments listed below (or combination of assignments) will provide opportunities for career development and future consideration for promotion to the rank of major (which will be primarily based on performance in one or more of the following positions):

Table 2: Key Developmental Positions for Captains		
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Company Commander Support Team Leader (CST) Mission Element Leader (CPT) Section Leader (NMT/CMT) Cyber Warfare/Ops Officer (Division CEMA Section only)	Company Commander Brigade/Regiment/SFG CEWO	Company Commander Development Crew Leader Senior Developer

(b) Developmental assignments for Cyber captains are designed to allow commanders wide latitude in tailoring the type, number, and order of assignments based on the developmental needs of the officer, the operational needs of the unit, the availability of developmental positions within the command, and the overall needs of the Army. Developmental assignments include but are not limited to:

Table 3: Developmental Positions for Captains		
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Career Program Mgr. (OCC) (post-KD) Cyber OC/T (CTCs) (post-KD) CY Research Scientist (ACI) (post-KD) Instructor (CyS/USMA) (post-KD) Analytic Support Officer Assistant S3 (BN/BDE) Battalion S2/S3 (CTB) AROC Officer Battle Captain (JOC) Mission Manager (JOC) Watch Officer (JOC) Branch Chief (OCO/DCO/DODIN) Cyber Planner Special Technical Ops (STO) Planner Deputy Team Leader (ECT) Effects Assessment Officer Evaluation Concepts Officer Remote Operations OIC Task Force (TF) CuOps Officer (CMF) Training/Exercises Officer	Cyber/EW OC/T (CTCs) (post-KD) CY/EW Rsrch. Scientist (post-KD) Instructor (CyS/USMA) (post-KD) Assistant S3 (BN/BDE) Battalion S2/S3 (CTB) Cyber/EW Planner Division/Corps CEWO MDTF Company XO	Career Program Mgr. (post-KD) CY Research Scientist (post-KD) Instructor (CyS/USMA) (post-KD) Assistant S3 (BN/BDE) Battalion S2/S3 (CTB) Product Engineer (915th CWB) Systems Development Chief

(c) Broadening assignments. Opportunities available for captains include, but are not limited to:

1. Advanced Civil Schooling.
2. Training with Industry.
3. DoD or interagency fellowships/internships.

(d) Self-development. Cyber captains should continue to gain an increased understanding of cyberspace and EW operations, as well as, MDO and ULO. Captains should also continue to gain an in-depth understanding of MDMP and the foundational knowledge required to effectively serve as a staff officer at the battalion, brigade, or division level. Military-orientated training for all designated Cyber Officers includes but is not limited to: Joint EW Theater Operations Course, Special Technical Operations Planners Course, Joint Network Attack Course, Electromagnetic Spectrum Operations Course, Space Fundamentals Course, Air Force Institute of Technology Cyber 200 and 300, Joint Operational Fires and Effects Course, Joint Targeting Course, Joint Firepower Course, Joint Information Operations Planners Course, Military Deception Planners Course, and NATO EW Course. Captains should pursue graduate-level education in a science, technology, engineering, or math (STEM) related discipline and/or obtain industry certifications related to information technology, networking, CO, cybersecurity, and other relevant disciplines.

(e) Desired experience. Cyber captains should possess in-depth knowledge and skills in leading cyberspace and EW operations at all echelons. Captains should serve in at least one key developmental assignment for a minimum of 18 months (optimally 24 months) in order to gain the necessary leadership and mission-related skills and experience. It is also important for Cyber captains to serve in developmental and broadening assignments to gain a wider range of knowledge and skills to enhance their understanding of the range of military operations, as well as, expand their awareness of JIM environments.

d. Major development. The professional development objectives for a major are to further expand and broaden the officer's tactical and technical experience and expertise in cyberspace and EW operations at all echelons. Cyber majors should focus on developing organizational leadership, management, and planning skills through a series of operating and generating force developmental assignments.

(1) Education.

(a) Military education required during this phase is the completion of Intermediate Level Education (ILE) at the U.S. Army Command and General Staff College (CGSC). The Army conducts ILE selection boards in conjunction with the Major ACC Promotion Selection Board to consider officers for resident or non-resident ILE opportunities. In addition to Army's CGSC, Command and Staff College (CSC)/ ILE attendance opportunities may include one of the following schools: the U.S. College of Naval Command and Staff, the U.S. Air Command and Staff College, the U.S. Marine Corps Command and Staff College, the Western Hemisphere Institute for Security Cooperation Command and General Staff Officer Course, or foreign military staff colleges which have been granted MEL 4 equivalency by the DCS, G-3. Officers may also compete to be selected for the School of Advanced Military Studies (SAMS) following the Army Operations Course.

(b) Cyber Officers directly appointed in the rank of major through the CDCP are required to attend the Army's Direct Commission Course, followed by the Cyber Direct Commission Officer Course, unless granted an exception to policy/waiver by the appropriate Army authority. Cyber Officers directly appointed in the rank of major are required to attend their designated CGSC/ILE course if receiving less than 14 years of total constructive service credit at the time of appointment. Cyber Officers directly appointed as majors with 14 or more years of credit are exempt from the CGSC/ILE attendance requirement in order to optimize initial mission-focused assignments and individual promotion opportunities/timelines. All Cyber Officers directly appointed as majors are exempt from captain PME requirements.

(c) Select Cyber majors may develop mastery of technologies and technical skillsets used within the cyberspace domain or EMS battlespace through highly-specialized training designed and/or designated by the Cyber Center of Excellence, U.S. Army Cyber Command, and/or U.S. Cyber Command.

(d) Cyber majors directed to fill AOC 17B assignments must complete the 17B CEWO Qualification Course (if not already 17B AOC-qualified) prior to reporting for their 17B assignment.

(e) VTIP majors transitioning into the Cyber Branch must attend the Cyber Operations Officer Course (CyOOC) for AOC 17A or the designed transition course/training pipeline for AOC 17D, depending on which AOC for which they are selected. If designated for 17B, VTIP officers must complete CyOOC for 17A, followed by the 17B CEWO Qualification Course.

(2) PME course credit. Cyber Officers can apply for PME course credit based on previous leadership experience and past academic or training experience, per AR 350–1 The approval authority for course credit for ILE is the Director of Training, TRADOC G-37, delegated from HQDA DCS G-3/5/7; however, due to the opportunities available for officers to attend resident, satellite, or non-resident ILE, approval of course credit is restrictive.

(3) Cyber Course Credit Program. Cyber Officers who acquire CO or EW knowledge, skills, and behaviors through military courses or experience and/or civilian industry, education, or training may apply for course credit for the portions of AOC qualification courses governed by the U.S. Army Cyber School, Fort Gordon, GA. The Cyber Course Credit Program is managed by the U.S. Army Cyber School IAW AR 350-1 for the evaluation of constructive, equivalent, and operational credit. The approval authority for awarding 17A, 17B, or 17D AOC qualification course credit (not including PME credit) is the Commandant, U.S. Army Cyber School. Cyber course credit, if approved, will be documented in a memorandum signed by the Commandant, U.S. Army Cyber School, or authorized delegate. The approval memorandum serves as verification of course credit toward 17A, 17B, or 17D AOC qualification in lieu of DA Form 1059.

(4) Assignments. Majors will normally be assigned to key developmental positions before broadening assignments.

(a) Key developmental assignments. Cyber majors should gain advanced experience and expertise in leading, managing, and planning cyberspace and EW operations at higher-level echelons through key developmental assignments. These assignments provide a credible developmental experience in the core skillsets required of future battalion commanders, as well as, Army and JIM officers. Cyber majors must serve in key developmental positions for a minimum of 18 months (optimally 24 months). Successful service in major key developmental positions for any 17-series AOC counts as key developmental credit for all 17-series Cyber majors. Additionally, majors serving in key developmental positions for lieutenant colonels will receive key developmental credit in their current rank/grade. Success in the assignments listed below (or combination of assignments) will provide opportunities for career development and future consideration for promotion to the rank of lieutenant colonel (which will be primarily based on performance in one or more of the following positions):

Table 4: Key Developmental Positions for Majors

17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Battalion XO Battalion S3 TF Commander (CMF/CNMF) Mission Team Leader (CMT/CPT/ECT) Support Team Leader (NST) Senior OC/T (CTCs)	Battalion XO Battalion S3 Company Commander (MDTF) Brigade/Regiment/SFG CEWO Senior OC/T (CTCs)	Battalion XO Battalion S3 Development Section Leader Development Team Leader (915th) Master Developer

(b) Developmental assignments for Cyber majors are designed to allow commanders wide latitude in tailoring the type, number, and order of assignments based on the developmental needs of the officer, the operational needs of the unit, the availability of developmental duty positions within the command, and the overall needs of the Army. Developmental assignments include, but are not limited to:

Table 5: Developmental Positions for Majors

17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Assignments Officer (HRC) (post-KD) Career Program Manager (post-KD) College Director (CyS) (post-KD) CY Research Scientist (ACI) (post-KD) Instructor (CyS/USMA/CAC) (post-KD) AROC Officer Battle Watch Chief (JOC) Senior Fires Officer (JOC) Joint Plans Analyst (JOC) Watch Officer (JOC) BDE Assistant S3 Course Manager (Cyber School) Cyber Branch Chief Cyber Integration Lead (JFHQ-CY) Cyber Mission Manager Cyber OC/T (CTCs) Cyber Operations Chief (JFHQ-CY) Cyber Planner Strategy/Policy Planner (SOCOM) TF Deputy Commander (CMF/CNMF) Training/Exercises/Plans Officer	Assignments Officer (post-KD) Career Program Manager (post-KD) College Director (CyS) (post-KD) CY/EW Rsrch. Scientist (post-KD) Instructor (post-KD) BDE Assistant S3 Course Manager (Cyber School) Cyber/EW OC/T (CTCs) Cyber/EW Planner Cyber/EW Integrator (CCoE) Cyber/EW Branch Chief Division/Corps/EAC CEWO	Assignments Officer (post-KD) Career Program Mgr. (post-KD) College Director (post-KD) Cyber Rsrch. Scientist (post-KD) Instructor (post-KD) BDE Assistant S3 Chief, Capabilities Integr. (IWOC) Course Manager (Cyber School) Cyber Branch Chief Cyber OC/T (CTCs)

(c) Broadening assignments. Opportunities available for majors include, but are not limited to:

1. Advanced Civil Schooling.
2. Training with Industry.
3. DoD and interagency fellowships/internships.

(d) Self-development. Cyber majors should continue efforts to become an expert in all aspects of cyberspace and EW operations and to acquire expertise in organizational leadership techniques. Majors must work to expand their knowledge and skills in order to serve effectively at the team, battalion, brigade, Army, and JIM levels.

(e) Desired experience. Cyber majors should possess expertise in leading cyberspace and EW operations at all echelons. Majors should serve in at least one key developmental assignment for a minimum of 18 months (optimally 24 months) in order to gain the necessary leadership and mission-related skills and experience. When feasible, broadening assignments will provide majors with a wider range of knowledge and skill.

e. Lieutenant colonel development. The professional development objective for a lieutenant colonel is to develop and demonstrate excellence in tactical and technical knowledge and skills. Cyber lieutenant colonels learn to effectively lead, train, motivate, and care for Soldiers while in command and staff environments.

(1) Education.

(a) Senior Cyber lieutenant colonels may be selected for Senior Service College (SSC). SSC attendance opportunities may include one of the following schools: U.S. Army War College (USAWC); National Defense University; Naval War College; Air War College; Marine Corps War College; Joint Advanced Warfighting School; USAWC Fellows Program; or foreign military schools granted MEL 1 equivalency. Lieutenant colonels not CSL-selected for resident education should enroll in distance learning education. Those selected to command will also attend a pre-command course, and those selected for Joint assignments must complete JPME II training. Other senior leader and executive courses will be considered to enhance leadership within cyberspace and EW operational units and CEMA-focused elements.

(b) Cyber Officers directly appointed in the rank of lieutenant colonel through the CDCP are required to attend the Army's Direct Commission Course, followed by the Cyber Direct Commission Officer Course, unless granted an exception to policy/waiver by the appropriate Army authority. Cyber Officer directly appointed in the rank of lieutenant colonel are exempt from all other PME requirements for previous ranks/grades.

(2) Assignments.

(a) Key developmental assignments. Cyber lieutenant colonels should gain mastery of leading cyberspace and EW operations, as well as, command and staff functions at all echelons through key developmental assignments. Cyber lieutenant colonels must serve in one or more key developmental positions for a minimum of 18 months (optimally 24 months). Successful service in lieutenant colonel key developmental positions for any 17-series AOC counts as key developmental credit for all 17-series Cyber lieutenant colonels. Additionally, lieutenant colonels serving in key developmental positions for colonels will receive key developmental credit in their current rank/grade. Success in the assignments listed below (or combination of assignments) will provide opportunities for career development and future consideration for promotion to the rank of lieutenant colonel (which will be primarily based on performance in one or more of the following positions):

Table 6: Key Developmental Positions for Lieutenant Colonels

17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Battalion Commander (CSL) Task Force Commander (CMF/CNMF) Mission Team Leader (NMT/CPT) Division CEWO	Battalion Commander (CSL) Division CEWO	Battalion Commander (CSL) Development Site Leader Master Developer

(b) Developmental assignments for Cyber lieutenant colonels are designed to allow commanders wide latitude in tailoring the type, number, and order of assignments based on the developmental needs of the officer, the operational needs of the unit, the availability of developmental duty positions within the command, and the overall needs of the Army. Developmental assignments include, but are not limited to:

Table 7: Developmental Positions for Lieutenant Colonels

17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
BDE Deputy Commander (post-CSL) ACM Capability Developer (CCoE) Assistant ACM Cyber/EW (CCoE) Battle Captain (JFHQ-CY) BDE S3 Chief, CTOC (ARCYBER) Chief, ITOC (JFHQ-CY) Chief, Doctrine Branch (CCoE) Chief, Information Dominance (HRC) Chief Research Scientist (ACI) Cyber Branch/Division Chief Cyber Warfare Officer (ECB) Deputy Director (OCC) Instructor (CAC/USMA/USN) Joint Cyberspace Analyst (JCS) Mission Director (USCYBERCOM) Senior/Lead Cyber Planner Senior Capabilities Analyst (IWOC) Senior Cyber OC/T (CTCs) Senior Watch Officer (IWOC) Technical Director (USCYBERCOM) Training Integrator (CCoE)	BDE Deputy Command (post-CSL) Assistant ACM Cyber/EW (CCoE) BDE S3 CEMA Ops/Training (FORSCOM) Chief, Capabilities Dev. (CCoE) Chief, Info Dominance (HRC) Chief Research Scientist (ACI) Corps/ASCC/CCMD CEWO Deputy Director (OCC) Lead Army Analysis/Ops (JEWC) Instructor (CAC/USMA/USN) J3 Branch Chief (DISA) Senior OC/T (CTCs) Senior Training Analyst (W1YYAA) Training Integrator (CCoE)	BDE Dep. Commander (post-CSL) Assistant ACM Cyber/EW BDE S3 Chief, Info Dominance (HRC) Chief, Doctrine Branch (CCoE) Chief Cyber Research (ACI) Cyber Branch/Division Chief Deputy Director (OCC) Instructor (CAC/USMA/USN) Mission Director (USCYBERCOM) Tech Director (USCYBERCOM)

(c) Broadening assignments include:

1. PhD program (e.g., Naval Postgraduate School (NPS) or Air Force Institute of Technology (AFIT)).
2. Training with Industry.
3. DoD and interagency fellowships.
4. ROTC Professor of Military Science.
5. ACOM/HQDA/CCMD/JIM/DCS/SGS assignments.

(3) Self-development. Lieutenant colonels not selected for resident SSC should enroll in nonresident SSC education. Other self-development includes doctoral-level STEM programs at NPS, AFIT, or other relevant institutions. Lieutenant colonels should also continue developing mastery of cyberspace and EW operations at all echelons through mentorship, self-study, education, training course, certifications, etc.

(4) Desired experience. Cyber lieutenant colonels should possess increased expertise in leading cyberspace and EW operations at all echelons. Lieutenant colonels should serve in at least one key developmental assignment for a minimum of 18 months (optimally 24 months) in order to gain the necessary leadership and mission-related skills and experience. When feasible, broadening assignments will provide majors with a wider range of knowledge and skills.

f. Colonel development. The professional development objective for a colonel is the sustainment of warfighting, training, and staff skills, along with the utilization of leadership, organizational, and executive talents. Cyber colonels are expected to be strategic, creative, and critical thinkers; builders of leaders and teams; competent warfighters in the range of military operations; skilled in governance, statesmanship, and diplomacy; and fluent in cultural context. They influence policy within the Army and the Department of Defense.

(1) Education.

(a) The majority of officers selected for promotion to colonel will have already attended or will be selected to attend SSC. Colonels not CSL-selected for resident education should enroll in distant learning education. Those selected to command will also attend a pre-command course. Cyber colonels serving as an Army Capabilities Manager (ACM) may attend the Combat Developers Course. Other Army or Joint senior leader and executive course should be considered to enhance leadership of CO, EW, or CEMA units/elements.

(b) Cyber Officers directly appointed in the rank of colonel through the CDCP are required to attend the Army's Direct Commission Course, followed by the Cyber Direct Commission Officer Course, unless granted an exception to policy/waiver by the appropriate Army authority. Cyber Officer directly appointed in the rank of colonel is exempt from all other PME requirements for previous ranks/grades.

(2) Assignments. Cyber colonels contribute to the Army by serving in crucial assignments in Cyber and EW focused operational units and Army or JIM environments. It is critical during this phase to develop the broad skills and competencies required of an agile and adaptive leader while maintaining branch competency.

(a) Key developmental assignments. Command selection is more limited for the Cyber colonel population. Therefore, Cyber Branch offers other senior key leadership opportunities that include increased responsibilities for commanding, leading, and managing CO and EW organizations and capabilities at the Army and JIM levels. Cyber colonels must serve in key developmental positions for a minimum of 18 months (optimally 24 months). Successful service in colonel key developmental positions for any 17-series AOC counts as key developmental credit for all 17-series Cyber colonels. Success in the assignments listed below (or combination of assignments) will provide opportunities for career development and future consideration for promotion (which will be primarily based on performance in one or more of the following positions):

Table 8: Key Developmental Positions for Colonels

17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Brigade Commander (CSL) ACM Cyber/EW (CSL) Corps CEWO (CSL)	Brigade Commander (CSL) Corps CEWO (CSL) ACM Cyber/EW (CSL)	Brigade Commander (CSL) ACM Cyber/EW (CSL) BDE Cap. Development Leader Master Developer

(b) Developmental assignments for Cyber colonels are designed to allow commanders wide latitude in tailoring the type, number, and order of assignments based on the developmental needs of the officer, the operational needs of the unit, the availability of developmental duty positions within the command, and the overall needs of the Army. Developmental assignments include, but are not limited to:

Table 9: Developmental Positions for Colonels

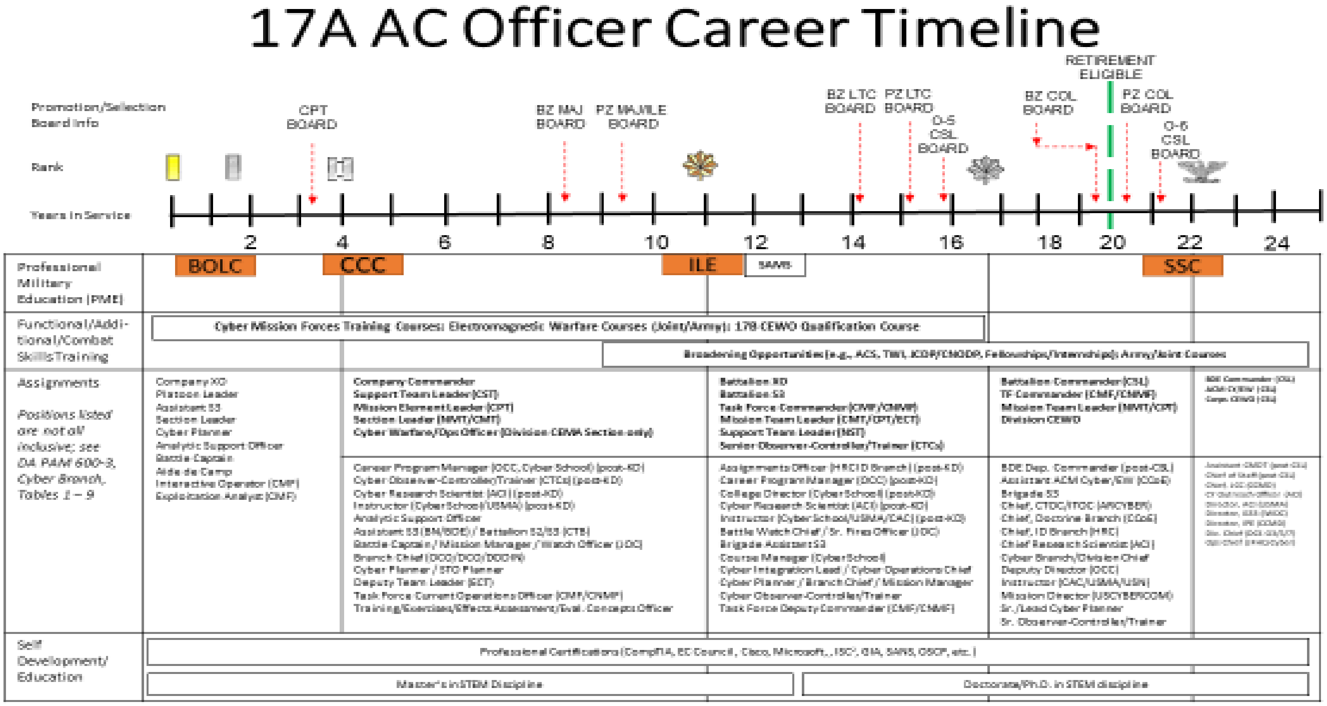
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Asst. Commandant (CyS) (post-CSL) Chief of Staff (post-CSL) Chief, Joint Cyber Center (CCMD) Cyber Outreach Officer (ACI) Director, Army Cyber Institute Director, G33 (IWOC) Director, IPE (CCMD) Division Chief (DCS G3/5/7) Operations Chief (JFHQ-CY)	Asst. CMDT (CyS) (post-CSL) Chief of Staff (post-CSL) ASCC/CCMD CEWO CEMA Division Chief Cyber Outreach Officer (ACI) Director, Army Cyber Institute Division Chief (DCS G3/5/7) Operations Chief (JFHQ-CY)	Asst. CMDT (CyS) (post-CSL) Chief of Staff (post-CSL) Cyber Outreach Officer (ACI) Director, ACI Division Chief (DCS G3/5/7) Operations Chief (JFHQ-CY)

(c) Broadening assignments. Opportunities available for colonels include, but are not limited to:

1. Branch immaterial positions (recruiting command staff and AC/RC positions).
2. DoD and interagency fellowships.
3. ACOM/HQDA/CCMD/JIM/DCS/SGS assignments.
4. Nominative assignments.

(3) Self-development. Cyber colonels must maintain their branch skills and keep current on all changes that affect the Soldiers they command, lead, and/or manage. Seeking post-CSL developmental or broadening assignments is important during this phase.

(4) Desired experience. The well-experienced Cyber colonel will have a variety of duty assignments as operational and strategic Cyber leaders and subject matter experts in both operating and generating force organizations, Army Staff, and JIM organizations. The Cyber colonel’s knowledge and experience will provide a significant contribution to the Army and the DoD. Colonels should serve in at least one key developmental assignment for a minimum of 18 months (optimally 24 months) in order to hone requisite knowledge and experience.


17A AC Officer Career Timeline
Promotion/Selection Board Info
CPT BOARD
BZ MAJ BOARD
PZ MAJ/ILE BOARD
BZ LTC BOARD
PZ LTC BOARD
O-5 CSL BOARD
RETIREMENT ELIGIBLE
BZ COL BOARD
PZ COL BOARD
O-6 CSL BOARD
Rank
Years in Service
2
4
6
8
10
12
14
16
18
20
22
24
Professional Military Education (PME)
BOLC
CCC
ILE
SAMS
SSC
Functional/Additional/Combat Skills Training
Cyber Mission Forces Training Courses; Electromagnetic Warfare Courses (Joint/Army); 17B CEWO Qualification Course
Broadening Opportunities (e.g., ACS, TWI, JCDP/CNODP, Fellowships/Internships); Army/Joint Courses
Assignments
Positions listed are not all inclusive; see DA PAM 600-3, Cyber Branch, Tables 1 – 9
Self Development/ Education
Professional Certifications (CompTIA, EC Council, Cisco, Microsoft, , ISC², GIA, SANS, OSCP, etc.)
Master's in STEM Discipline
Doctorate/Ph.D. in STEM discipline

Company XO
Platoon Leader
Assistant S3
Section Leader
Cyber Planner
Analytic Support Officer
Battle Captain
Aide de Camp
Interactive Operator (CMF)
Exploitation Analyst (CMF)

Company Commander
Support Team Leader (CST)
Mission Element Leader (CPT)
Section Leader (NMT/CMT)
Cyber Warfare/Ops Officer (Division CEMA Section only)

Career Program Manager (OCC, Cyber School) (post-KD)
Cyber Observer-Controller/Trainer (CTCs) (post-KD)
Cyber Research Scientist (ACI) (post-KD)
Instructor (Cyber School/USMA) (post-KD)
Analytic Support Officer
Assistant S3 (BN/BDE) / Battalion S2/S3 (CTB)
Battle Captain / Mission Manager / Watch Officer (JOC)
Branch Chief (DCO/DCO/DODIN)
Cyber Planner / STO Planner
Deputy Team Leader (ECT)
Task Force Current Operations Officer (CMF/CNMF)
Training/Exercises/Effects Assessment/Eval. Concepts Officer

Battalion XO
Battalion S3
Task Force Commander (CMF/CNMF)
Mission Team Leader (CMT/CPT/ECT)
Support Team Leader (NST)
Senior Observer-Controller/Trainer (CTCs)

Assignments Officer (HRC ID Branch) (post-KD)
Career Program Manager (OCC) (post-KD)
College Director (Cyber School) (post-KD)
Cyber Research Scientist (ACI) (post-KD)
Instructor (Cyber School/USMA/CAC) (post-KD)
Battle Watch Chief / Sr. Fires Officer (JOC)
Brigade Assistant S3
Course Manager (Cyber School)
Cyber Integration Lead / Cyber Operations Chief
Cyber Planner / Branch Chief / Mission Manager
Cyber Observer-Controller/Trainer
Task Force Deputy Commander (CMF/CNMF)

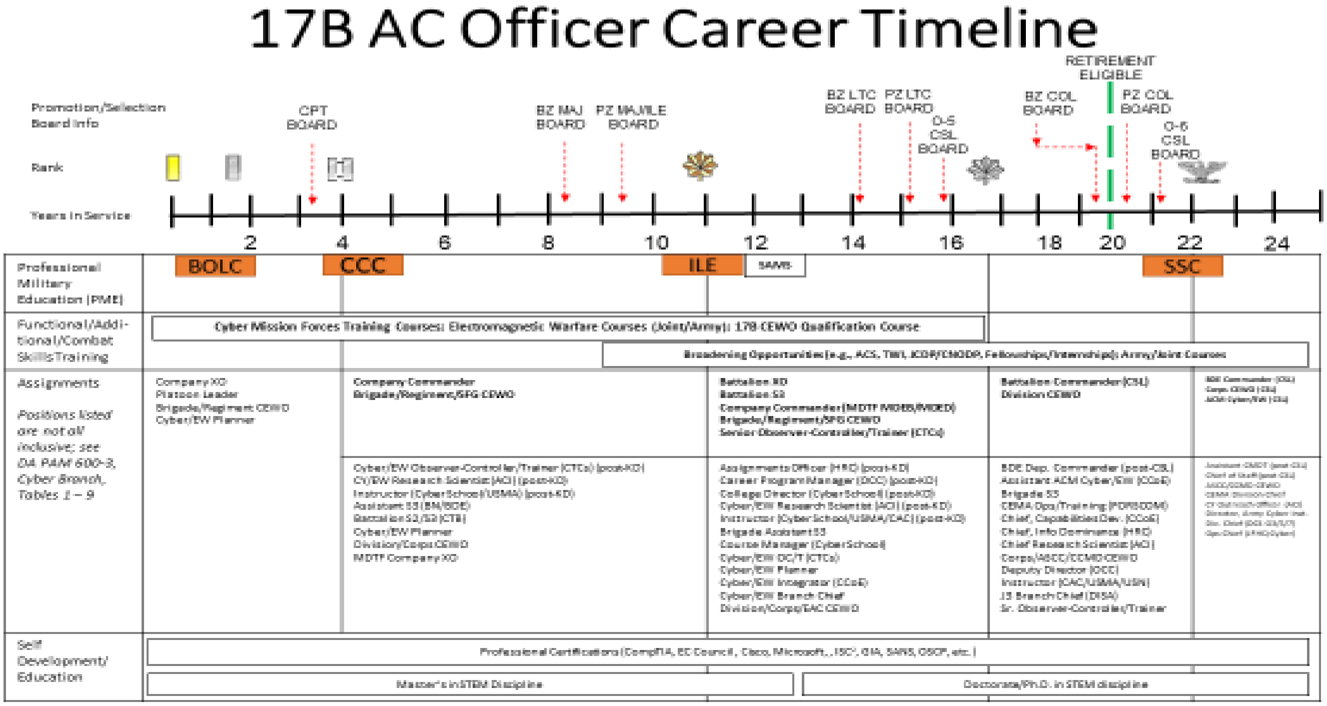
Battalion Commander (CSL)
TF Commander (CMF/CNMF)
Mission Team Leader (NMT/CPT)
Division CEWO

BDE Dep. Commander (post-CSL)
Assistant ACM Cyber/EW (CCoE)
Brigade S3
Chief, CTOC/ITOC (ARCYBER)
Chief, Doctrine Branch (CCoE)
Chief, ID Branch (HRC)
Chief Research Scientist (ACI)
Cyber Branch/Division Chief
Deputy Director (OCC)
Instructor (CAC/USMA/USN)
Mission Director (USCYBERCOM)
Sr./Lead Cyber Planner
Sr. Observer-Controller/Trainer

BDE Commander (CSL)
ACM-CY/EW (CSL)
Corps. CEWO (CSL)

Assistant CMDT (post-CSL)
Chief of Staff (post-CSL)
Chief, JCC (CCMD)
CY Staff/Action Officer (ACI)
Director, ACI (USMA)
Director, SSS (NSOC)
Director, IPE (CCMD)
Div. Chief (DCS-G3/5/7)
Ops Chief (ARCYBER/Cyber)

Figure 1: 17A AC Officer Career Timeline


17B AC Officer Career Timeline
Promotion/Selection Board Info
CPT BOARD
BZ MAJ BOARD
PZ MAJ/ILE BOARD
BZ LTC BOARD
PZ LTC BOARD
O-5 CSL BOARD
RETIREMENT ELIGIBLE
BZ COL BOARD
PZ COL BOARD
O-6 CSL BOARD
Rank
Years in Service
2
4
6
8
10
12
14
16
18
20
22
24
Professional Military Education (PME)
BOLC
CCC
ILE
SAMS
SSC
Functional/Additional/Combat Skills Training
Cyber Mission Forces Training Courses; Electromagnetic Warfare Courses (Joint/Army); 17B CEWO Qualification Course
Broadening Opportunities (e.g., ACS, TWI, JCDP/CNODP, Fellowships/Internships); Army/Joint Courses
Assignments
Positions listed are not all inclusive; see DA PAM 600-3, Cyber Branch, Tables 1 – 9
Self Development/ Education
Professional Certifications (CompTIA, EC Council, Cisco, Microsoft, , ISC², GIA, SANS, OSCP, etc.)
Master's in STEM Discipline
Doctorate/Ph.D. in STEM discipline

Company XO
Platoon Leader
Brigade/Regiment CEWO
Cyber/EW Planner

Company Commander
Brigade/Regiment/SFG CEWO

Cyber/EW Observer-Controller/Trainer (CTCs) (post-KD)
CY/EW Research Scientist (ACI) (post-KD)
Instructor (Cyber School/USMA) (post-KD)
Assistant S3 (BN/BDE)
Battalion S2/S3 (CTB)
Cyber/EW Planner
Division/Corps CEWO
MDTF Company XO

Battalion XO
Battalion S3
Company Commander (MDTF MIDEB/MIDED)
Brigade/Regiment/SFG CEWO
Senior Observer-Controller/Trainer (CTCs)

Assignments Officer (HRC) (post-KD)
Career Program Manager (OCC) (post-KD)
College Director (Cyber School) (post-KD)
Cyber/EW Research Scientist (ACI) (post-KD)
Instructor (Cyber School/USMA/CAC) (post-KD)
Brigade Assistant S3
Course Manager (Cyber School)
Cyber/EW OC/T (CTCs)
Cyber/EW Planner
Cyber/EW Integrator (CCoE)
Cyber/EW Branch Chief
Division/Corps/EAC CEWO

Battalion Commander (CSL)
Division CEWO

BDE Dep. Commander (post-CSL)
Assistant ACM Cyber/EW (CCoE)
Brigade S3
CEMA Ops/Training (FORSCOM)
Chief, Capabilities Dev. (CCoE)
Chief, Info Dominance (HRC)
Chief Research Scientist (ACI)
Corps/ASCC/CCMD CEWO
Deputy Director (OCC)
Instructor (CAC/USMA/USN)
J3 Branch Chief (DISA)
Sr. Observer-Controller/Trainer

BDE Commander (CSL)
Corps. CEWO (CSL)
ACM-Cyber/EW (CSL)

Assistant CMDT (post-CSL)
Chief of Staff (post-CSL)
ASCC/CCMD CEWO
CEMA Division Chief
CY Staff/Action Officer (ACI)
Director, Army Cyber Inst.
Div. Chief (DCS-G3/5/7)
Ops Chief (ARNG Cyber)

Figure 2: 17B AC Officer Career Timeline

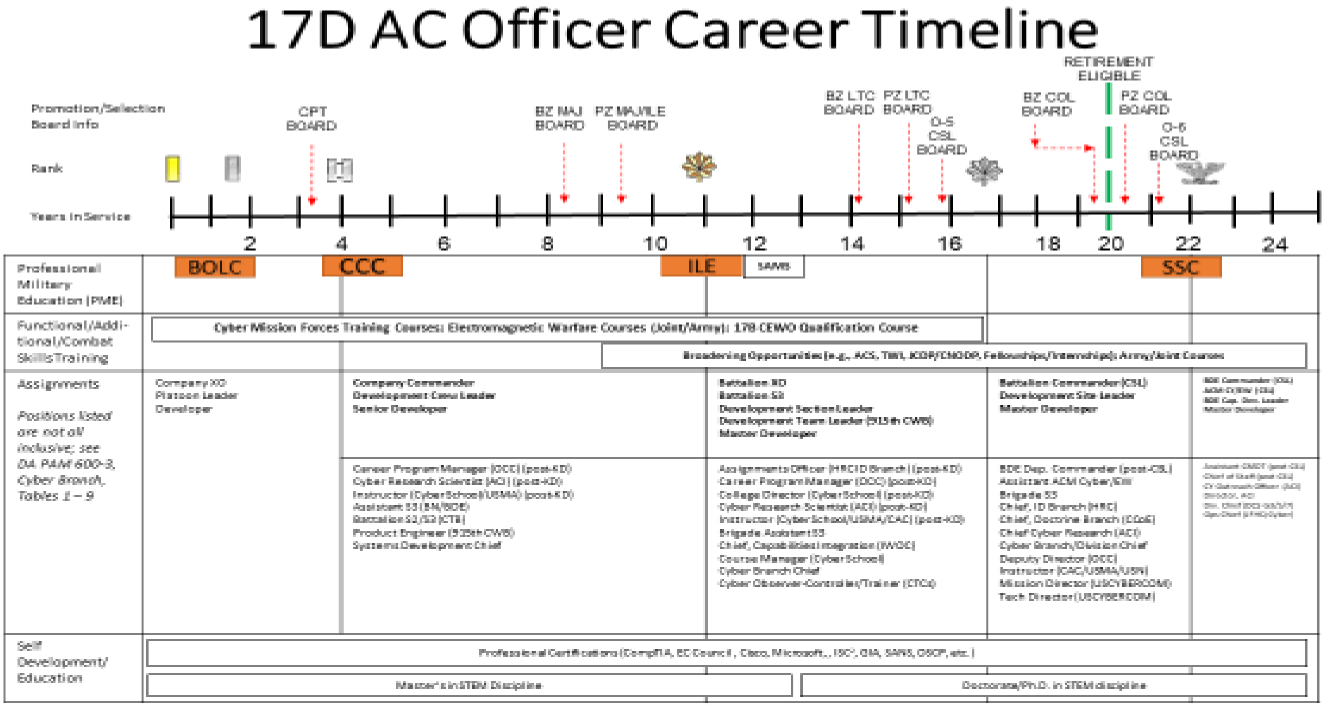

17D AC Officer Career Timeline
Promotion/Selection Board Info
CPT BOARD
BZ MAJ BOARD
PZ MAJ/ILE BOARD
BZ LTC BOARD
PZ LTC BOARD
O-5 CSL BOARD
RETIREMENT ELIGIBLE
BZ COL BOARD
PZ COL BOARD
O-6 CSL BOARD
Rank
Years in Service
2
4
6
8
10
12
14
16
18
20
22
24
Professional Military Education (PME)
BOLC
CCC
ILE
SAMS
SSC
Functional/Additional/Combat Skills Training
Cyber Mission Forces Training Courses; Electromagnetic Warfare Courses (Joint/Army); 17B CEWO Qualification Course
Broadening Opportunities (e.g., ACS, TWI, JCDP/CNODP, Fellowships/Internships); Army/Joint Courses
Assignments
Positions listed are not all inclusive; see DA PAM 600-3, Cyber Branch, Tables 1 – 9
Company XO
Platoon Leader
Developer
Company Commander
Development Cone Leader
Senior Developer
Career Program Manager (OCC) (post-KD)
Cyber Research Scientist (ACI) (post-KD)
Instructor (Cyber School/USMA) (post-KD)
Assistant S3 (BN/BDE)
Battalion S2/S3 (CTB)
Product Engineer (915th CWB)
Systems Development Chief
Battalion XO
Battalion S3
Development Section Leader
Development Team Leader (915th CWB)
Master Developer
Assignments Officer (HRC ID Branch) (post-KD)
Career Program Manager (OCC) (post-KD)
College Director (Cyber School) (post-KD)
Cyber Research Scientist (ACI) (post-KD)
Instructor (Cyber School/USMA/CAC) (post-KD)
Brigade Assistant S3
Chief, Capabilities Integration (IWOC)
Course Manager (Cyber School)
Cyber Branch Chief
Cyber Observer-Controller/Trainer (CTCs)
Battalion Commander (CSL)
Development Site Leader
Master Developer
BDE Dep. Commander (post-CSL)
Assistant ACM Cyber/EW
Brigade S3
Chief, ID Branch (HRC)
Chief, Doctrine Branch (CCoE)
Chief Cyber Research (ACI)
Cyber Branch/Division Chief
Deputy Director (OCC)
Instructor (CAC/USMA/USN)
Mission Director (USCYBERCOM)
Tech Director (USCYBERCOM)
BDE Commander (CSL)
ACM Cyber/EW (CSL)
BDE Cap. Dev. Leader
Master Developer
Assistant CMDT (post-CSL)
Chief of Staff (post-CSL)
CY Outreach Officer (ACI)
Director, ACI
Div. Chief DCS G3/5/7
Ops Chief (ARCYBER)
Self Development/Education
Professional Certifications (CompTIA, EC Council, Cisco, Microsoft, ISC², GIA, SANS, OSCP, etc.)
Master's in STEM Discipline
Doctorate/Ph.D. in STEM discipline

Figure 3: 17D AC Officer Career Timeline

4. Reserve Component (RC) Cyber Officers

a. General career development. U.S. Army National Guard (ARNG) and U.S. Army Reserve (USAR) Cyber Officers serve the same role as their Active Component (AC) counterparts within the confines of approved RC force structures. The unique nature of the RC Cyber Officer's role as a "Citizen Soldier" poses a significant professional development challenge. To fulfill their wartime mission of leading, planning, integrating, synchronizing, and executing cyberspace and EW operations, RC Cyber Officers rely upon extensive interaction between the AC and the RC, as well as, maintaining skills through civilian education, industry organizations, professional certifications, online collaboration tools, and cyber-related industry civilian employment experience. To provide flexibility to RC Cyber Officers, MEL 6 (Captains Career Course) completion for a branch other than Cyber may be authorized by the Office of the Chief of Cyber, on behalf of the Commandant, U.S. Army Cyber School, so long as either Cyber BOLC or CyOOC is completed for AOC 17A qualification.

b. Branch developmental opportunities. RC Cyber Officers should adhere to the same standards and professional development patterns in individual training, operational assignments, and self-development as their AC counterparts. RC officers should build a solid foundation in leadership skills; cyberspace operations (Army and Joint); and EW mission sets to successfully serve in the branch. Due to geographic location, position availability, and other career-related considerations, RC Cyber Officers may not have the opportunity to serve in as many cyberspace and EW operations positions as their AC officer counterparts; however, this issue is offset by the opportunity to serve in positions for a longer period of time depending on the availability of cyber forces positions.

c. Officer development.

(1) Lieutenant. The professional development objective for this phase of an RC Cyber Officer's career is to develop the requisite Cyber Branch skills, knowledge, and behaviors. The focus of the RC Cyber lieutenant is the development of CO skills and the utilization of these skills in an assignment on or in support of a CMF team. Select lieutenants may also develop EW focused skills for utilization in tactical and operational assignments.

(2) Captain. The professional development objective for an RC Cyber captain is to expand their expertise and lead section/team/unit-level CO and EW missions. The primary focus of the RC Cyber captain

is the development of tactical and technical leadership and management skills to conduct and synchronize cyberspace and EW operations in Army-level and JIM environments.

(3) Major. RC Cyber majors must have completed common core ILE to be competitive for promotion to lieutenant colonel. To be best qualified, RC Cyber majors should seek key developmental positions within CMF teams, Cyber Protection Centers, Cyber units, brigades, Special Operations Groups, or other unique positions of a similar level of responsibility. Optimally, RC Cyber majors should spend 24 to 36 months in at least one of these positions.

(4) Lieutenant colonel. To be best qualified, RC Cyber lieutenant colonels should seek key developmental positions within CMF teams, Cyber Protection Centers, Training Support Element teams, the Army Reserve Cyber Protection Brigade (ARCPB), the Cyber Training Support Element (CTSE), Divisions, and/or Army Reserve Intelligence Support to Cyber Operations (ARISCO) positions, as well as, cyber effects support staff officers, battalion commanders, Cyber-specific brigade-level XO/S3 positions, and other principal staff principals. For the ARNG, lieutenant colonels should seek duty with the 91st Cyber Brigade, Infantry Divisions, or Information Operations Support Center (IOSC) as an XO or S3. Optimally, lieutenant colonels should spend 24 to 36 months in at least one of these positions. RC lieutenant colonels are selected for SSC by a RC selection board.

(5) Colonel. RC Cyber colonels serve as brigade-level commanders for ARCPB, CTSE, or ARISCO, in a variety of important staff positions to include USARC G-39, and in various Cyber Branch related generalist positions. ARNG colonels will serve as brigade-level commanders for the 91st Cyber Brigade or the Deputy of the IOSC, and in various Cyber Branch related generalist positions at the State or National levels. RC Colonels are selected for SSC by an RC selection board.

(6) Battalion or brigade command. To be ready for battalion or brigade command, RC officers must meet the appropriate educational requirements for the grade and position. Attendance of a pre-command course is also recommended prior to assumption of command.

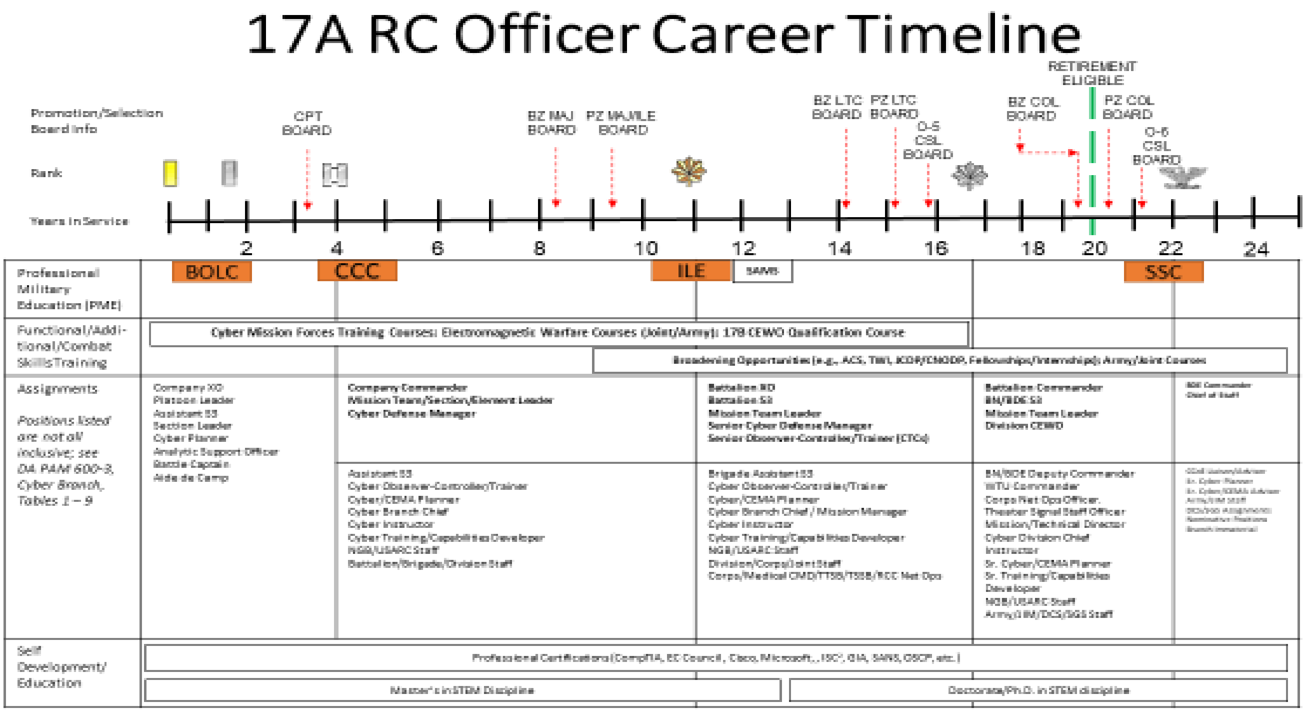
(7) Continuing development. Officers desiring consideration for key positions in RC cyber units should aggressively pursue positions that develop essential warfighting leadership skills. Officers should also seek out self-development opportunities to become an expert in all aspects of cyberspace and EW effects coordination, to include JIM operations. Self-development should include Army or Joint correspondence courses, civilian education, and institutional training. Officers should devote time to a professional reading program to broaden their warfighting perspective.

(8) Branch transfers. RC officers may request a branch transfer into the Cyber Branch as prescribed by the policies and procedures for their Component. RC officers transferring into the Cyber Branch must attend CyOOC for AOC 17A (or the designated transition course/training pipeline for AOC 17D if/when available to RC officers). If designated for AOC 17B, branch transfer RC Cyber Officers must complete CyOOC for 17A, followed by the 17B CEWO Qualification Course, unless granted an exception/waiver to this requirement by the Commandant, U.S. Army Cyber School. For RC Cyber Officers, the qualification standards at each rank/grade, as well as, PME requirements are the same as for their counterpart AC officers. Commanders should closely manage branch transfer officers and assign them to a qualifying position concurrent with enrollment or following the completion of their 17-series AOC-qualification course(s). Officers should not normally be assigned to a qualifying position prior to enrolling in or completing branch/AOC-specific qualification requirements.

(9) Formal education.

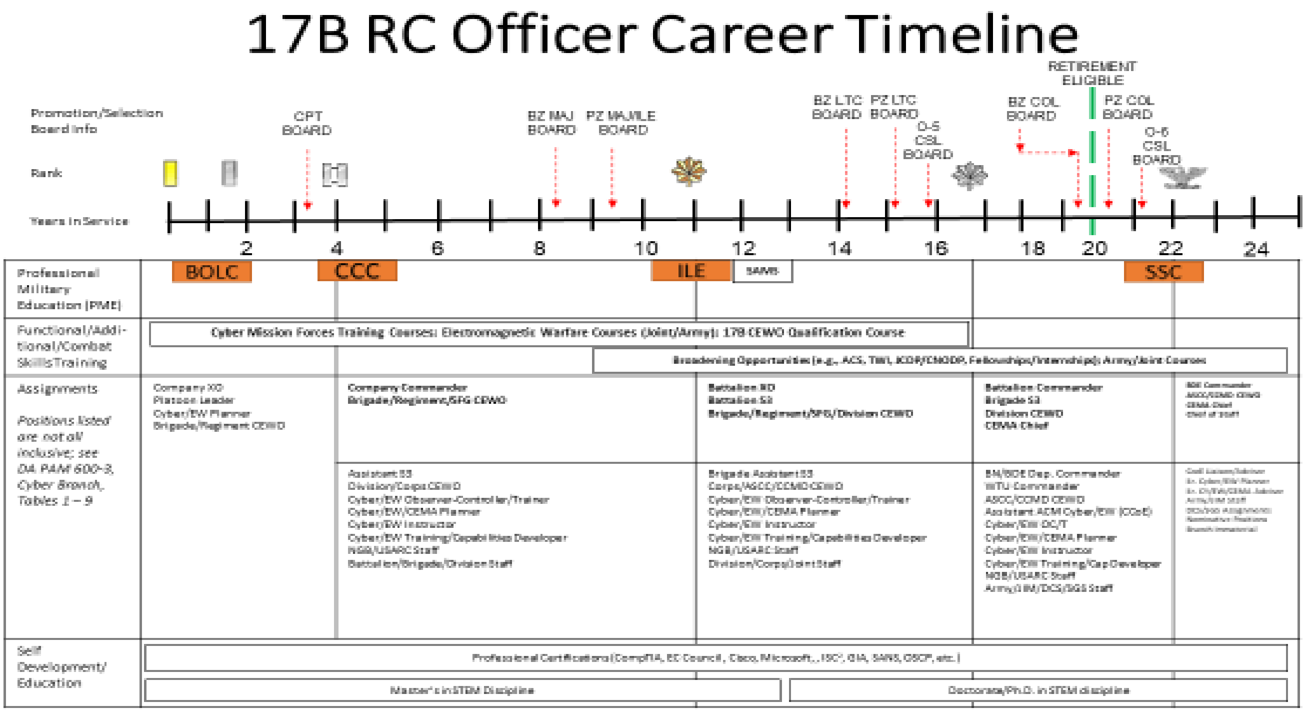
(b) PME course credit. RC Cyber Officers can apply for PME course credit based on previous leadership experience and past academic or training experience, per AR 350-1. The approval authority for course credit for the PME portions of BOLC or CCC is the Director of Training, TRADOC G-37, delegated from HQDA DCS G-3/5/7.

(c) Cyber Course Credit Program. Cyber Officers who acquire relevant CO or EW knowledge, skills, and behaviors through military courses or experience and/or civilian industry, education, or training may apply for course credit for portions of AOC qualification courses governed by the U.S. Army Cyber School, Fort Gordon, GA. The Cyber Course Credit Program is managed by the U.S. Army Cyber School IAW AR 350-1, for the evaluation and awarding of constructive, equivalent, and operational credit. The approval authority for awarding 17A, 17B, and 17D qualification course credit (not including PME credit) is the Commandant, U.S. Army Cyber School, Fort Gordon, GA. Cyber course credit, if approved, will be documented in a memorandum signed by the Commandant, U.S. Army Cyber School (or authorized delegate). The approval memorandum serves as verification of course credit toward 17A, 17B, and/or 17D AOC qualification in lieu of DA Form 1059.



Professional Military Education (PME)	BOLC	CCC	ILE SAMS		SSC
Functional/Additional/Combat Skills Training	Cyber Mission Forces Training Courses: Electromagnetic Warfare Courses (Joint/Army): 17B CEWO Qualification Course				
		Broadening Opportunities (e.g., ACS, TWI, JCDP/CMODP, Fellowships/Internships): Army/Joint Courses			
Assignments *Positions listed are not all inclusive; see DA PAM 600-3, Cyber Branch, Tables 1 – 9*	Company XO Platoon Leader Assistant S3 Section Leader Cyber Planner Analytic Support Officer Battle Captain Aide de Camp	**Company Commander** **Mission Team/Section/Element Leader** **Cyber Defense Manager**	**Battalion XO** **Battalion S3** **Mission Team Leader** **Senior Cyber Defense Manager** **Senior Observer-Controller/Trainer (CTCs)**	**Battalion Commander** **BN/BDE S3** **Mission Team Leader** **Division CEWO**	**BDE Commander** **Chief of Staff**
		Assistant S3 Cyber Observer-Controller/Trainer Cyber/CEMA Planner Cyber Branch Chief Cyber Instructor Cyber Training/Capabilities Developer NGB/USARC Staff Battalion/Brigade/Division Staff	Brigade Assistant S3 Cyber Observer-Controller/Trainer Cyber/CEMA Planner Cyber Branch Chief / Mission Manager Cyber Instructor Cyber Training/Capabilities Developer NGB/USARC Staff Division/Corps/Joint Staff Corps/Medical CMD/TTSB/TSSB/RCC Net Ops	BN/BDE Deputy Commander WTU Commander Corps Net Ops Officer. Theater Signal Staff Officer Mission/Technical Director Cyber Division Chief Instructor Sr. Cyber/CEMA Planner Sr. Training/Capabilities Developer NGB/USARC Staff Army/JIIM/DCS/SGS Staff	CCoE Liaison/Advisor Sr. Cyber Planner Sr. Cyber/CEMA Advisor Army/JIIM Staff DCS/ISO Assignments Nominative Positions Branch Immaterial
Self Development/ Education	Professional Certifications (CompTIA, EC Council , Cisco, Microsoft, , ISC², GIA, SANS, OSCP, etc.)				
	Master's in STEM Discipline			Doctorate/Ph.D. in STEM discipline	

Figure 4: 17A RC Officer Career Timeline



Professional Military Education (PME)	BOLC	CCC	ILE SAMS		SSC
Functional/Additional/Combat Skills Training	Cyber Mission Forces Training Courses: Electromagnetic Warfare Courses (Joint/Army): 17B CEWO Qualification Course				
		Broadening Opportunities (e.g., ACS, TWI, JCDP/CMODP, Fellowships/Internships): Army/Joint Courses			
Assignments *Positions listed are not all inclusive; see DA PAM 600-3, Cyber Branch, Tables 1 – 9*	Company XO Platoon Leader Cyber/EW Planner Brigade/Regiment CEWO	**Company Commander** **Brigade/Regiment/SFG CEWO**	**Battalion XO** **Battalion S3** **Brigade/Regiment/SFG/Division CEWO**	**Battalion Commander** **Brigade S3** **Division CEWO** **CEMA Chief**	**BDE Commander** **ASCC/CCMD CEWO** **CEMA Chief** **Chief of Staff**
		Assistant S3 Division/Corps CEWO Cyber/EW Observer-Controller/Trainer Cyber/EW/CEMA Planner Cyber/EW Instructor Cyber/EW Training/Capabilities Developer NGB/USARC Staff Battalion/Brigade/Division Staff	Brigade Assistant S3 Corps/ASCC/CCMD CEWO Cyber/EW Observer-Controller/Trainer Cyber/EW/CEMA Planner Cyber/EW Instructor Cyber/EW Training/Capabilities Developer NGB/USARC Staff Division/Corps/Joint Staff	BN/BDE Dep. Commander WTU Commander ASCC/CCMD CEWO Assistant ACM Cyber/EW (CCoE) Cyber/EW OC/T Cyber/EW/CEMA Planner Cyber/EW Instructor Cyber/EW Training/Cap Developer NGB/USARC Staff Army/JIIM/DCS/SGS Staff	CCoE Liaison/Advisor Sr. Cyber/EW Planner Sr. CY/EW/CEMA Advisor Army/JIIM Staff DCS/ISO Assignments Nominative Positions Branch Immaterial
Self Development/ Education	Professional Certifications (CompTIA, EC Council , Cisco, Microsoft, , ISC², GIA, SANS, OSCP, etc.)				
	Master's in STEM Discipline			Doctorate/Ph.D. in STEM discipline	

Figure 5: 17B RC Officer Career Timeline

5. Warrant Officer Development

a. *Unique knowledge and skills of a Cyber warrant officer*. Cyber branch warrant officers must maintain the characteristics identified herein.

1. Cyber branch warrant officers are leaders and skilled technicians. They have technically-unique skills, knowledge, and attributes that require continuing professional development.
2. Cyber branch warrant officers must possess expert knowledge and skill in Cyberspace and Electromagnetic Warfare operations supporting mission command; such knowledge and skill require practical experience in tactics, combined arms operations, and the employment of systems and processes.
3. Cyber branch warrant officers sustain knowledge and skills through institutional training and education, duty in operational assignments, and continuous self-development. Cyber branch warrant officers may deploy with units, teams, or individuals to support Army, Joint, Interagency, and Intergovernmental and Multinational (JIIM) applications of Cyberspace operations.

b. *Cyber branch warrant officer military occupational specialties (MOSs).* Cyber branch warrant officers are experts who provide technical and tactical expertise and experience and invaluable leadership throughout all levels of command. MOSs for Cyber branch warrant officers are: 170A - Cyber Warfare Technician, 170B - Electromagnetic Warfare Technician, and 170D – Cyber Capabilities Developer Technician.

(1) 170A Cyber Warfare Technician Active Component Warrant Officer Development.

(a) Characteristics required of Cyber Warfare Technician. Cyber Warfare Technicians plan, supervise, assess and execute offensive and defensive Cyberspace operations. They lead small teams to accomplish unit objectives. They provide technical guidance, expertise, and advice to commanders and their staff on the management and application of Army and JIIM Cyberspace operations. They must be consummate professionals; self-motivated and self-disciplined. They must be awarded and maintain a current TOP SECRET (TS) Sensitive Compartmented Information (SCI) clearance to maintain the MOS. Additionally, Cyber Warfare Technicians must be capable of passing a counterintelligence scope polygraph (CSP) to hold the MOS. Soldiers who refuse to take or fail a CSP will be reclassified.

(b) Unique knowledge and skills of a Cyber Warfare Technician. The Cyber Warfare Technician is a Subject Matter Expert (SME) on Cyberspace Operations and is a leader, trainer, and advisor to commanders at all levels. The Cyber Warfare Technician assists in leading and planning while engaging in both Defensive and Offensive Cyberspace Operations (DCO and OCO). The Cyber Warfare Technician is primarily responsible for carrying out the technical aspects of OCO and DCO while using Cyber capabilities in and through Cyberspace to defend against, target, and neutralize threats. The Cyber Warfare Technician must master all knowledge related to the Cyberspace domain and understand the Electromagnetic spectrum and the Department of Defense Information Network (DODIN) environment, including associated doctrine, policies, statutes, and laws. As Cyber Officers, Cyber Warfare Technicians must operate without direct oversight or guidance, be self-motivated, and provide timely and effective technical products, effects, and solutions. Cyber Warfare Technicians mainly assess from Cyber Operations Specialists (17C) who demonstrate a high degree of technical expertise in all facets of Cyber Operations. Cyber Warfare Technicians perform the following functions/tasks:

1. Advise commanders on the availability and employment of Cyberspace capabilities.
2. Assess the effects of defensive and offensive cyberspace operations.
3. Plan, lead, and execute Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR), Cyberspace Surveillance and Reconnaissance (S&R), Cyberspace Operational Preparation of the Environment (OPE), Cyberspace Attack, and Cyberspace Defense.
4. Integrate Cyber effects into planning/targeting processes.
5. De-conflict, integrate, and synchronize Cyberspace operations.
6. Analyze relevant/current situations to predict operational Cyber requirements.
7. Defend operational networks.
8. Defend weapon platforms and systems.
9. Develop and mentor all Cyber Operations Personnel.
10. Integrate EW capabilities into Cyber operational planning.

(c) Assignments: Cyber Warfare Technicians are primarily assigned to units specifically conducting offensive and defensive Cyberspace operations. These assignments provide extensive exposure to operations in and through the Cyberspace domain in support of multi-domain battles. Select warrant officers can also expect to receive assignments that broaden their experience as Cyber Warfare Technicians and may serve in a generating force capacity such as the following:

1. Instructor / Writer (CCoE,USMA)
2. Sr. Instructor / Writer (CCoE, USMA)
3. Cyber Career Program Manager
4. Sr. Cyber Career Program Manager
5. CCoE CCWO
6. Cyber CWOB

(d) Military Oriented Training: In addition to Professional Military Education, military-orientated training for all Cyber Warfare Technician warrant officers can include:

1. Warrant Officer Cryptologic Career Program (WOCCP)
2. Computer Network Operations Development Program (CNODP)
3. Special Technical Operations Planners Course (V8)
4. Special Technical Operations Chief Course (V9)
5. Joint Network Attack Course (JNAC)
6. Joint Fires and Effect Course
7. Joint Targeting Staff Course

(e) Self-development. Lifelong learning, supported by civilian STEM degree programs, military education, and Training with Industry, provides opportunities to develop competencies throughout the warrant officer's career. For development, senior cyber technicians require assignment-oriented, joint training courses and advanced civil schooling.

(f) WO1/CW2 development.

1. Entry level. Upon warrant officer selection, all non-commissioned officers (warrant officer candidates upon arrival) will complete Warrant Officer Candidate School (WOCS). WOCS provides the basic skills necessary to prepare the warrant officer candidate to become an effective Army warrant officer.

2. Education. After graduation from WOCS and appointment to WO1, each warrant officer will attend the 19-week Warrant Officer Basic Course (WOBC) at Fort Gordon, GA. The 170A Cyber Warfare Technician Warrant Officer Basic Course (WOBC) provides Cyber Warfare Technicians the education, training, and core skills necessary to lead Cyberspace operations successfully. The emphasis is on Army tactics, techniques, and procedures (TTP) to prepare the warrant officers to lead and direct the execution of authorized Cyber effects. Company grade warrant officers need to develop a basic understanding of technical integration of Cyberspace Defense, Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR), Cyberspace Surveillance and Reconnaissance (S&R) Cyberspace Operational Preparation of the Environment (OPE), and Cyberspace Attack in support of multi-domain operations. Additionally, warrant officers should possess increased knowledge in a related special skill area to increase competitiveness. Completing an associate's or baccalaureate degree is a recommended goal before becoming eligible for promotion to CW3.

3. Desired experience. Junior Cyber Warfare Technicians must attain and maintain senior-level certification in at least one Cyberspace Operations work role. Continuous education, training, and experience in the execution of Cyberspace operations prepare the junior 170A warrant officer for future assignments and selection to CW3.

(g) CW3 development.

1. Education. The 170A Warrant Officer Advanced Course (WOAC) focuses on advanced technical training and common leader development subjects designed to prepare officers for Field Grade Cyber Warfare Technician positions. The residential course at the Army Cyber School at Fort Gordon, GA, consists of 16-weeks of advanced technical and tactical training in Cyberspace Operations. Additionally, CW3s should complete WOAC before promoting CW4 and must complete before assignment to a broadening, nominative, or specialty billet. Completing a baccalaureate or master's degree in a related STEM discipline is also a recommended goal before becoming eligible for promotion to CW4.

2. Desired experience. CW3s must have the requisite senior-level expertise to perform one cyber work role and have a basic understanding of multiple work roles before serving as a Cyber Mission Force team senior technical advisor. Additionally, CW3s must possess the technical comprehension and competence in the management of Cyberspace Defense; Cyberspace ISR; Cyberspace S&R, Cyberspace OPE. Finally, CW3s should master cyberspace attack actions at the tactical and strategic level before becoming a CW4.

(h) CW4 development.

1. Education. The Warrant Officer Intermediate Level Education (WOILE) is a professional development course with a two-week Phase one distance learning (DL) portion, followed by a five-week resident Phase two-portion taught at the Warrant Officer Career Center (WOCC), Fort Rucker, AL and a final five-week Phase three taught at the Cyber School, Fort Gordon, GA. WOILE provides intermediate-level professional military education and leader development (PME- LD) training that prepares Field Grade warrant officers (CW3/CW4) to function as staff officers, trainers, managers, systems integrators, and leaders at various

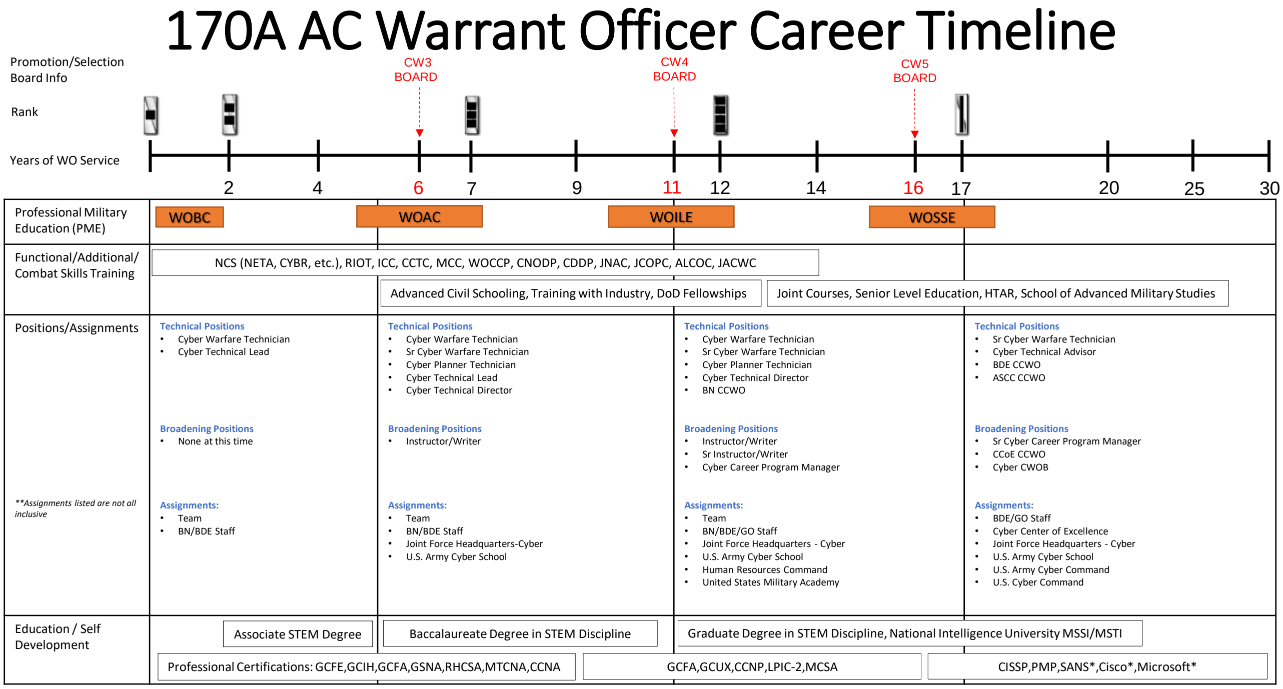
levels of Army and JIIM organizations while executing multi-domain and large scale combat operations through decisive action. CW4s should complete WOILE by the one-year time-in-grade point. Additionally, CW4 should complete WOILE for promotion to CW5 and must be complete before assignment to CW4 broadening, nominative, or specialty billet.

2. Desired experience. CW4s should have experience leading and/or coordinating offensive and defensive Cyberspace operations before being assigned to senior Cyber technical advisor positions. It is highly desirable that CW4s attain master-level expertise in at least one Cyber work role and must have a basic level understanding of multiple work roles. Completing a master's degree in a related STEM discipline is a highly desired goal before becoming eligible for promotion to CW5.

(i) CW5 development.

1. Education. The Warrant Officer Senior Service Education (WOSSE) is a two-phase course consisting of a Phase one (DL) portion followed by a four-week Phase two (resident) portion attended by the Army's most senior warrant officers. The educational goal is to provide senior CW4s new CW5s with the master-level education, knowledge, and effective leadership skills necessary to apply their technical expertise to support leaders on Army and strategic-level joint staffs during multi-domain operations. CW5s should attend WOSSE by the one-year time-in-grade point. CW5s must complete before assignment to a Command Chief Warrant Officer billet. Additionally, CW5s should continue work in an associated graduate-level field of study.

2. Desired experience. All CW5 170As should have cyber operational experience leading, advising, coordinating, and executing either OCO or DCO operations at all levels. The cyber branch highly desires CW5s to have operational experience in both OCO and DCO operations and have attained proficiency in all critical tasks through combined experiences and career self-development in every aspect of their career path.



Professional Military Education (PME)	WOBC	WOAC	WOILE	WOSSE
Functional/Additional/ Combat Skills Training	NCS (NETA, CYBR, etc.), RIOT, ICC, CCTC, MCC, WOCCP, CNODP, CDDP, JNAC, JCOPC, ALCOC, JACWC	Advanced Civil Schooling, Training with Industry, DoD Fellowships		Joint Courses, Senior Level Education, HTAR, School of Advanced Military Studies
Positions/Assignments ***Assignments listed are not all inclusive*	Technical Positions • Cyber Warfare Technician • Cyber Technical Lead Broadening Positions • None at this time Assignments: • Team • BN/BDE Staff	Technical Positions • Cyber Warfare Technician • Sr Cyber Warfare Technician • Cyber Planner Technician • Cyber Technical Lead • Cyber Technical Director Broadening Positions • Instructor/Writer Assignments: • Team • BN/BDE Staff • Joint Force Headquarters-Cyber • U.S. Army Cyber School	Technical Positions • Cyber Warfare Technician • Sr Cyber Warfare Technician • Cyber Planner Technician • Cyber Technical Director • BN CCWO Broadening Positions • Instructor/Writer • Sr Instructor/Writer • Cyber Career Program Manager Assignments: • Team • BN/BDE/GO Staff • Joint Force Headquarters - Cyber • U.S. Army Cyber School • Human Resources Command • United States Military Academy	Technical Positions • Sr Cyber Warfare Technician • Cyber Technical Advisor • BDE CCWO • ASCC CCWO Broadening Positions • Sr Cyber Career Program Manager • CCoE CCWO • Cyber CWOB Assignments: • BDE/GO Staff • Cyber Center of Excellence • Joint Force Headquarters - Cyber • U.S. Army Cyber School • U.S. Army Cyber Command • U.S. Cyber Command
Education / Self Development	Associate STEM Degree	Baccalaureate Degree in STEM Discipline	Graduate Degree in STEM Discipline, National Intelligence University MSSI/MSTI	
	Professional Certifications: GCFE,GCIH,GCFA,GSNA,RHCSA,MTCNA,CCNA		GCFA,GCUX,CCNP,LPIC-2,MCSA	CISSP,PMP,SANS*,Cisco*,Microsoft*

Figure 6: 170A AC Warrant Officer Career Timeline

(2) 170A Cyber Warfare Technician Reserve Component Warrant Officer Development.

(a) General career development. RC warrant officer (USAR and ARNG) development objectives and qualifications parallel those of their AC counterparts.

(b) Branch development opportunities. Even though geographical considerations limit some RC warrant officers, all should strive for operational Cyber assignments that yield the same developmental opportunities as their AC counterparts.

(c) Training and development. Required training and recommended branch developmental assignments by grade are as follows:

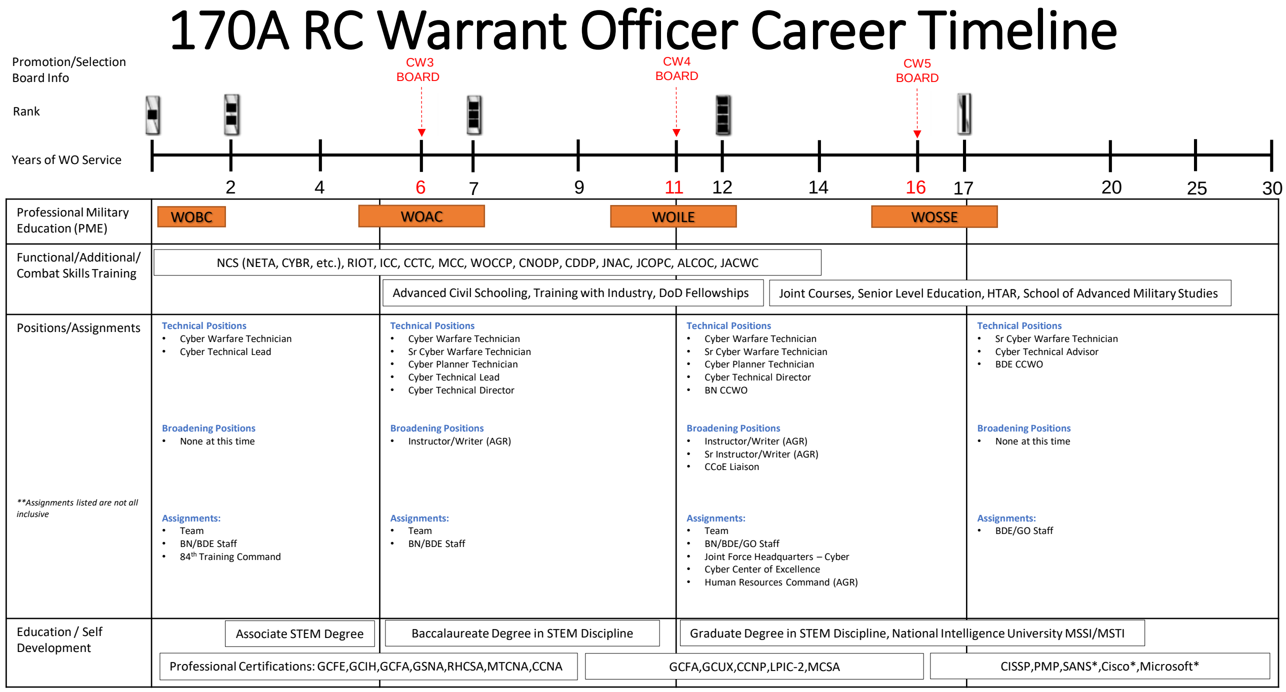
1. Warrant Officer One. Must complete WOCS and WOBC before promotions to CW2. Assignments include team leader and section chief. WO1 positions concentrate in Cyber Protection Team TDA organizations within the USAR and ARNG.

2. Chief Warrant Officer Two. Warrant officers with at least one year in grade as a CW2 can attend WOAC but must complete the course before promoting CW3. Assignments include team leader, section chief, and operations chief. CW2 positions concentrate in Cyber Protection Team TDA organizations within the USAR and ARNG.

3. Chief Warrant Officer Three. Warrant officers with at least one year time-in-grade as a CW3 can attend WOILE but must complete the course before promoting CW4. Assignments include senior operations tech, systems architect, team leader, information protection technician, and instructor. CW3 positions concentrate in Cyber Protection Team TDA organizations within the USAR and ARNG.

4. Chief Warrant Officer Four. Warrant officers with at least one year of time-in-grade as a CW4 can attend W O SSE but must complete the course before promoting CW5. Assignments include senior technician, instructor, detachment commander, and section or branch chief in a joint assignment. CW4 positions concentrate in Cyber Protection Team TDA organizations within the USAR and ARNG.

5. Chief Warrant Officer Five. Must be assigned to authorized Cyber Branch CW5 positions. CW5 positions are key staff officer positions at major commands. CW5s advise commanders at all levels on doctrine, structure, assignments, and training. Potential assignments include Command Chief Warrant Officer (CCWO), Brigade Senior Technical Advisor, Component Cyber Advisor, or Proponent Branch Chief.



Professional Military Education (PME)	WOBC	WOAC	WOILE	WOSSE
Functional/Additional/ Combat Skills Training	NCS (NETA, CYBR, etc.), RIOT, ICC, CCTC, MCC, WOCCP, CNODP, CDDP, JNAC, JCOPC, ALCOC, JACWC	Advanced Civil Schooling, Training with Industry, DoD Fellowships	Joint Courses, Senior Level Education, HTAR, School of Advanced Military Studies	
Positions/Assignments ***Assignments listed are not all inclusive*	Technical Positions • Cyber Warfare Technician • Cyber Technical Lead Broadening Positions • None at this time Assignments: • Team • BN/BDE Staff • 84th Training Command	Technical Positions • Cyber Warfare Technician • Sr Cyber Warfare Technician • Cyber Planner Technician • Cyber Technical Lead • Cyber Technical Director Broadening Positions • Instructor/Writer (AGR) Assignments: • Team • BN/BDE Staff	Technical Positions • Cyber Warfare Technician • Sr Cyber Warfare Technician • Cyber Planner Technician • Cyber Technical Director • BN CCWO Broadening Positions • Instructor/Writer (AGR) • Sr Instructor/Writer (AGR) • CCoE Liaison Assignments: • Team • BN/BDE/GO Staff • Joint Force Headquarters – Cyber • Cyber Center of Excellence • Human Resources Command (AGR)	Technical Positions • Sr Cyber Warfare Technician • Cyber Technical Advisor • BDE CCWO Broadening Positions • None at this time Assignments: • BDE/GO Staff
Education / Self Development	Associate STEM Degree Professional Certifications: GCFE,GCIH,GCFA,GSNA,RHCSA,MTCNA,CCNA	Baccalaureate Degree in STEM Discipline	Graduate Degree in STEM Discipline, National Intelligence University MSSI/MSTI GCFA,GCUX,CCNP,LPIC-2,MCSA	CISSP,PMP,SANS*,Cisco*,Microsoft*

Figure 7: 170A RC Warrant Officer Career Timeline

(3) 170B Electromagnetic Warfare Technician Warrant Officer Development.

(a) Characteristics required of Electromagnetic Warfare Technician. The 170B Electromagnetic Warfare Technician plans, directs, supervises, and assesses Electromagnetic Warfare and Cyberspace operations. The Electromagnetic Warfare Technician serves as the technical and tactical EW expert prepared to organize, manage, and lead small teams/sections/cells to accomplish unit objectives. They provide technical guidance, expertise, and advice to commanders and staffs on the management and operation of Army, Joint, Interagency, and Multinational applications of Electromagnetic Warfare and Cyberspace Operations. They must be consummate professionals; self-motivated and self-disciplined, and live the Army Values. They must possess a current TOP SECRET (TS) Sensitive Compartmented Information (SCI) clearance to be awarded and maintain the MOS.

(b) Unique knowledge and skills of a 170B Electromagnetic Warfare Technician. The Electromagnetic Warfare Technician is the Subject Matter Expert (SME) on Electromagnetic Warfare and the integration of Cyberspace operations. The Electromagnetic Warfare Technician is a leader, trainer, and advisor to staffs and commanders at all levels. The Electromagnetic Warfare Technician analyzes, plans, organizes, executes, monitors, integrates, and assesses Electromagnetic Warfare operations, threat environment, and technical requirements. The Electromagnetic Warfare Technician synchronizes effects with the fires cell/section to disrupt or destroy Electromagnetic Warfare targets, whether by lethal or nonlethal means. The Electromagnetic Warfare Technician provides advice on the technical and tactical employment of both organic and non-organic EW systems. The Electromagnetic Warfare Technician should have a general understanding of Cyberspace Operations and in the Cyber Mission Force (CMF). The Electromagnetic Warfare Technician facilitates and manages unit maintenance, oversight, and training programs pertaining to Electromagnetic Warfare. Electromagnetic Warfare Technicians mainly assess Electromagnetic Warfare Operations Specialists (17E) who possess a high degree of success spanning multiple echelons and demonstrate technical expertise in all facets of Electromagnetic Warfare. Electromagnetic Warfare Technicians perform the following vital functions/tasks:

1. Advise commanders on capabilities and employment of Electromagnetic Warfare assets and capabilities.

2. Execute Electromagnetic Attack in support of a commander’s requirements.

3. Conduct Electromagnetic Support to meet the commander’s requirement (geolocation, direction finding, immediate threat warning, and emitter analysis)

4. Implement Electromagnetic Protection measures (masking, emission control).

5. Monitor Electromagnetic Spectrum (EMS) for indications and warnings, enabling immediate threat recognition and targeting.

6. Assist in identifying intelligence gaps/requirements, priorities, target selection standards, attack guidance, and targeting.

7. Assist and coordinate with S2/G2/J2 on Intelligence Preparation of the Battlefield and Electromagnetic Order of Battle (EOB) as it pertains to EW.

8. Deconflict Electromagnetic Warfare with the Analysis Control Element and Collection Management in the collection process.

9. Coordinate external support for EW mission requirements and integrate EW into planning/targeting processes.

10. Supervise Cyberspace Electromagnetic Activities training programs and all assets assigned.

11. Enable Cyberspace Operations through close access and the request for cyber effects.

(c) Assignments: Electromagnetic Warfare Technicians are primarily assigned at the ASCC and below levels. These assignments allow tactical commanders to integrate Electromagnetic Warfare capabilities and exposure to Cyberspace operations to support multi-domain operations and large scale combat operations. Select warrant officers can also expect to receive assignments that broaden their experience as Electromagnetic Warfare Technicians and may serve in a generating force capacity such as the following (not all-inclusive):

1. Warrant Officer Assignment Human Resource Command
2. EW Career Program Manager
3. Instructor / Writer (WOBC/WOAC/WOILE/USMA)
4. Sr. Instructor / Writer (WOBC/WOAC/WOILE/USMA)
5. Staff Officer (EW)
6. Cyber CWOB
7. Training, Advising, and Counseling (TAC) Officer

(d) Military Oriented Training: In addition to Professional Military Education, military-orientated training for all Cyber and Electromagnetic Warfare Operations Technicians can include (not all-inclusive):

1. Joint EW Theater Operations Course
2. Special Technical Operations Planners Course (V8)
3. Special Technical Operations Chief Course (V9)
4. Space Cadre Course (3Y)
5. Cyber 200
6. Cyber 300
7. Joint Firepower Course
8. Joint Advanced Cyber Warfare Course
9. Military Deception Planners Course
10. Aerial Precision Geolocation Course (V3)
11. Close Access Tactical-Recon (CAT-R)
12. NATO EW Course
13. NATO Targeting Course

14 Joint Targeting Staff Course

15 Joint Network Attack Course (JNAC)

16 Joint Fires and Effect Course

17. Space 200

18. Space 300

(e) Self-development. Lifelong learning, supported by civilian STEM degree programs, military education, and Training with Industry, provides opportunities to develop competencies throughout the warrant officer's career. Assignment-oriented, joint training courses, and advanced civil schooling are needed to develop characteristics required of a senior Cyber and Electromagnetic Warfare Operations Technician based on current and projected duty assignments.

(f) WO1/CW2 development.

1. Entry level. Upon warrant officer selection, all non-commissioned officers (warrant officer candidates upon arrival) will complete Warrant Officer Candidate School (WOCS). WOCS provides the basic skills necessary to prepare the warrant officer candidate to become an effective Army warrant officer.

2. Education. After graduation from WOCS and appointment to WO1, each warrant officer will attend the 15-week Warrant Officer Basic Course (WOBC) at Fort Gordon, GA. The 170B Electromagnetic Warfare Technician Basic Course provides Electromagnetic Warfare Warrant Officers the education, training, and core skills necessary to lead Electromagnetic Warfare operations. The emphasis is on Army tactics, techniques, and procedures to prepare the warrant officers to lead and direct authorized effects throughout the electromagnetic spectrum. Company grade warrant officers need to develop a basic understanding of technical integration of effects of friendly and adversary Electromagnetic Warfare systems on the Electromagnetic Spectrum (EMS), Cyberspace Electromagnetic Activities (CEMA) concepts, Cyberspace Operational Preparation of the Environment (OPE), and offensive/defensive Cyberspace operations in support of Multi-Domain Operation (MDO). Completion of an associate's or baccalaureate degree is a recommended goal before becoming a CW3.

3. Desired experience. Junior 170B Electromagnetic Warfare Technicians must attain and maintain expertise on the science of signal theory, application of Electromagnetic order of battle, and the request, limitation, and application of Electromagnetic Warfare and Cyberspace effects for implementation at the Corps and below. Continuous education, training, and experience in the coordination and execution of CEMA at echelons Corps and below prepare the junior 170B warrant officer for future assignments and selection to CW3.

(g) CW3 development.

1. Education. The 170B Warrant Officer Advanced Course (WOAC) focuses on advanced technical training and common leader development subjects designed to prepare warrant officers for Field Grade Cyber and Electromagnetic Warfare Operations Technician positions. The residential course at Fort Gordon, GA, consists of 8-weeks of advanced technical and tactical training in Electromagnetic Warfare and Cyberspace Operations. Additionally, CW3s should complete WOAC before promoting CW4 and must complete before assignment to a broadening, nominative, or specialty billet. Completing a baccalaureate or master's degree in a related STEM discipline is also a recommended goal before becoming eligible for promotion to CW4.

2. Desired experience. CW3s should have requisite journeyman-level expertise, technical comprehension, and competence in the employment of Electromagnetic Warfare and Cyberspace assets and capabilities at the tactical level. Electromagnetic Warfare Technicians at the CW3 level are self-aware and adaptive integrators of systems, assets, and capabilities across multiple echelons and services. Increased responsibilities require warrant officers to exercise leadership, mandate an ability to operate and integrate staff functions at the tactical to an operational level. The Electromagnetic Warfare Technicians CW3 must continue their developmental growth while recognizing the increased opportunities within the operating force, broadening assignments, functional training, and self-development requirements that capitalize on their technical skills. Warrant officers at this rank should continue their role as a coach, mentors, and advisors to junior warrant officers.

(h) CW4 development.

1. The Warrant Officer Intermediate Level Education (WOILE) is a professional development course with a two-week Phase one distance learning (DL) portion, followed by a five-week resident Phase two-portion taught at the Warrant Officer Career Center (WOCC), Fort Rucker, AL and a final five-week Phase three taught at the Cyber School, Fort Gordon, GA. WOILE provides intermediate-level professional military education and leader development (PME- LD) training that prepares Field Grade warrant officers (CW3/CW4) to function as staff officers, trainers, managers, systems integrators, and leaders at various levels of Army and joint organizations while executing multi-domain operation through decisive action. CW4s should complete WOILE by the one-year time-in-grade point. Additionally, CW4 should complete WOILE for promotion to CW5 and must be complete before assignment to CW4 broadening, nominative, or specialty billet.

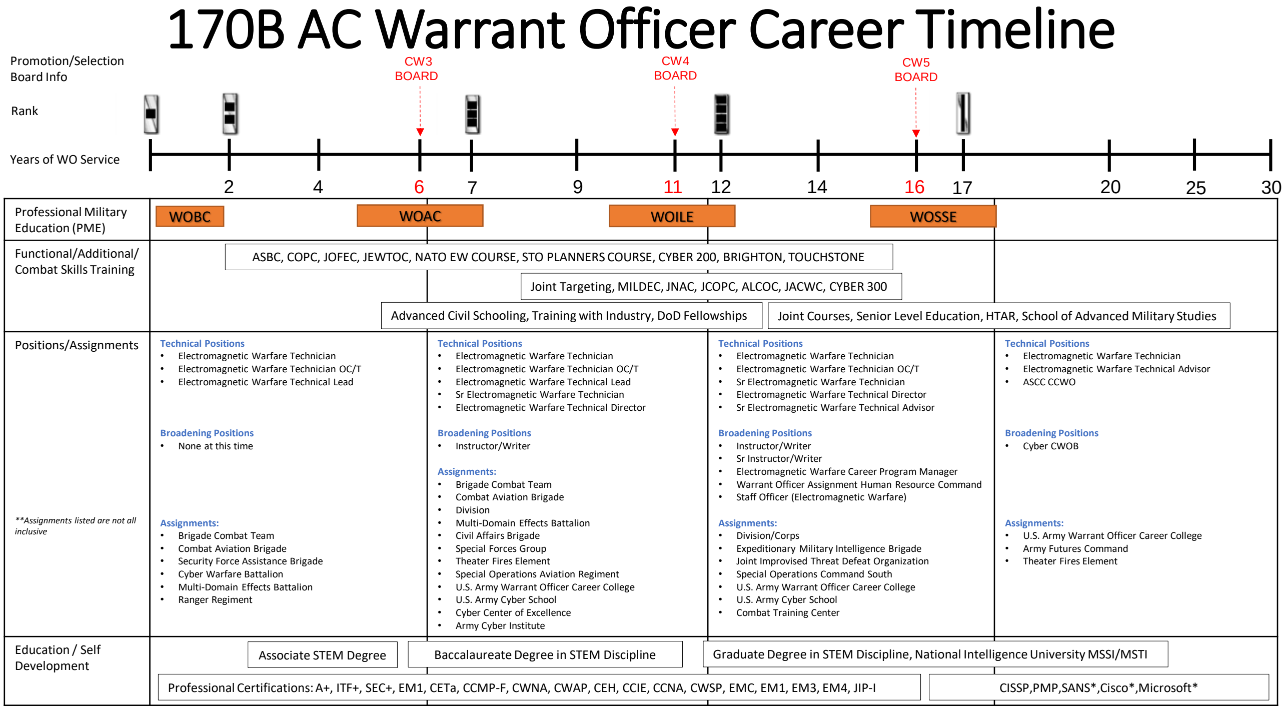
2. Desired experience. Electromagnetic Warfare Technicians at the CW4 level are senior-level technical and tactical experts that should exude character, competence, and commitment while thriving in complex and uncertain environments. CW4s are highly adept and adaptive leaders, trainers, and advisors who operate by design in specialized roles across a range of Army and military operations. They bring an unequaled

depth and breadth of knowledge, experience, and perspective to the organizations in which they serve. Increased responsibilities mandate an ability to operate and integrate within staff functions at all levels. As they become more senior, they focus on integrating branch and Army systems at the national level.

(i) CW5 development.

1. Education. The Warrant Officer Senior Service Education (WOSSE) is a two-phase course consisting of a Phase one (DL) portion followed by a four-week Phase two (resident) portion attended by the Army's most senior warrant officers. The educational goal is to provide senior CW4s or new CW5s with the master-level education, knowledge, and influential leadership skills necessary to apply their technical expertise to support leaders on strategic-level joint staff during multi-domain operations. CW5s should continue work in an associated graduate-level field of study.

2. Desired experience. Electromagnetic Warfare Technicians at the CW5 level are master-level technical and tactical experts who perform the primary duties of technical leader, manager, integrator, and advisor. They are the senior technical expert in their branch and serve at the highest levels. By necessity, they need to be comfortable operating in ambiguity and skilled at solving ill-structured problems. CW5s are highly adept and adaptive leaders, trainers, and advisors who operate by design in specialized roles across a range of Army operations. They bring an unequaled depth and breadth of knowledge, experience, and perspective to the organizations in which they serve. Increased responsibilities mandate an ability to operate and integrate within staff functions at the tactical to the strategic level and necessitate the ability to thrive in increasingly complex and uncertain environments. CW5 assignments are available both in and outside one's standard career path, which is nominative or broadening.


170B AC Warrant Officer Career Timeline
Promotion/Selection Board Info
CW3 BOARD
CW4 BOARD
CW5 BOARD
Rank
Years of WO Service
2
4
6
7
9
11
12
14
16
17
20
25
30
Professional Military Education (PME)
WOBC
WOAC
WOILE
WOSSE
Functional/Additional/ Combat Skills Training
ASBC, COPC, JOFEC, JEWTOC, NATO EW COURSE, STO PLANNERS COURSE, CYBER 200, BRIGHTON, TOUCHSTONE
Joint Targeting, MILDEC, JNAC, JCOPC, ALCOC, JACWC, CYBER 300
Advanced Civil Schooling, Training with Industry, DoD Fellowships
Joint Courses, Senior Level Education, HTAR, School of Advanced Military Studies
Education / Self Development
Associate STEM Degree
Baccalaureate Degree in STEM Discipline
Graduate Degree in STEM Discipline, National Intelligence University MSSI/MSTI
Professional Certifications: A+, ITF+, SEC+, EM1, CETa, CCMP-F, CWNA, CWAP, CEH, CCIE, CCNA, CWSP, EMC, EM1, EM3, EM4, JIP-I
CISSP,PMP,SANS*,Cisco*,Microsoft*

Positions/Assignments ***Assignments listed are not all inclusive*	**Technical Positions** • Electromagnetic Warfare Technician • Electromagnetic Warfare Technician OC/T • Electromagnetic Warfare Technical Lead **Broadening Positions** • None at this time **Assignments:** • Brigade Combat Team • Combat Aviation Brigade • Security Force Assistance Brigade • Cyber Warfare Battalion • Multi-Domain Effects Battalion • Ranger Regiment	**Technical Positions** • Electromagnetic Warfare Technician • Electromagnetic Warfare Technician OC/T • Electromagnetic Warfare Technical Lead • Sr Electromagnetic Warfare Technician • Electromagnetic Warfare Technical Director **Broadening Positions** • Instructor/Writer **Assignments:** • Brigade Combat Team • Combat Aviation Brigade • Division • Multi-Domain Effects Battalion • Civil Affairs Brigade • Special Forces Group • Theater Fires Element • Special Operations Aviation Regiment • U.S. Army Warrant Officer Career College • U.S. Army Cyber School • Cyber Center of Excellence • Army Cyber Institute	**Technical Positions** • Electromagnetic Warfare Technician • Electromagnetic Warfare Technician OC/T • Sr Electromagnetic Warfare Technician • Electromagnetic Warfare Technical Director • Sr Electromagnetic Warfare Technical Advisor **Broadening Positions** • Instructor/Writer • Sr Instructor/Writer • Electromagnetic Warfare Career Program Manager • Warrant Officer Assignment Human Resource Command • Staff Officer (Electromagnetic Warfare) **Assignments:** • Division/Corps • Expeditionary Military Intelligence Brigade • Joint Improvised Threat Defeat Organization • Special Operations Command South • U.S. Army Warrant Officer Career College • U.S. Army Cyber School • Combat Training Center	**Technical Positions** • Electromagnetic Warfare Technician • Electromagnetic Warfare Technical Advisor • ASCC CCWO **Broadening Positions** • Cyber CWOB **Assignments:** • U.S. Army Warrant Officer Career College • Army Futures Command • Theater Fires Element

Figure 8: 170B AC Warrant Officer Career Timeline

(4) 170B Electromagnetic Warfare Technician Reserve Component Warrant Officer Development.

(a) General career development. RC warrant officer (USAR and ARNG) development objectives and qualifications parallel those of their AC counterparts.

(b) Branch development opportunities. Even though geographical considerations limit some RC warrant officers, all should strive for operational Electromagnetic warfare technical assignments that yield the same developmental opportunities as their AC counterparts.

(c) Training and development. Required training and recommended branch developmental assignments by grade are as follows:

1. Warrant Officer One. Must complete WOCS and WOBC before promotions to CW2. Assignments include EW technical advisor and team chief. WO1 positions concentrate in brigade-level MTOE organizations.

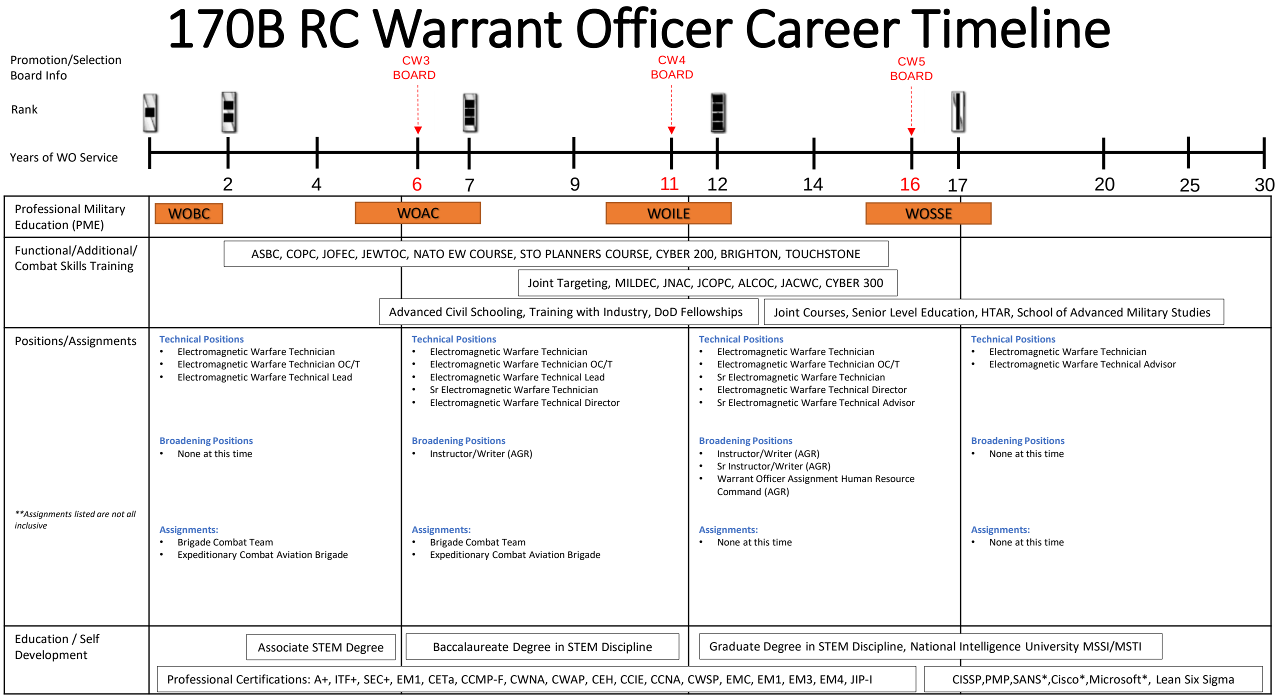
2. Chief Warrant Officer Two. Warrant officers with at least one year in grade as a CW2 can attend but must complete WOAC before promoting CW3. Assignments include technical advisor, team chief, section

chief, and platoon leader. CW2 positions concentrate in brigade-level MTOE organizations.

3. Chief Warrant Officer Three. Warrant officers with at least one year in grade as a CW3 can attend but must complete WOILE before promoting CW4. Assignments include EW technical advisor, team chief platoon leader, and instructor. CW3 positions concentrate in brigade-level TDA organizations within the USAR and the ARNG.

4. Chief Warrant Officer Four. Warrant officers with at least one year in grade as a CW4 can attend but must complete WOSSE before promoting CW5. Assignments include senior EW technical advisor and instructor. CW4 positions concentrate in division-level TDA organizations within the USAR and ARNG.

5. Chief Warrant Officer Five. Must be assigned to authorized Cyber Branch CW5 positions. CW5 positions are key staff officer positions at major commands. CW5s advise commanders at all levels on doctrine, structure, assignments, and training.


170B RC Warrant Officer Career Timeline
Promotion/Selection Board Info
CW3 BOARD
CW4 BOARD
CW5 BOARD
Rank
Years of WO Service
2
4
6
7
9
11
12
14
16
17
20
25
30
Professional Military Education (PME)
WOBC
WOAC
WOILE
WOSSE
Functional/Additional/ Combat Skills Training

ASBC, COPC, JOFEC, JEWTOC, NATO EW COURSE, STO PLANNERS COURSE, CYBER 200, BRIGHTON, TOUCHSTONE

Joint Targeting, MILDEC, JNAC, JCOPC, ALCOC, JACWC, CYBER 300

Advanced Civil Schooling, Training with Industry, DoD Fellowships

Joint Courses, Senior Level Education, HTAR, School of Advanced Military Studies

Positions/Assignments				
***Assignments listed are not all inclusive*	**Technical Positions** • Electromagnetic Warfare Technician • Electromagnetic Warfare Technician OC/T • Electromagnetic Warfare Technical Lead **Broadening Positions** • None at this time **Assignments:** • Brigade Combat Team • Expeditionary Combat Aviation Brigade	**Technical Positions** • Electromagnetic Warfare Technician • Electromagnetic Warfare Technician OC/T • Electromagnetic Warfare Technical Lead • Sr Electromagnetic Warfare Technician • Electromagnetic Warfare Technical Director **Broadening Positions** • Instructor/Writer (AGR) **Assignments:** • Brigade Combat Team • Expeditionary Combat Aviation Brigade	**Technical Positions** • Electromagnetic Warfare Technician • Electromagnetic Warfare Technician OC/T • Sr Electromagnetic Warfare Technician • Electromagnetic Warfare Technical Director • Sr Electromagnetic Warfare Technical Advisor **Broadening Positions** • Instructor/Writer (AGR) • Sr Instructor/Writer (AGR) • Warrant Officer Assignment Human Resource Command (AGR) **Assignments:** • None at this time	**Technical Positions** • Electromagnetic Warfare Technician • Electromagnetic Warfare Technical Advisor **Broadening Positions** • None at this time **Assignments:** • None at this time

Education / Self Development

Associate STEM Degree

Baccalaureate Degree in STEM Discipline

Graduate Degree in STEM Discipline, National Intelligence University MSSI/MSTI

Professional Certifications: A+, ITF+, SEC+, EM1, CETa, CCMP-F, CWNA, CWAP, CEH, CCIE, CCNA, CWSP, EMC, EM1, EM3, EM4, JIP-I

CISSP,PMP,SANS*,Cisco*,Microsoft*, Lean Six Sigma

Figure 9: 170B RC Warrant Officer Career Timeline

(5) 170D Cyber Capabilities Developer Technician Active Component Warrant Officer development.

(a) Characteristics required of Cyber Capabilities Developer Technician. Cyber Capabilities Developer Technicians develop and implement software and hardware capabilities that support offensive and defensive Cyberspace operations. Their software and hardware solutions help accomplish unit objectives. They provide technical guidance, expertise, and advice to commanders and their staff on developing and implementing capabilities that support Army and JIIM Cyberspace operations. They must be consummate professionals, self-motivated and self-disciplined. They must maintain a current TOP SECRET (TS) Sensitive Compartmented Information (SCI) clearance to maintain the MOS. Additionally, Cyber Capabilities Developer Technicians must pass a counterintelligence scope polygraph (CSP) to hold the MOS. Soldiers who refuse to take or fail a CSP will reclassify.

(b) Unique knowledge and skills of a Cyber Capabilities Developer Technician. The Cyber Capabilities Developer Technician is a Subject Matter Expert (SME) on developing and implementing software and hardware capabilities and is a leader, trainer, and advisor to commanders at all levels. The Cyber Capabilities Developer Technician is a versatile, highly trained individual responsible for analyzing system vulnerabilities, product research, capability development, documentation, and implementation of software and hardware capabilities that operate in and through cyberspace and serve as a force multiplier for maneuver forces. The Cyber Capabilities Developer Technician advances in skills and abilities as they progress through their careers. They are required to stay current with technology and maintain their proficiency in their skill set. Cyber Officers, Cyber Capabilities Developer Technicians must operate without direct oversight or guidance, be self-motivated, and provide timely and effective technical products and solutions. Cyber Capabilities Developer Technicians do not have an enlisted feeder MOS. Accessions are open to all Army and sister-service MOSs and non-military personnel (civilians) from all civilian sectors. Cyber Capabilities Developer Technicians perform the following functions/tasks:

1. Analysis of system vulnerabilities.
2. Software and hardware capability research.
3. Software and hardware capability development and documentation.
4. Software and hardware capability implementation.

(c) Assignments: Cyber Capabilities Developer Technicians are primarily assigned to units specifically conducting offensive and defensive Cyberspace operations. These assignments provide extensive exposure to operations in and through the Cyberspace domain in support of multi-domain battles. Select warrant officers can also expect to receive assignments that broaden their experience as Cyber Capabilities Developer Technicians and may serve in a generating force capacity such as the following:

1. WOBC/WOAC Instructor
2. Training/Course Developer
3. TRADOC Capability Manager
4. TRADOC Deputy Technical Director

(d) Military Oriented Training: In addition to Professional Military Education, military-orientated training for all Cyber Capabilities Developer Technician warrant officers can include:

1. Computer Network Operations Development Program (CNODP)
2. Advanced Civil Schooling
3. Training with Industry
4. Army and DoD Fellowships

(e) Self-development. Lifelong learning, supported by civilian STEM degree programs, military education, and Training with Industry, provides opportunities to develop competencies throughout the warrant officer's career. Assignment-oriented, joint training courses, and advanced civil schooling are needed to develop characteristics required of a senior Cyber Capabilities Developer Technician.

(f) WO1/CW2 development.

1. Entry level. Upon warrant officer selection, all non-commissioned officers (warrant officer candidates upon arrival) will complete Warrant Officer Candidate School (WOCS). WOCS provides the basic skills necessary to prepare the warrant officer candidate to become an effective Army warrant officer.

2. Education. After graduation from WOCS and appointment to WO1, each warrant officer will attend the 72-week Warrant Officer Basic Course (WOBC) at Fort Gordon, GA. The 170D Cyber Capabilities Developer Technician Basic Course provides Cyber Capabilities Developer Technicians with the education, training, and core skills necessary to develop software and hardware capabilities that successfully support Cyberspace operations. The training emphasizes developing and implementing capabilities to prepare the warrant officers to support authorized Cyber effects. Company grade warrant officers need to develop a basic understanding of technical integration of Cyberspace Defense, Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR), Cyberspace Surveillance and Reconnaissance (S&R) Cyberspace Operational Preparation of the Environment (OPE), and Cyberspace Attack in support of multi-domain operations. Completing an associate's or baccalaureate degree is a recommended goal before becoming eligible for promotion to CW3.

3. Desired experience. Junior Cyber Capabilities Developer Technicians must attain and maintain basic-level certification as a capabilities developers. Continuous education, training, and experience in developing and integrating capabilities that support Cyberspace operations prepare the junior 170D warrant officer for future assignments and selection to CW3. A Basic-level Cyber Capabilities Developer Technician is proficient in the C and Python programming languages at an intermediate level and has a basic-level understanding of data structures, algorithms, object-oriented programming, secure design, operating systems, x86 assembly, and SQL. A Basic-level Cyber Capabilities Developer Technician is responsible for completing assigned tasks and modules with guidance and supervision from a Senior or Master Basic-level Cyber Capabilities Developer Technician to create a capability in support of operational requirements.

(g) CW3 development.

1. Education. The 170D Warrant Officer Advanced Course (WOAC) focuses on advanced technical training and common leader development subjects designed to prepare officers for Field Grade Cyber Capabilities Developer Technician positions. At the Army Cyber School at Fort Gordon, GA, the residential course consists of 14-weeks of advanced technical and tactical training in software and hardware capability development. Additionally, CW3s should complete WOAC before promoting CW4 and must complete before assignment to a broadening, nominative, or specialty billet. Completing a baccalaureate or master's degree in a related STEM discipline is also a recommended goal before becoming eligible for promotion to CW4.

2. Desired experience. A CW3 Cyber Capabilities Developer Technician must have Senior-level expertise within a specialized focus area and is responsible for the direction of a project within this specialty.

The specialty areas are Unix access capabilities; Windows access capabilities; RF access capabilities; network architecture and applications; Unix persistence capabilities; Windows persistence capabilities; embedded capabilities; and other (e.g., data science and machine learning). The access specialties involve reverse engineering software and hardware to identify vulnerabilities and craft exploits for those vulnerabilities. Thus these specialties make use of platform-specific reverse engineering and low-level programming. The persistence specialties aim to use provided access to install software that allows Cyberspace operators persistent access and convenient control of a targeted system. These specialties involve a deep understanding of a platform along with technical stealth and tradecraft. The Unix specialties might further specialize in iOS or Android. A Senior-level Cyber Capabilities Developer Technician also provides oversight and direction to Basic-level Cyber Capabilities Developer Technician working under their tutelage. They are also responsible for decomposing projects into components assigned to Basic-level Cyber Capabilities Developer Technician. Before becoming a CW4, a CW3 must master the functions above.

(h) CW4 development.

1. Education. The Warrant Officer Intermediate Level Education (WOILE) is a professional development course with a two-week Phase one distance learning (DL) portion, followed by a five-week resident Phase two portion taught at the Warrant Officer Career Center (WOCC), Fort Rucker, AL and a final five-week Phase three taught at the Cyber School, Fort Gordon, GA. WOILE provides intermediate-level professional military education and leader development (PME- LD) training that prepares Field Grade warrant officers (CW3/CW4) to function as Master-level Cyber Capabilities Developers, trainers, managers, systems integrators, and leaders at various levels of Army and JIIM organizations. CW4s should complete WOILE by the one-year time-in-grade point. Additionally, CW4 should complete WOILE for promotion to CW5 and must be complete before assignment to CW4 broadening, nominative, or specialty billet. Completing a master's degree in a related STEM discipline is a highly desired goal before becoming eligible for promotion to CW5.

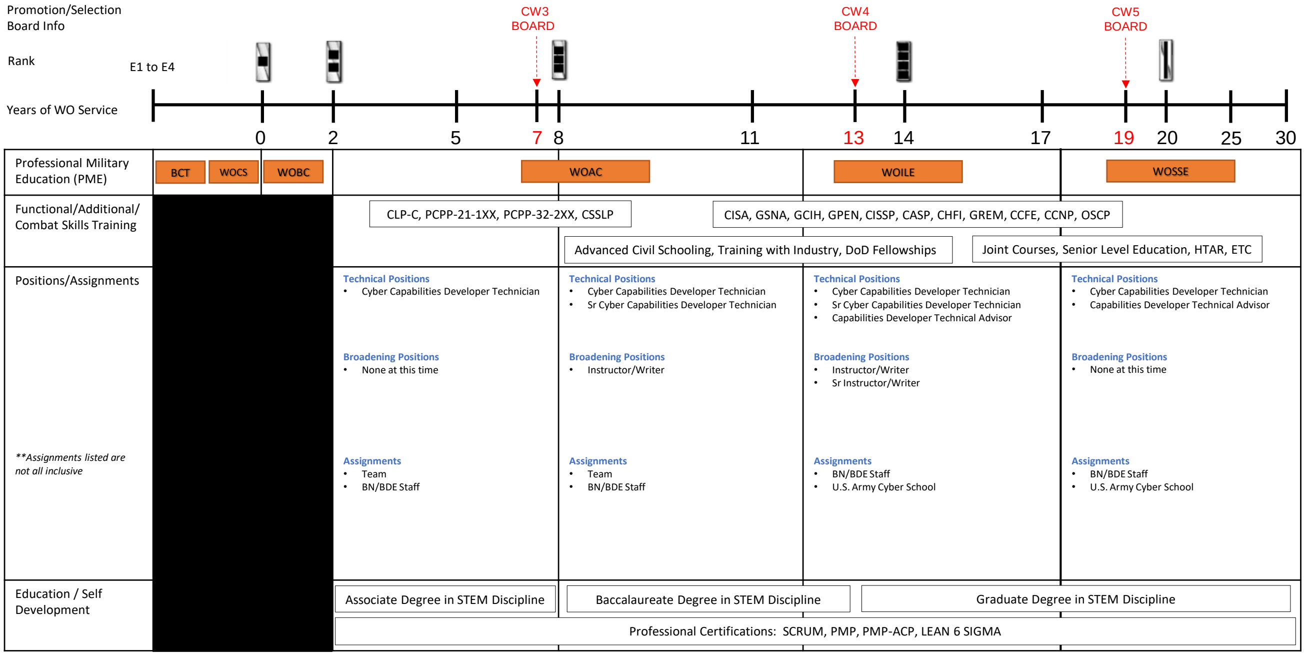
2. Desired experience. A CW4 Cyber Capabilities Developer Technician has mastered their specialty and is responsible for providing guidance and technical direction over multiple projects in this specialty. Additionally, they mentor Senior-level Cyber Capabilities Developer Technicians as they progress to the Master-level. Master Cyber Capabilities Developer Technicians provide the highest level of technical insight during the design of new software and hardware capabilities.

(i) CW5 development.

1. Education. The Warrant Officer Senior Service Education (WOSSE) is a two-phase course consisting of a Phase one (DL) portion followed by a four-week Phase two (resident) portion attended by the Army's most senior warrant officers. The educational goal is to provide senior CW4s new CW5s with the master-level education, knowledge, and influential leadership skills necessary to apply their technical expertise to support Army and strategic-level joint staff leaders during multi-domain operations. CW5s should attend WOSSE by the one-year time-in-grade point. CW5s must complete before assignment to a Command Chief Warrant Officer billet. Additionally, CW5s should continue work in an associated graduate-level field of study.

2. Desired experience. All CW5 Cyber Capabilities Developer Technician should have software and hardware operational experience in support of both OCO and DCO at all levels and have attained proficiency of all critical tasks through combined experiences and career self-development in every aspect of their career path.

170D AC Warrant Officer Career Timeline



Professional Military Education (PME)	BCT WOCS WOBC	WOAC	WOILE	WOSSE
Functional/Additional/ Combat Skills Training		CLP-C, PCPP-21-1XX, PCPP-32-2XX, CSSLP Advanced Civil Schooling, Training with Industry, DoD Fellowships	CISA, GSNA, GCIH, GPEN, CISSP, CASP, CHFI, GREM, CCFE, CCNP, OSCP	Joint Courses, Senior Level Education, HTAR, ETC
Positions/Assignments ***Assignments listed are not all inclusive*		**Technical Positions** • Cyber Capabilities Developer Technician **Broadening Positions** • None at this time **Assignments** • Team • BN/BDE Staff	**Technical Positions** • Cyber Capabilities Developer Technician • Sr Cyber Capabilities Developer Technician **Broadening Positions** • Instructor/Writer **Assignments** • Team • BN/BDE Staff	**Technical Positions** • Cyber Capabilities Developer Technician • Sr Cyber Capabilities Developer Technician • Capabilities Developer Technical Advisor **Broadening Positions** • Instructor/Writer • Sr Instructor/Writer **Assignments** • BN/BDE Staff • U.S. Army Cyber School
				Technical Positions • Cyber Capabilities Developer Technician • Capabilities Developer Technical Advisor **Broadening Positions** • None at this time **Assignments** • BN/BDE Staff • U.S. Army Cyber School
Education / Self Development		Associate Degree in STEM Discipline	Baccalaureate Degree in STEM Discipline	Graduate Degree in STEM Discipline
		Professional Certifications: SCRUM, PMP, PMP-ACP, LEAN 6 SIGMA		

Figure 10: 170D AC Warrant Officer Career Timeline