Cyber Branch

A. Introduction

1. **Purpose of the Cyber Branch.** The Cyber Branch executes dynamic real-world operations to enable global force projection through sensing and understanding the information dimension, engineering and integrating exquisite capabilities, and gaining advantages in technological and data-centric environments. To achieve its mission objectives, the Cyber Branch engages the enemy in and through the cyberspace domain and electromagnetic spectrum to deny, degrade, disrupt, destroy, or manipulate their capabilities while ensuring freedom of maneuver for friendly forces. Cyber Officers lead, plan, integrate, synchronize, and execute offensive and defensive cyberspace operations, electromagnetic warfare, and cyberspace electromagnetic activities at all echelons to support multidomain operations (MDO) and large-scale combat operations (LSCO) by creating windows of relative advantage in the warfighting domains and dimensions. Cyberspace Operations (CO) are the employment of cyber capabilities with the primary purpose of achieving objectives in or through the cyberspace domain. 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) is military action using electromagnetic and directed energy to control the electromagnetic spectrum or combat the enemy. EW includes electromagnetic attack, electromagnetic protection, and electromagnetic support. Cyberspace Electromagnetic Activities (CEMA) focus on the planning, integration, and synchronization of CO and EW as part of the combat arms approach through the operations process.

2. **Proponent information.** Commandant and Chief of Cyber, U.S. Army Cyber School, Fort Eisenhower, GA 30905. For more information, contact the Officer Division, Office of the Chief of Cyber at: usarmy.eisenhower.cyber-coe.mbx.occ-officers@army.mil.

3. **Functions.** Cyber Officers develop expertise to project power in and through cyberspace and the electromagnetic spectrum, as well as understand their roles within competition, crisis, and conflict. Cyber Officers must understand LSCO to ensure synchronized, relevant, and integrated effects to enable success in ever-changing strategic, operational, and tactical environments. The Cyber Warfare Officer leads, plans, integrates, synchronizes, and executes CO through the employment of Cyber Mission Forces (CMF) and other cyber units. The Cyber Electromagnetic Warfare Officer (CEWO) is the combatant commander's subject matter expert for leading, planning, integrating, synchronizing, and executing CO, EW, and CEMA; understands electromagnetic spectrum operations (EMSO); and is a key contributor to spectrum management operations (SMO). The Cyber Capability Development Officer (CCDO) leads the development and delivery of cyberspace capabilities to enable CO and EW missions. Cyber Officers serve in Army, joint, interagency, intergovernmental, and multinational (JIIM) positions, performing the following functions and tasks:

(a) Execute mission command of CO, EW, and CEMA units, elements, and sections.

(b) Integrate CO, EW, and CEMA capabilities into MDO and LSCO.

(c) Plan multi-faceted CO and EW missions and campaigns against adversaries.

(d) Develop and deliver software and hardware CO and EW capabilities and solutions.

(e) Develop doctrine, organizational structures, and equipment for CO and EW missions and

units.
(f) Serve in staff positions and organizations requiring CO, EW, and CEMA expertise.

(g) Understand EMSO and provide key contributions to SMO.

4. **Branch eligibility.** For Cyber Branch eligibility requirements, review DA Pamphlet 611-21, Chapter 3, Section 3-17. Officers of other branches who desire to transfer into the Cyber Branch should submit a request in accordance with AR 614-100, Chapter 4, and U.S. Army Human Resources Command's most recent Voluntary Transfer Incentive Program (VTIP) MILPER message and instructions. Reserve Component officers must follow the branch transfer policies and procedures for their Component.

5. **Cyber Course Credit Program.** Cyber Officers who acquire the requisite CO or EW knowledge, skills, and behaviors through education, training, certification, or experience may apply for course credit for U.S. Army Cyber School governed area of concentration (AOC) qualification courses and modules. The Cyber Course Credit Program is managed by the U.S. Army Cyber School IAW AR 350-1 and the current Cyber Course Credit Program Standard Operating Procedures for the evaluation and awarding of constructive, equivalent, and operational credit for select cyber courses and modules. The approval authority for awarding 17A, 17B, or 17D AOC qualification course credit (not including credit for the Army-mandated portions of PME, such as common core) 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, and when appropriate, may be combined with documentation of course completion of Army-mandated PME portions to achieve PME completion. Cyber Officers who believe they meet course credit criteria for an entire PME course, including the Army-mandated portions, may apply for full PME credit to the TRADOC Director of Training, G-37/TR, as delegated by the HQDA DCS G-3/5/7 IAW AR 350-1, Paragraph 3-20.

B. Officer Characteristics Required

1. **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 Department of the Army Civilians, who create CO and EW effects against the enemy while protecting friendly forces from the same. They must understand all aspects of CO, EW, and CEMA along with combined arms tactics, techniques, and procedures to support MDO and LSCO. They must be mentally and physically disciplined, possessing both intrapersonal and interpersonal skills to enable them to perform as agile, adaptive, and innovative officers in all situations.

2. **Characteristics required of all officers.** Cyber Officers are selected and relied upon for their leadership potential and abilities; technical aptitude and knowledge; ethics and moral courage; and resilience. The Cyber Branch values inspirational leaders within its ranks, who possess relevant education and are logical, analytical, innovative, technologically adept problem solvers. Cyber Officers are agile, adaptive, self-motivated, and able to operate without direct supervision. They are trained and educated to perform their essential duties of leading, planning, integrating, synchronizing, executing, and assessing CO, EW, and CEMA, as well as developing and delivering technical capabilities and solutions.

3. **Unique knowledge and skills of a Cyber Officer.** Cyber Officers must possess the following

knowledge and skills:

(a) Breadth of knowledge of the cyberspace domain, electromagnetic spectrum, and DODIN, including associated laws, policies, regulations, capabilities, and technologies.

(b) Strong leadership attributes and competencies required to effectively lead in Army and JIIM environments.

(c) Understanding of and ability to execute MDMP/JPP staff processes to employ CO, EW, and CEMA actions and assets to support combatant commanders and contribute to MDO and LSCO.

(d) Conduct CEMA to support combat operations and national defense in both classified and unclassified environments.

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

(f) Identify and refine the development of CO and EW capabilities and technical solutions.

4. **Unique attributes for Cyber Officers.** The Cyber Branch requires dynamic, competent, well-trained leaders at all echelons who understand MDO and LSCO to effectively lead, plan, integrate, synchronize, and execute CO, EW, and CEMA. Cyber Officers must also be technologically adept, innovative, logical, analytical problem solvers and inspirational leaders, possessing the following attributes:

(a) Systems thinking and logical intelligence. Cyber Officers must link technologies and capabilities with complex mission variables and assess their impacts on military operations. This includes understanding the nuances between the three cyberspace domain layers (physical, logical, and cyber-persona) and their interrelationship with the land, air, maritime, and space domains. They must also be capable of assessing friendly and adversary capabilities regarding processes, components, functionalities, dependencies, and interactions through which the whole system accomplishes a function.

(b) Multi-echelon and multidomain collaboration. Cyber Officers must be effective and efficient in multi- echelon and multidomain collaboration. Leading, planning, integrating, synchronizing, and executing CO, EW, and CEMA often affects multiple services, agencies, domains, and dimensions, which requires strong collaborative skills.

(c) 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, EW, and CEMA capabilities, effects, and functions.

(d) Innovative and adaptive mindset. Cyber Officers must be ready to provide CO, EW, and CEMA capabilities, effects, and functions anywhere in the world in an innovative and adaptive manner for either short or long durations. This includes Army and JIIM assets that must be integrated and synchronized during MDO and LSCO.

(e) Intellectual curiosity. Cyber Officers must be self-motivated as continuous learners, who explore the breadth and depth of knowledge regarding the cyberspace domain, electromagnetic spectrum, and related technological fields.

C. Cyber Branch Officer Development

1. **Cyber Officer development – areas of concentration.** Cyber Officers receive training and education for AOCs 17A, 17B, and/or 17D. Experience in a variety of CO, EW, and CEMA assignments at Army and JIIM echelons is essential for Cyber Officer development. Permeability between the 17-series AOCs is highly encouraged to develop well-rounded and adaptable leaders in the branch. Although highly technical skills are valued for Cyber Officers, strong performance in a range of Army and JIIM assignments will maximize their promotion potential. Additionally, successful service in key developmental positions for any 17-series AOC (minimum of 18 months) is essential and 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 (minimum of 18 months), key developmental credit may be awarded for their current rank/grade. Prior to attending the 17B CEWO Qualification Course, Cyber Officers (starting at lieutenant) must first be qualified as AOC 17A. Cyber Officers 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. However, 17D officers may also have opportunities to serve in 17A or 17B positions. 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.

(a) Cyber Warfare Officer (17A). Duties include leading, directing, managing, planning, integrating, synchronizing, and/or executing CO and CEMA at all Army and JIIM echelons. The 17A is well-versed in the 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 intelligence preparation of the operational environment; cyberspace attack; and cyberspace security. Cyber Warfare Officers deliver effects in and through cyberspace, manifesting in cyberspace or one or more of the warfighting domains and dimensions, which 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, and across the other domains and dimensions. 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, LSCO, and the competition continuum.

(b) Cyber Electromagnetic Warfare Officer (17B). Duties include leading, directing, managing, planning, integrating, synchronizing, and/or executing CO, EW, and CEMA at all Army and JIIM echelons. The 17B is adept in the tactics, techniques, and procedures for coordinating CO, EW, and CEMA missions, with an emphasis on electromagnetic attack, electromagnetic protection, and electromagnetic support. CEWOs develop expertise in EW with a solid understanding of EMSO. CEWOs deliver effects in and through the EMS, cyberspace, and other domains and dimensions designed to deny, degrade, disrupt, destroy, or manipulate adversary activities or operations. The 17B plans, integrates, and synchronizes CO, EW, and CEMA with actions to enable commanders to mass effects and gain and maintain positions of relative advantage in the EMS, cyberspace, and across the other domains and dimensions. CEWOs command, lead, direct, and manage CO, EW, and CEMA units, elements, and sections, and contribute to the success of SMO. The 17B also understands friendly and adversary cyberspace and EMS capabilities, objectives, organizations, and operations, as well as the broader aspects of MDO, LSCO, and the competition continuum.

(c) Cyber Capability Development Officer (17D). Duties include leading, directing, managing, planning, integrating, synchronizing, and/or executing capability development to support CO and EW missions. The 17D is skilled in designing, developing, and delivering relevant, timely, and effective software, hardware, radio frequency, and other technical solutions. The CCDO serves as a developer within a development element or associated organization at any echelon. The 17D also understands friendly and adversary cyberspace and EMS capabilities, objectives, organizations, and/or operations, as well as the broader aspects of MDO, LSCO, and the competition continuum to perform robust cyber capabilities development efforts.

2. **Lieutenant development.** The professional development objective for a lieutenant is to learn and use Cyber Branch knowledge, skills, and behaviors to successfully serve as a platoon leader, section/element crew lead, and executive or staff officer. Success for some lieutenants is serving as a basic developer, analytic support officer, interactive operator, or exploitation analyst. The primary focus for the Cyber lieutenant is leading, planning, and executing CO or EW missions through the application of their technical and tactical acumen.

(a) Education. After commissioning, most Cyber lieutenants will attend Cyber Basic Officer Leader Course (CyBOLC) for AOC 17A, while some will be identified to attend 17D CCDO BOLC instead. Selected lieutenants will also attend the AOC 17B CEWO Qualification Course, following successful completion of AOC 17A CyBOLC. 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 (BOLC- A), followed by the Cyber Direct Commission BOLC (BOLC-B), unless granted an exception to policy/waiver by the appropriate Army authority IAW AR 350-1 and other applicable guidance.

(b) Developmental assignments. Cyber lieutenants will serve in leadership and operational positions for company-grade officer development. 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 Section/Element/Crew Lead Analytic Support Officer Interactive Operator Exploitation Analyst	Company XO Platoon Leader Section/Element/Crew Lead	Company XO Platoon Leader Section/Element/Crew Lead Basic Developer

(c) Self-development. Cyber lieutenants should focus on CO and EW fundamentals; small unit tactics; troop leading procedures; unit-specific functional training; CMF work role qualifications; verbal and written communication skills; logistics and basic administrative activities; fundamentals of training management; and other tactical and technical proficiency skills.

(d) Desired experience. Cyber lieutenants should primarily gain experience from serving in one or more leadership positions in the operational force following BOLC graduation. Some lieutenants may serve in highly technical work roles to utilize specific training or skills, while others may be assigned to staff positions for broader development.

3. **Captain development.** The professional development objective for a captain is to expand their leadership skills; CO, EW, and CEMA knowledge; and use of planning processes to serve

successfully as a company commander, team/element/section lead, or staff officer. The primary focus of the Cyber captain is to solidify their technical and tactical knowledge by pursuing a diverse range of assignments in Army and JIIM environments. This allows captains to gain understanding of warfighting and combined arms maneuver.

(a) Education. Military education required during this phase is the completion of the Cyber Captains Career Course (CCC).

1) Cyber captains must attend the Cyber CCC, which should occur as close to promotion to captain as possible but not later than their seventh year of federal commissioned service.

2) Cyber Officers directly appointed in the rank of captain through the CDCP are required to attend the Army's Direct Commission Course (BOLC-A), followed by the Cyber Direct Commission BOLC (BOLC-B), unless granted an exception to policy/waiver by the appropriate Army authority IAW AR 350-1 and other applicable guidance. Cyber Officers directly appointed in the rank of captain through the CDCP are required to attend 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 Cyber CCC attendance requirement to optimize initial mission-focused assignments and individual promotion opportunities/timelines.

3) Select Cyber captains may develop mastery of technologies and technical skillsets used in the cyberspace domain or EMS through specialized training designed or designated by the U.S. Army Cyber Center of Excellence, U.S. Army Cyber Command, or U.S. Cyber Command.

(b) AOC 17B qualification. Cyber captains filling AOC 17B positions 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 Cyber CCC.

(c) VTIP. Captains transferring into the Cyber Branch must attend the Cyber Warfare Officer Transition Course for AOC 17A. If designated for AOC 17B, VTIP captains must complete both the 17A Cyber Warfare Officer Transition Course and the 17B CEWO Qualification Course. Those VTIP captains who have not already completed CCC must also complete Cyber CCC.

(d) Assignments. Cyber captains will serve in key developmental and developmental assignments for career progression and professional development. Broadening opportunities may provide a wider range of knowledge and skills.

1) Key developmental assignments provide Cyber captains with the desired operational experience in small unit leadership focused on CO, EW, and CEMA at this developmental phase. Key developmental assignments 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. Cyber captains are encouraged to pursue key developmental positions across all 17-series AOCs to demonstrate their ability to lead in Army and JIIM environments. Completion of a key developmental assignment for any Cyber AOC counts as key developmental credit for all Cyber AOCs in their current rank/grade. 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 Lead Mission Element/Section Lead Analytic Support Officer CEWO	Company Commander CEWO Support Team Lead Mission Element/Section Lead Analytic Support Officer	Company Commander Development Section Lead Support Team Lead Senior Developer

2) 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 Prgm Mgr (OCC) (post-KD) Cyber OC/T (CTCs) (post-KD) Instructor (post-KD) Research Scientist (ACI) (post-KD) Assistant S3 (BN/BDE) AROC Officer Battle Captain (JOC) Mission Manager (JOC) Watch Officer (JOC) Branch Chief (OCO/DCO/DODIN) Cyber/CEMA Planner Special Tech Ops (STO) Planner Effects Assessment Officer Remote Operations OIC CMF TF CuOps Officer Training/Exercises Officer	Career Prgm Mgr (post-KD) Cyber OC/T (CTCs) (post-KD) Instructor (post-KD) Research Scientist (post-KD) Assistant S3 (BN/BDE) Cyber/CEMA Planner STO Planner	Career Prgm Mgr (post-KD) Instructor (post-KD) Research Scientist (post-KD) Assistant S3 (BN/BDE) Battle Captain (JOC) Branch Chief Product Engineer STO Engineer

3) Broadening opportunities available for captains include but are not limited to:

a) Advanced Civil Schooling.
b) Training with Industry.
c) DoD or interagency fellowships/internships.

4) Self-development. Cyber captains should continue to gain an increased understanding of CO, EW, and CEMA, as well as enhancing their technical prowess and tactical proficiency. 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 battalion, brigade, or division. Captains are encouraged to pursue graduate-level education in a

science, technology, engineering, or math (STEM) discipline and obtain technical certifications related to information technology, networking, CO, cybersecurity, programming, and other related disciplines.

5) Desired experience. Cyber captains should primarily gain experience from serving as a company commander, team/element/section lead, unit CEWO, senior developer, or staff officer in Army and JIIM environments. Captains will hone their knowledge, skills, and behaviors through challenging key developmental and developmental assignments to prepare for promotion to major.

4. **Major development.** The professional development objectives for a major are to further expand and broaden the officer's tactical and technical experience and expertise with CO, EW, and CEMA at all echelons. Cyber majors should focus on developing organizational leadership, management, and planning skills through a series of key developmental and developmental assignments.

(a) Education. 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).

1) The Army conducts ILE selection boards in conjunction with the Major Army Competitive Category 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, National Intelligence University, 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 HQDA G-3. Majors may also compete to be selected for the School of Advanced Military Studies (SAMS), when eligible.

2) Cyber Officers directly appointed in the rank of major through the CDCP are required to attend the Army's Direct Commission Course (BOLC-A), followed by the Cyber Direct Commission BOLC (BOLC- B), unless granted an exception to policy/waiver by the appropriate Army authority IAW AR 350-1 and other applicable guidance. 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 to optimize initial mission-focused assignments and individual promotion opportunities/timelines. All Cyber Officers directly appointed as majors are exempt from captain PME requirements.

3) Select Cyber majors may develop mastery of technologies and technical skillsets used in the cyberspace domain or EMS through specialized training designed or designated by the U.S. Army Cyber Center of Excellence, U.S. Army Cyber Command, or U.S. Cyber Command.

(b) AOC 17B qualification. Cyber majors filling AOC 17B positions must complete the 17B CEWO Qualification Course (if not already 17B AOC-qualified) prior to reporting for their 17B assignment.

(c) VTIP. Majors transferring into the Cyber Branch must attend the Cyber Warfare Officer Transition Course for AOC 17A. If designated for AOC 17B, VTIP majors must complete both the

17A Cyber Warfare Officer Transition Course and the 17B CEWO Qualification Course.

(d) Assignments. Cyber majors will serve in key developmental and developmental assignments for career progression and professional development. Broadening opportunities may provide a wider range of knowledge and skills.

1) Key developmental assignments provide Cyber majors with increased experience and expertise in leading, managing, and executing CO, EW, and CEMA at higher echelons. These assignments provide a credible developmental experience in the core skillsets required of future battalion commanders, Command Selection List (CSL) key billets, Army and JIIM staff officers. Cyber majors must serve in key developmental positions for a minimum of 18 months. Cyber majors are encouraged to pursue key developmental positions across all 17-series AOCs to demonstrate their ability to lead in Army and JIIM environments. Completion of a key developmental assignment for any Cyber AOC counts as key developmental credit for all Cyber AOCs in their current rank/grade. Additionally, Cyber majors serving in key developmental positions for lieutenant colonel 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)
Commander (TRP/DET) Battalion XO Battalion S3 Mission/Support Team Lead CEWO Senior OC/T (CTC/MCTP) BDE Analytic Support Officer BDE Technical Director	Commander (TRP/DET) Battalion XO Battalion S3 CEWO Mission/Support Team Lead Senior OC/T (CTC/MCTP) BDE Analytic Support Officer BDE Technical Director	Commander (TRP/DET) Battalion XO Battalion S3 Development Site/Team Lead Mission/Support Team Lead BDE Technical Director Master Developer

2) 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)
Career Manager (HRC)(post-KD) Career Prgm Mgr(OCC)(post-KD) College Director (post-KD) Instructor (post-KD) Research Scientist (post-KD) Army Remote Ops Ctr Officer Battle Watch Chief (JOC)	Career Manager (post-KD) Career Prgm Mgr (post-KD) College Director (post-KD) Instructor (post-KD) Research Scientist (post-KD) BDE Assistant S3 Branch/Division Chief Course Manager (CySch)	Career Manager (post-KD) Career Prgm Mgr (post-KD) College Director (post-KD) Instructor (post-KD) Research Scientist (post-KD) BDE Assistant S3 Branch/Division Chief Course Manager (CySch)

Senior Fires Officer (JOC) Joint Plans Analyst (JOC) Watch Officer (JOC) BDE Assistant S3 Branch/Division Chief Course Manager (CySch) Cyber Integration Lead(JFHQ-CY) Cyber Ops Chief (JFHQ-CY) Cyber/CEMA Planner Mission Manager Master Developer OC/T (CTC/MCTP) Strategy/Policy Planner SAMS Planner Army/Joint Staff Officer	Cyber/CEMA Planner Cyber/EW Integrator (CCoE) EW Operations Planner (JEWC) SAMS Planner Army/Joint Staff Officer	Cyber Integration Lead OC/T (CTC) R&D Ops Lead (ACI/TWC) Senior Fires Officer (JOC) SAMS Planner Army/Joint Staff Officer

3) Broadening opportunities available for majors include but are not limited to:

a) Advanced Civil Schooling (ACS).
b) Training with Industry (TWI).
c) DoD and interagency fellowships/internships.

(e) Self-development. Cyber majors should continue efforts to gain expertise in all aspects of CO, EW, and CEMA, as well as acquiring expertise in organizational leadership. Majors must work to expand their knowledge and skills to serve effectively at the CMF team, battalion, brigade, Army, and JIIM levels. Majors are encouraged to hold or pursue a graduate degree in a STEM discipline and obtain technical certifications related to information technology, networking, CO, cybersecurity, programming, and other relevant disciplines.

(f) Desired experience. Cyber majors should gain expertise by serving in key developmental leadership and staff positions, while building upon their knowledge and skills to prepare for battalion commander. When feasible, broadening opportunities will provide majors a wider range of knowledge and skills.

5. **Lieutenant colonel development.** The professional development objective for a lieutenant colonel is to achieve and demonstrate excellence in tactical and technical knowledge and skills. Cyber lieutenant colonels should lead, train, motivate, and care for Soldiers while in command and staff environments. They are also encouraged to compete for CSL positions.

(a) Education.

1) Lieutenant colonels selected to command will also attend a pre-command course and those selected for Joint assignments must complete JPME II training. 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. Other senior leader and executive

courses will be considered to enhance leadership within CO and EW operational units and CEMA-focused elements.

2) Cyber Officers directly appointed in the rank of lieutenant colonel through the CDCP are required to attend the Army's Direct Commission Course (BOLC-A), followed by the Cyber Direct Commission BOLC (BOLC-B), unless granted an exception to policy/waiver by the appropriate Army authority IAW AR 350-1 and other applicable guidance. Cyber Officer directly appointed in the rank of lieutenant colonel are exempt from all other PME requirements for previous ranks/grades.

(b) VTIP. For lieutenant colonels who transfer into the Cyber Branch through VTIP, no Cyber School training is required; however, pending available seats, they may request to attend the Cyber Warfare Officer Transition Course, 17B CEWO Course, and/or Cyber School functional courses.

(c) Assignments. Cyber lieutenant colonels will serve in CSL, key developmental, and developmental assignments for career progression and professional development. Broadening opportunities may provide a wider range of knowledge and skills.

1) Key developmental assignments enable Cyber lieutenant colonels to gain mastery in leading CO, EW, and CEMA missions, as well as command and staff functions at all Army and JIIM echelons. Cyber lieutenant colonels should serve in one or more key developmental positions and are encouraged to pursue CSL opportunities. Completion of a key developmental assignment for any Cyber AOC counts as key developmental credit for all Cyber AOCs in their current rank/grade. Additionally, Cyber 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 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) CMF/CNMF TF CDR (CSL) BDE Deputy CDR (post-CSL) Division CEWO Brigade S3 Mission Team Lead	Battalion Commander (CSL) CMF/CNMF TF CDR (CSL) BDE Deputy CDR (post-CSL) Division CEWO Brigade S3 Mission Team Lead	Battalion Commander (CSL) CMF/CNMF TF CDR (CSL) BDE Deputy CDR (post-CSL) CSD Director Brigade S3 Mission Team Lead Tech Director (ASCC/CCMD) Master Developer

2) 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)
Assistant ACM Cyber/EW Battle Captain (JFHQ-CY) Chief, CTOC/ITOC Chief, Doctrine Branch (CCoE) Chief, ID Branch (HRC) Chief Research Scientist (ACI) Cyber Branch/Division Chief College Director (CySch) Corps/ASCC/CCMD CEWO Deputy Director (OCC) Instructor (CAC/USMA/USN) Joint Cyberspace Analyst (JCS) Joint/Army Staff Officer Mission Director (USCYBERCOM) SAMS Planner (pre-KD/CSL) Senior/Lead Cyber/CEMA Planner Senior Capability Analyst (IWOC) Senior OC/T (CTC) Senior Watch Officer (IWOC) Tech Director (USCYBERCOM) Training Integrator (CCoE) Army/Joint Staff Officer	Assistant ACM Cyber/EW CEMA Ops/Trng (FORSCOM) Chief, Capabilities Development Chief, ID Branch (HRC) Chief Research Scientist (ACI) College Director (CySch) Corps/ASCC/CCMD CEWO Deputy Director (OCC) Instructor (CAC/USMA/USN) Lead Army Analysis/Ops (JCER) J3 Branch Chief (DISA) Joint/Army Staff Officer SAMS Planner (pre-KD/CSL) Senior OC/T (CTC) Senior Trng Analyst (HQDA G3) Training Integrator (CCoE) Army/Joint Staff Officer	Assistant ACM Cyber/EW Chief, ID Branch (HRC) Chief, Doctrine Branch (CCoE) Chief Cyber Research (ACI) Cyber Branch/Division Chief Deputy Director (OCC) Instructor (CAC/USMA/USN) Joint/Army Staff Officer Mission Dir (USCYBERCOM) SAMS Planner (pre-KD/CSL) Army/Joint Staff Officer

3) Broadening opportunities available for lieutenant colonels include but are not limited to:

a) PhD program (e.g., Naval Postgraduate School or Air Force Institute of Technology).
b) Training with Industry (TWI).
c) DoD and interagency fellowships.
d) ACOM/HQDA/CCMD/JIM/DCS/SGS assignments.

(d) Self-development. Cyber lieutenant colonels not selected for resident SSC should enroll in nonresident SSC education. Lieutenant colonels are encouraged to hold or pursue advanced degrees in STEM fields relevant to CO, EW, and CEMA leadership positions. Educational self-development opportunities may include doctoral-level STEM programs at NPS, AFIT, or similar institutions. Lieutenant colonels should also continue developing mastery of CO, EW, and CEMA leadership at all Army and JIIM echelons through mentorship, self-study, education, training, and certifications.

(e) Desired experience. Cyber lieutenant colonels should achieve and demonstrate expertise in leading CO, EW, and CEMA at all echelons, primarily through CSL and key developmental assignments. When feasible, broadening opportunities will provide lieutenant colonels a wider range of knowledge and skills.

6. **Colonel development.** The professional development objective for a colonel is the sustainment of warfighting, training, and staff officer skills, along with the utilization of leadership, organizational, and executive talents. Cyber colonels are encouraged to compete for CSL positions. They 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. Colonels influence policy within the Army and the Department of Defense.

(a) Education.

1) Most 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 courses may be considered to enhance leadership of CO, EW, or CEMA units/elements.

2) Cyber Officers directly appointed in the rank of colonel through the CDCP are required to attend the Army's Direct Commission Course (BOLC-A), followed by the Cyber Direct Commission BOLC (BOLC- B), unless granted an exception to policy/waiver by the appropriate Army authority IAW AR 350-1 and other applicable guidance. Cyber Officers directly appointed in the rank of colonel are exempt from all other PME requirements for previous ranks/grades.

(b) VTIP. For colonels who transfer into the Cyber Branch through VTIP, no Cyber School training is required; however, pending available seats, they may request to attend the Cyber Warfare Officer Transition Course, 17B CEWO Course, or Cyber School functional courses.

(c) Assignments. Cyber colonels will serve in CSL, key developmental, and developmental assignments for career progression and professional development. Broadening opportunities may provide a wider range of knowledge and skills.

1) Key developmental assignments. Selection for Brigade Command is more limited for the Cyber colonel population, so the Cyber Branch offers other senior leadership opportunities that include increased responsibilities for commanding, leading, and managing CO, EW, and CEMA organizations and capabilities at the Army and JIIM levels. Completion of a key developmental assignment for any Cyber AOC counts as key developmental credit for all Cyber AOCs in their current rank/grade. Success in the assignments listed below (or combination of assignments) will provide opportunities for career development and advancement (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) Corps CEWO (CSL) ACM Cyber/EW (CSL) ASCC CEWO Chief of Staff (post-CSL) G3/J3 G3/J3	Brigade Commander (CSL) Corps CEWO (CSL) ACM Cyber/EW (CSL) ASCC CEWO Chief of Staff (post-CSL) G3/J3	Brigade Commander (CSL) Corps CEWO (CSL) ACM Cyber/EW (CSL) Division Chief, Capabilities Dev Lead Developer (CMF/CNMF) Chief of Staff (post-CSL) G3/J3

2) 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 (post-CSL) Div Chief (DAMO-SO) (post-CSL) CEMA Division Chief Chief, Joint Cyber Center (CCMD) Cyber Outreach Officer (ACI) Director, G33 (IWOC) Director, IPE (CCMD) Operations Chief (JFQH-CY) Army/Joint Staff Officer	Asst. Commandant (post-CSL) Div Chief (DAMO-SO)(post-CSL) CEMA Division Chief Chief, Joint Cyber Center (CCMD) Cyber Outreach Officer (ACI) Director, G33 (IWOC) Director, IPE (CCMD) Operations Chief (JFHQ-CY) Army/Joint Staff Officer	Asst. Commandant (post-CSL) Div Chief(DAMO-SO)(post-CSL) CEMA Division Chief Chief, Joint Cyber Center Cyber Outreach Officer (ACI) Deputy CTO (ARCYBER) Deputy J7 (CCMD) Division Chief (HQDA G3/5/7) Operations Chief (JFHQ-CY) Army/Joint Staff Officer

3) Broadening opportunities available for colonels include but are not limited to:

a) Branch immaterial positions.
b) DoD and interagency fellowships.
c) ACOM/HQDA/CCMD/JIM/DCS/SGS assignments.
d) Nominative assignments.

(d) Self-development. Cyber colonels must maintain their branch skills and stay current on all changes that affect the Soldiers they command, lead, and manage. Seeking post-CSL developmental assignments is important during this phase. Colonels are encouraged to hold or pursue advanced degrees in STEM fields relevant to CO, EW, and CEMA leadership positions.

(e) Desired experience. A well-experienced Cyber colonel will have a variety of duty assignments as senior leaders in operational and generating forces, Army staff, and JIIM organizations. A Cyber colonel's knowledge and experience should provide a significant contribution to the Army and the Department of Defense.

17A AC Officer Career Timeline

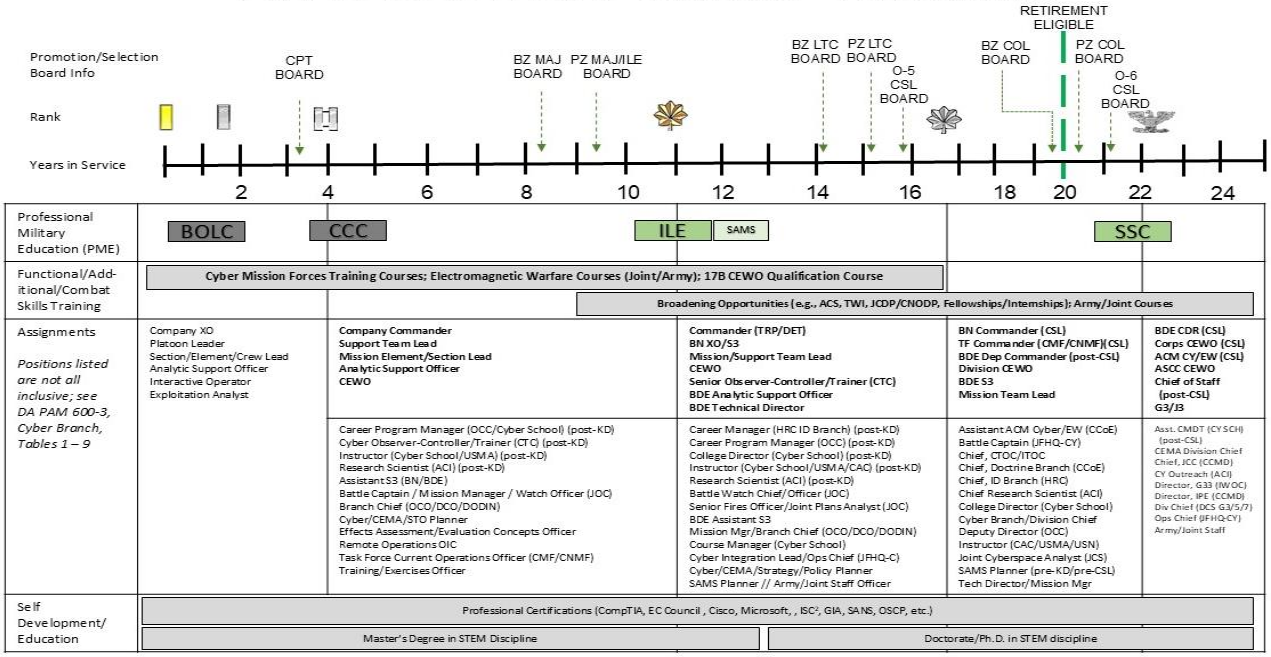


Figure 1: 17A AC Officer Career Map

17B AC Officer Career Timeline

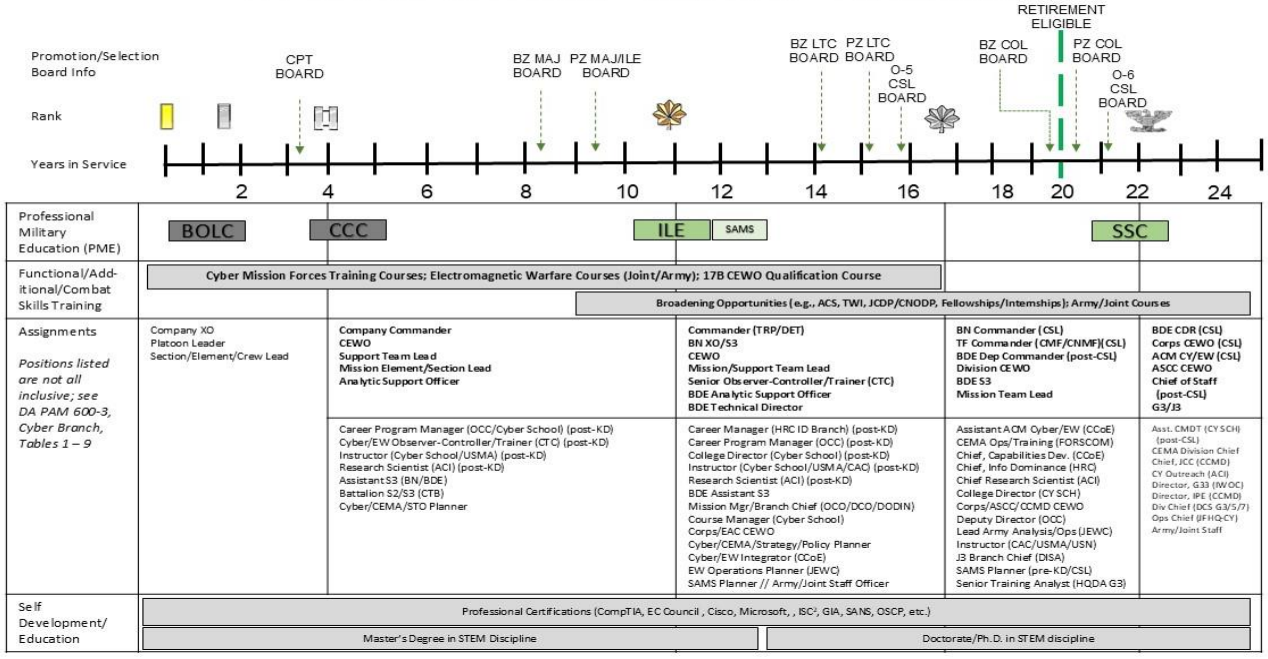


Figure 2: 17B AC Officer Career Map

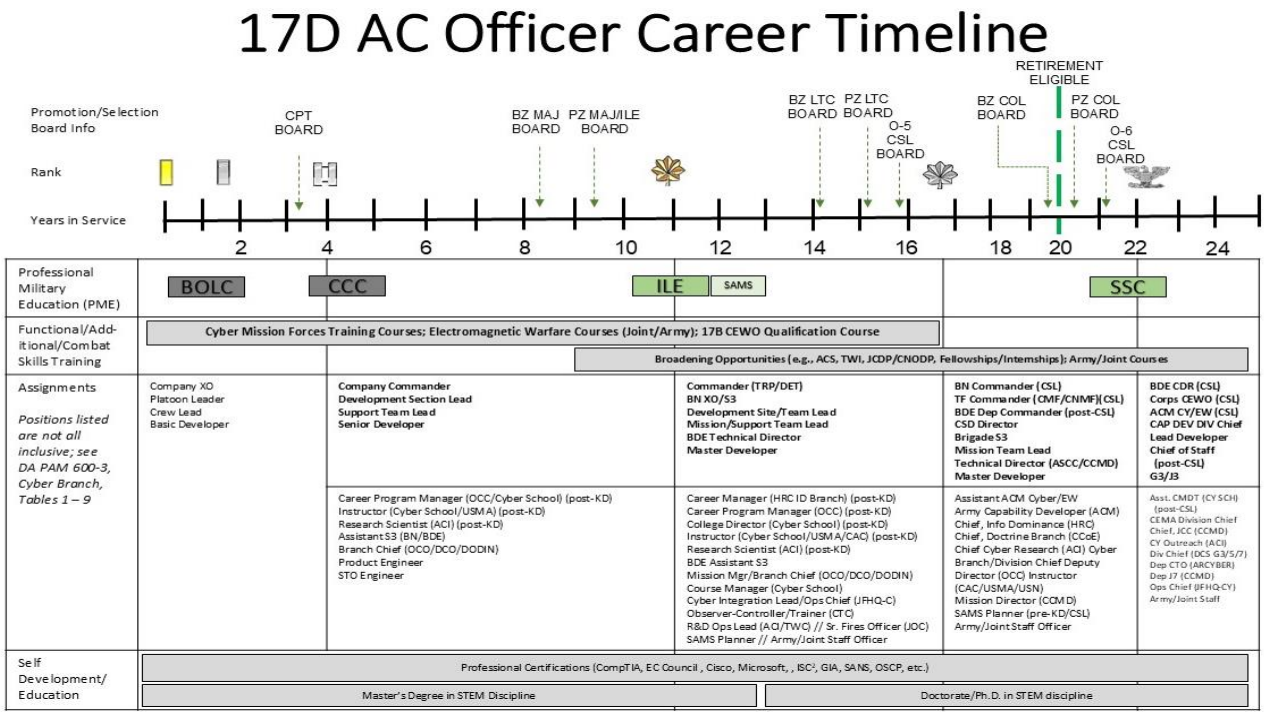


Figure 3: 17D AC Officer Career Map

D. **Reserve Component (RC) Cyber Officers**

1. **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 CO, EW, and CEMA, RC Cyber Officers rely upon extensive interaction between the AC and RC, as well as maintaining skills through civilian education, industry organizations, professional certifications, online collaboration tools, and cyber-related industry civilian employment experience.

2. **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 in Army and Joint environments, 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 depending on the availability of Cyber positions.

3. **Officer development.**

(a) Lieutenant. The professional development objective for an RC Cyber lieutenant is to gain the requisite Cyber Branch skills, knowledge, and behaviors. The focus of the RC Cyber lieutenant is the development of CO and EW skills for utilization in developmental assignments.

Table 10: Developmental Positions for RC Lieutenants (in addition to Table 1)		
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Cyber Operations Officer Crew/Section Lead Cyber/CEMA Planner Executive Officer	CEWO Cyber/EW/CEMA Planner Executive Officer	Basic Developer Executive Officer

(b) Captain. The professional development objective for an RC Cyber captain is to expand their expertise and lead section/team/company-level CO, EW, and CEMA missions. The primary focus of the RC Cyber captain is the development of tactical and technical leadership and management skills to conduct and synchronize CO, EW, and CEMA missions in Army and JIIM environments. RC captains should serve in one or more key developmental position.

Table 11: Key Developmental Positions for RC Captains (in addition to Table 2)		
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Commander Team Lead (CSC/CWC) Cyber Warfare Officer (BDE)	Commander CEWO (BDE)	Commander Senior Developer

(c) 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 Cyber teams/units, Cyber Protection Centers, brigades, special operations groups, or other positions of a similar level of responsibility. Optimally, RC Cyber majors should spend 24 to 36 months in a key developmental or equivalent position.

Table 12: Key Developmental Positions for RC Majors (in addition to Table 4)		
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Commander Team Chief (DCOE) Team Lead (Cyber Protection Team) Cyber Warfare Officer (BDE)	Commander CEWO (BDE/DIV)	Commander Master Developer

(d) 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.

Table 13: Key Developmental Positions for RC Lieutenant Colonels (in addition to Table 6)		
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Commander Deputy Commander	Commander Deputy Commander	Commander Deputy Commander

Brigade XO/S3 Mission Leader Team Chief/Lead CEWO (DIV)	Brigade XO/S3 CEWO (DIV) Mission Leader Team Chief/Lead	Brigade XO/S3 Mission Leader Team Chief/Lead Master Developer

(e) 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.

Table 14: Key Developmental Positions for RC Colonels (in addition to Table 8)		
17A (Cyber Warfare Officer)	17B (CEWO)	17D (CCDO)
Commander CEWO (Corps and Above) Chief of Staff G3/J3	Commander CEWO (Corps and Above) Chief of Staff G3/J3	Commander Chief of Staff G3/J3 Master Developer

(f) 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.

(g) 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.

(h) 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 (major and below) transferring into the Cyber Branch must attend the Cyber Warfare Officer Transition Course for AOC 17A. If designated for AOC 17B, branch transfer RC Cyber Officers (major and below) must complete the Cyber Warfare Officer Transition Course 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). RC officers should not normally be assigned to a qualifying position prior to enrolling in or completing branch/AOC-specific qualification requirements.

(i) Education. RC Cyber Officers must complete the initial training and PME requirements for their current rank/grade. RC Cyber Officers seeking to obtain PME course credit or participate in the Cyber Course Credit Program must do so IAW AR 350-1, the U.S. Army Cyber School Course Credit Program SOP, and all applicable regulations and policies. To provide flexibility to RC Cyber captains, MEL 6 (Captains Career Course) completion for a branch other than Cyber may be

authorized by the Director, Office of the Chief of Cyber, on behalf of the Commandant, U.S. Army Cyber School, so long as either Cyber BOLC or Cyber Warfare Officer Transition Course is completed for AOC 17A qualification.

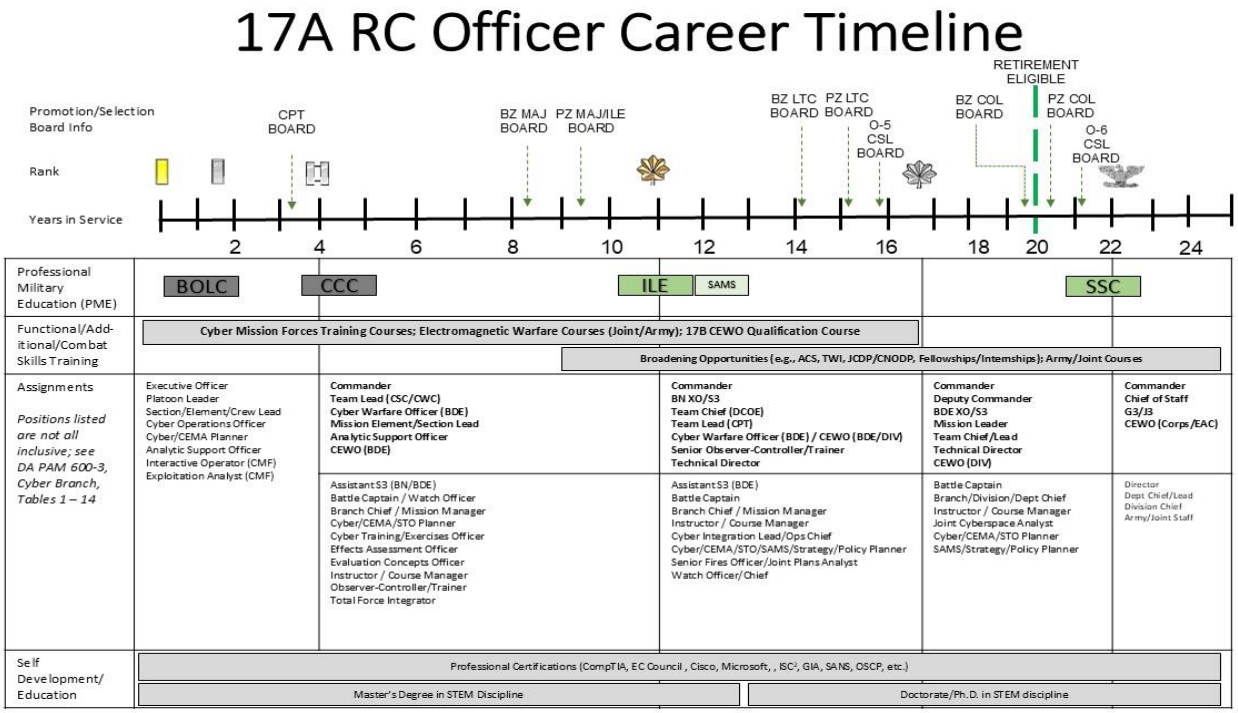


Figure 4: 17A RC Officer Career Map

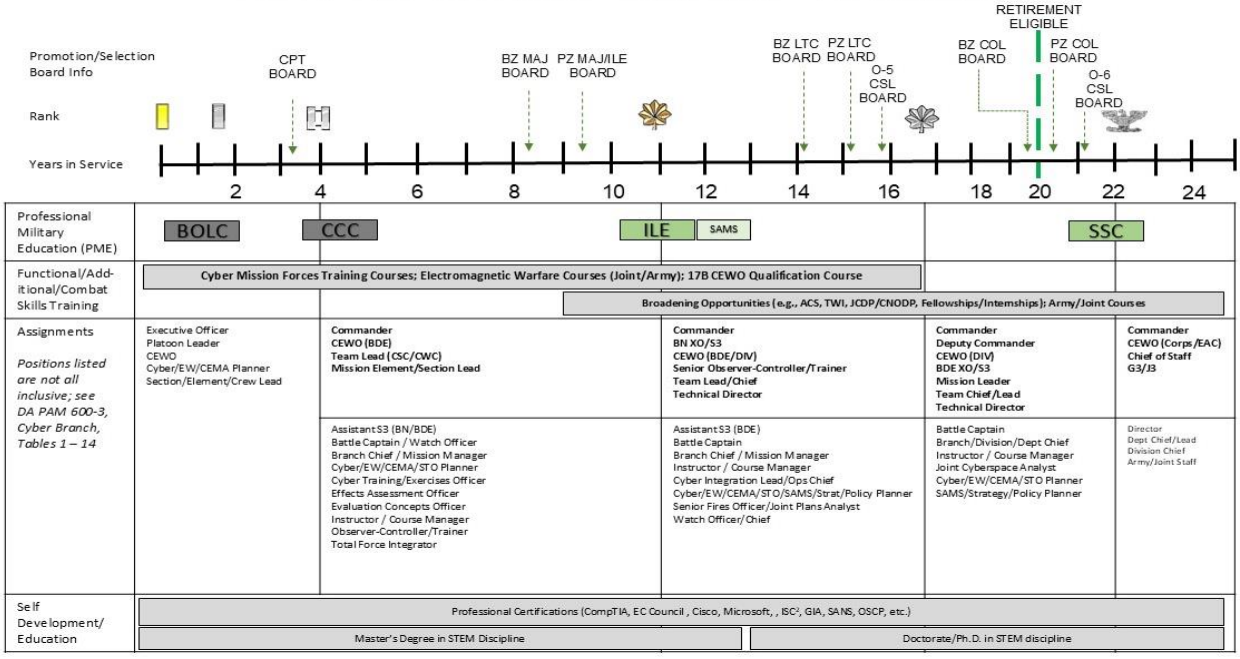


Figure 5: 17B RC Officer Career Map

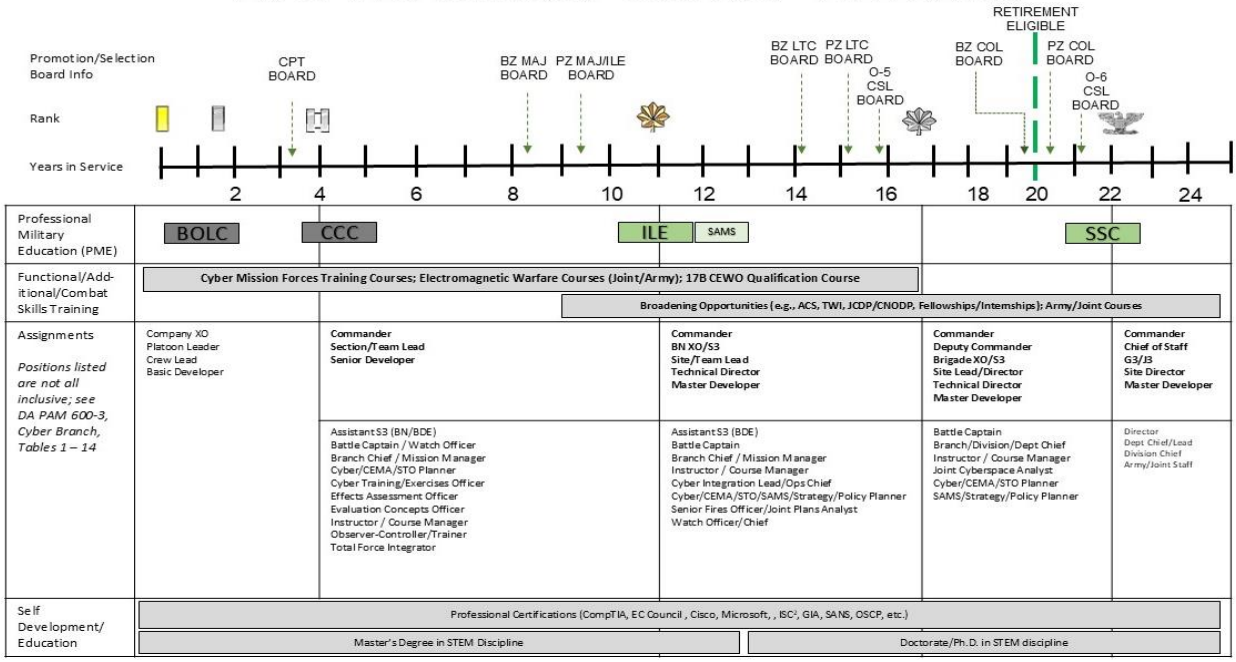


Figure 6: 17D RC Officer Career Map

E. Cyber Warrant Officer Development

1. **Unique knowledge and skills of a Cyber Warrant Officer.** Cyber Warrant Officers must maintain the characteristics identified herein.

(a) Cyber Warrant Officers are adaptive technical leaders, innovative integrators of emerging technologies, dynamic trainers, and trusted advisors.

(b) Cyber Warrant Officers must possess expert knowledge and skill in Cyberspace and Electromagnetic Warfare Operations to support mission command; such knowledge and skill require practical experience in tactics, multidomain operations (MDO), and the employment of systems and processes.

(c) Cyber Warrant Officers, through tiered progressive assignment and education, administer, manage, maintain, operate, and integrate Army systems and equipment across the full spectrum of Army operations.

(d) Cyber Warrant Officers may deploy with units, teams, or as individuals to support Army, Joint, Interagency, and Intergovernmental and Multinational (JIIM) applications of Cyberspace and Electromagnetic Warfare Operations.

2. **Cyber Warrant Officer military occupational specialties (WOMOSs).** Cyber Warrant Officers are Subject Matter Experts (SME) who provide technical and tactical expertise and experience and invaluable leadership throughout all echelons of command. MOSs for Cyber Warrant Officers are: 170A - Cyber Warfare Technician, 170B - Electromagnetic Warfare Technician, and 170D – Cyber Capability Developer Technician.

3. **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, maintain, and sustain 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 SME on Cyberspace Operations and is a leader, trainer, and advisor to commanders at all echelons. 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 Cyberspace capabilities to project power in and through Cyberspace to deliver effects, 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. Cyber Warfare Technicians must operate autonomously, be self-motivated, and deliver impactful technical solutions and effects. Cyber Warfare Technicians mainly assess from 17, 25, and 35 series MOSs who demonstrate a high degree of technical expertise in all facets of Cyberspace 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 4) Reconnaissance (ISR), Cyberspace Surveillance and Reconnaissance, Cyberspace Operational Preparation of the Environment (OPE), Cyberspace Attack, and Cyberspace Defense.

4) Integrate Cyberspace effects into planning/targeting processes.

5) De-conflict, integrate, and synchronize Cyberspace Operations.

6) Analyze relevant/current situations to predict operational Cyberspace requirements.

7) Identify, locate, and neutralize adversaries within operational networks.

8) Defend operational networks.

9) Defend weapon platforms and systems.

10) Develop and mentor all Cyberspace Operations personnel.

11) Integrate EW capabilities into Cyberspace 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 multidomain operations. Select Warrant Officers who have completed the PME commensurate with their rank/grade (W2/WOAC, W3/WOAC, W4/WOILE, W5/WOSSE) can also receive broadening assignment opportunities that extend beyond the scope of their core technical skills to support command initiatives within the operating or generating force (ref Figure 6).

(d) Proficiency Standards: Newly assessed Cyber Warfare Technicians will be required to certify at one or both of the following proficiency standards to determine experience level based on technical application in a work role.

Senior	Considered fully qualified. Completed all training required to execute the tasks for a work role and possesses the experience and judgement to operate without supervision. An individual with Senior proficiency may train and supervise an individual with Basic proficiency.
Master	All Senior level requirements, to include: An individual with Master proficiency may train and supervise training and qualification of unit personnel on execution of unit tactical and operational missions with their respective work roles. Master level proficiency includes advising leadership on mission challenges, direction, and risk mitigation strategies; development, oversight, and implementation of training to address technical competence shortfalls; evaluation of mission effectiveness; and providing recommended solutions and implementing strategies to address gaps during mission execution.

(e) Work Roles: Cyber Warfare Technicians serve in various technical tracks that focus on one of the following work roles, at one of the proficiency standards mentioned above:

Exploitation Analyst	OCO	Exploitation Analysts (EA) are responsible for developing tactical Cyberspace Operational plans which incorporate appropriate cyber tools and techniques for the remote operators to properly navigate the network. EAs identify system and network vulnerabilities and develop access and reconnaissance strategies that enable the execution of Cyberspace Operations. They utilize multiple sources of data to understand and map target networks and identify tool gaps and submit tool requirements to the appropriate development organization. EAs coordinate with supported elements to determine requirements.

Interactive Operator	OCO	Interactive Operators (ION) develop offensive exploitation opportunities, conduct exploitation, and maintain situational awareness of ongoing network operations. They conduct network reconnaissance and vulnerability analysis to map networks, identify strong points, vulnerabilities among network segments, and develop plans and strategies for the application of Cyberspace capabilities. Using in-depth technical expertise in network architectures and protocols, computer components and peripherals, programming concepts and languages and assembly codes, IONs develop exploitation opportunities and maintain situational awareness of ongoing network operations. They are the "hands on keyboard" operator who is driving the mission through technical knowledge and ability.
Host Analyst	DCO	Host Analysts (HA) possess knowledge of Enterprise Services and their security and configuration. HAs have intermediate knowledge in files systems, permissions, and operation system configurations. They capture the memory of individual processes and analyzes it using built-in tools and capabilities. They also have advanced knowledge of client systems, file system structure and common processes, Virtualized Software Security, and PowerShell Security (Windows). HAs are able to develop common automation tasks and custom modules and functions to identify anomalies or suspicious machines, as well as develop advanced rules and dashboards utilizing various languages and capabilities. HAs are capable of capturing system memory and able to analyze it for potentially malicious processes, connections, and anything else that is running and not written to disk. They also perform initial triage procedures on potentially malicious systems and best business practices.
Network Analyst	DCO	Network Analysts (NA) are responsible for providing analytic expertise in network traffic to support DCO. In addition to the core responsibilities of a Basic Network Analyst, they must understand how to develop network traffic signatures and discover anomalies through net flows and packet analysis. NAs understand data correlation and can develop tailored queries and dashboards in order gain a holistic view of the network. They can construct an overall timeline of an intrusion thru network traffic from initial inject, method of inject, time it was reported, and when/how it was cleared. Additionally, they must understand how to utilize scripting languages to parse collected data for analysis as well as automate simple DCO tasks.

Data Engineer	DCO	Data Engineers provide expertise in extracting data from multiple sources, transforming it into a usable form, and loading into data stores for use by analysts to conduct DCO. Data Engineers design and implement data ingest and egress interfaces across data pipelines, at echelon, and automate data collection and processing. In conjunction with the Analytic Support Officer and Analysts, Data Engineers design, implement, and enforce a standardized data schema to ensure data is transportable across data pipelines, at echelon, for analysis and can be enriched with other standardized data feeds. They also ensure optimal placement and migration of data between services for real-time ingest, short-term storage, and long-term storage, and assist in exploratory data analysis and visualizations to improve data reliability, efficiency, and quality.
Analytic Support Officer	DCO	Analytic Support Officers (ASO) contribute to Commander's decision-making process by collecting, analyzing, and responding to data using mathematics, programming, and domain knowledge to enable the unit to efficiently gain and exploit situational awareness. They are the subject matter expert for the analytic function at each echelon. The ASO ensures analytic readiness, conducts analytic planning, executes analysis, and grows analytic capabilities. ASO is not an entry-level work role. Individuals who become ASOs should have first served at least six months in Cyberspace operations and previously qualified on a different work role or have otherwise proved fundamental competence within the Cyberspace domain. A Basic-level ASO will train, study, and qualify for the ASO role, culminating in the completion of the exam and review by the board. ASOs will progress to the Master level, where the ASO will specialize in a particular area of data science or computer science. If the ASO does not progress to Master, they will likely transition to a role such as an Operational Research Systems Analyst (ORSA) or another full-time data science role.

(f) Military Oriented Training: In addition to Professional Military Education, military-orientated training for all Cyber Warfare Technicians can include:

1) Computer Network Operations Development Program (CNODP)

2) Special Technical Operations Planners Course (V8)

3) Joint Cyber Analysis Course (JCAC)

4) Joint Operations Fires and Effect Course (JOFEC)

5) Joint Targeting Staff Course

(g) Self-development. Lifelong learning, supported by civilian STEM degree programs, military education, certifications, online study programs, and Training with Industry (TWI), 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.

(h) WO1/CW2 development.

1) Entry level. Upon Warrant Officer selection, Warrant Officer candidates 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 Eisenhower, GA. The 170A Cyber Warfare Technician Warrant Officer Basic Course (WOBC) provides Cyber Warfare Technicians the education, training, and core skills necessary to plan, execute, and lead Cyberspace Operations successfully. The emphasis is on Army tactics, techniques, and procedures (TTP) to prepare the warrant officers to execute and direct the delivery of cyberspace effects and defensive actions required to neutralize threats. Junior grade Warrant Officers need to develop a baseline understanding of technical integration of Cyberspace Defense, Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR), Cyberspace Surveillance and Reconnaissance Cyberspace Operational Preparation of the Environment (OPE), and Cyberspace Attack in support of MDO. Additionally, Warrant Officers should demonstrate specialization within a specialized work role. However, they should possess advanced knowledge in related or supporting mission areas to increase mission impact, technical competence, and competitiveness. Completing an associate's or baccalaureate degree is recommended for promotion to CW3.

3) Desired experience. Junior Cyber Warfare Technicians must attain and maintain senior-level certification in at least one (1) 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.

(i) CW3 development.

1) Education. The 170A Warrant Officer Advanced Course (WOAC) focuses on advanced technical training and common leader development subjects designed to prepare Warrant Officers for Field Grade Cyber Warfare Technician positions. The Phase two, residential course, at the Army Cyber School at Fort Eisenhower, 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 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 Surveillance & Reconnaissance, Cyberspace OPE. Finally,

CW3s should master Cyberspace actions at the tactical and strategic level before becoming a CW4.

(j) CW4 development.

1) Education. The Warrant Officer Intermediate Level Education (WOILE) is a professional five-week resident development course. Phase one is taught at the Warrant Officer Career Center (WOCC), Fort Novosel, AL and phase two is taught at the Cyber School, Fort Eisenhower, 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 multidomain operations and LSCO through decisive action. CW4 should complete WOILE prior to promotion to CW5 and must be complete before assignment to CW4 broadening, nominative, or specialty billet.

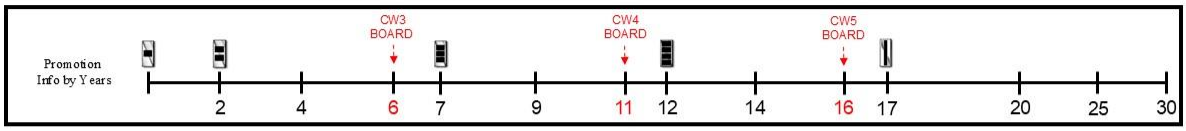
2) Desired experience. CW4s should have experience leading and/or coordinating offensive and defensive Cyberspace Operations before being assigned to senior Cyber technical advisor positions. It is highly desirable that CW4s attain master-level expertise in at least one work role and must have a functional 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.

(k) 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 senior CW4s and CW5s. The educational goal is to provide field grade Warrant Officers 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 multidomain 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. CW5s should continue to work on a graduate/post-graduate degree in an associated field of study.

2) Desired experience. All CW5 170As should have Cyberspace Operational experience leading, advising, coordinating, and executing either OCO or DCO operations at all echelons. 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.

170A AC Warrant Officer Career Timeline



			WO1	CW2	CW3	CW4	CW5
Operational Domain	Developmental		Cyber Warfare Tech	Cyber Warfare Tech Mission Element Lead Section Lead	Cyber Warfare Tech Senior Cyber Warfare Tech	Senior Cyber Warfare Tech	
	Broadening Opportunities	Operating Force			Cyber Tech Lead IPE STA	BN SWOA Cyber STA	ASCC CCWO BDE CCWO
		Generating Force		Advanced Civil Schooling Training with Industry DoD Fellowships	Instructor/Writer Line of Effort Lead Advanced Civil Schooling Training with Industry DoD Fellowships	Senior Instructor/Writer Senior Line of Effort Lead PCA STA DoD Fellowships	Cyber CWOB CCoE CCWO Cyber Tech Director (CTED) Senior Career Program Manager
Institutional Domain	PME		WOBC	WOAC	WOILE	WOSSE	
	Functional Training		EA Course, FORGE, MCC CNODP, SANS, COPC, BOC, AOC				
Structured Self-Development			Associates Degree	Associates Degree	Baccalaureate Degree	Baccalaureate Degree Graduate Degree	Graduate Degree
Guided Self-Development						Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies	Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies
Assignment Locations				Team BN/BDE ECT MDEB	Team BN/BDE MDEB US Army Cyber School US Military Academy Joint Force Headquarters-Cyber Cyber Center of Excellence	Team BN/BDE GO Staff Cyber Center of Excellence Joint Force Headquarters- Cyber US Army Cyber School Army Futures Command Special Forces Command Department of the Army	BDE/GO Staff ARCYBER USCC Joint Force Headquarters-Cyber US Army Cyber School Cyber Center of Excellence

Figure 6: 170A AC Warrant Officer Career Map

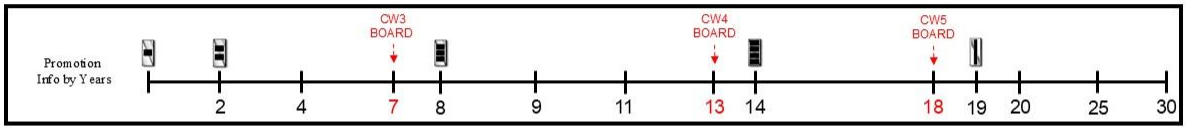
4. **170A Cyber Warfare Technician Reserve Component Warrant Officer Development.**

(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. For details, reference AR 135-155.

170A RC Warrant Officer Career Timeline



			WO1	CW2	CW3	CW4	CW5
Operational Domain	Developmental		Cyber Warfare Tech	Cyber Warfare Tech Mission Element Lead Section Lead	Cyber Warfare Tech Senior Cyber Warfare Tech	Senior Cyber Warfare Tech	
	Broadening Opportunities	Operating Force			Cyber Tech Lead	BN SWOA	Senior Cyber Warfare Tech (IMA) CCWO
		Generating Force		DoD Fellowships	DoD Fellowships	DoD Fellowships	
Institutional Domain	PME		WOBC		WOAC	WOILE	WOSSE
	Functional Training		EA Course, FORGE, MCC CNODP, SANS, COPC, BOC, AOC				
Structured Self-Development			Associates Degree	Associates Degree	Baccalaureate Degree	Baccalaureate Degree Graduate Degree	Graduate Degree
Guided Self-Development						Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies	Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies
Assignment Locations				Team BN/BDE Joint Force Headquarters	Team BN/BDE/DIV MDEB US Army Cyber School Cyber Center of Excellence Joint Force Headquarters National Guard Bureau	Team Cyber Warfare Company BN/BDE GO Staff Cyber Center of Excellence US Army Cyber School Joint Force Headquarters National Guard Bureau	BDE

Figure 7: 170A RC Warrant Officer Career Map

5. **170B Electromagnetic Warfare Technician Warrant Officer Development.**

(a) Characteristics required of Electromagnetic Warfare Technician. The 170B Electromagnetic Warfare Technician plans, directs, executes, supervises, and assesses Electromagnetic Warfare and Cyberspace Operations. They also plan, direct, supervise, and assess Cyberspace Operations integration at the tactical edge, as required. 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 JIIM 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 participates in the entire targeting process, develops, nominates targets, and synchronizes effects with the fires cell/section to deny, degrade, manipulate, disrupt or destroy EMS-enabled or designated 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 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 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 intent.

3) Conduct Electromagnetic Support to meet a commander's objectives (geolocation, direction finding, immediate threat warning, and emitter identification, which may require emitter analysis)

4) Implement Electromagnetic Protection measures (masking, emission control) with assistance from the Fires Cell and S6/G6/J6.

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 and adversary communications and non- communications systems (i.e. military comms and data links, RADAR, and telemetry).

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

9) Coordinate internal and external Army, Joint, and Multinational support for EW mission requirements and integrate EW into Army and joint 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 Cyberspace effects.

12) Coordinate with S2/G2/J2, Cyber Solutions Detachment, and Army Reprogramming and Analysis Team for EW systems reprogramming and updates.

(c) Assignments: Electromagnetic Warfare Technicians are primarily assigned at the brigade and higher echelons. These assignments allow tactical commanders to integrate Electromagnetic Warfare capabilities and exposure to Cyberspace Operations to support multidomain operations and LSCO. Select Warrant Officers who have completed the PME commensurate with their rank/grade (W2/WOAC, W3/WOAC, W4/WOILE, W5/WOSSE) can also receive broadening assignment opportunities that extend beyond the scope of their core technical skills to support command initiatives within the operating or generating force, as reflected on the career map.

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

1) Cyber Effects Application Course

2) Special Technical Operations Planners Course (V8)

3) Army Space Cadre Basic Course (3Y)

4) Joint Firepower Course (5U)

5) Military Deception Planners Course

6) Mission Command Digital Master Gunner Course

7) Aerial Precision Geolocation Course (V3)

8) Close Access Tactical-Recon (CAT-R)

9) NATO EW Operational Planning Course

10) NATO Joint EW Course

11) NATO Targeting Course

12) Joint Targeting Staff Course

13) Joint Intermediate Target Development (JITD)

14) Joint Operations Fires and Effect Course (JOFEC)

15) Space 200

16) 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 Warrant Officer candidates 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 Eisenhower, 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 functional 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 multidomain operations. Completion of an associate's or baccalaureate degree is a recommended goal before becoming a CW3.

3) Desired experience. Junior 170B Electromagnetic Warfare Technicians should be subject matter experts 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 Eisenhower, 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 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 and leverage 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 five-week resident development course. Phase one is taught at the Warrant Officer Career Center (WOCC), Fort Novosel, AL and phase two is taught at the US Army Cyber School, Fort Eisenhower, 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 multidomain

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.

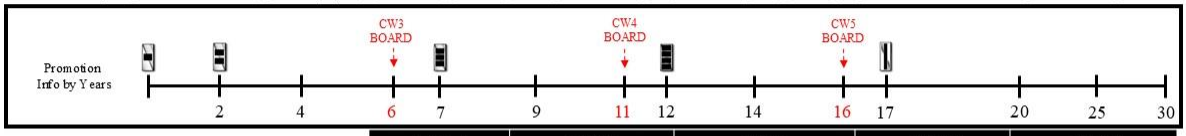
2) Desired experience. Electromagnetic Warfare Technicians at the CW4 level are senior-level technical and tactical experts that should exude character, competence, and commitment while thriving in complex and uncertain environments. CW4s are highly adept and adaptive leaders, trainers, and advisors 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 senior CW4s and CW5s. The educational goal is to provide field grade Warrant Officers 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 multidomain 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. CW5s should continue work on a graduate/post-graduate degree in associated 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



			WO1	CW2	CW3	CW4	CW5
Operational Domain	Developmental		EW Tech	EW Tech	EW Tech Senior EW Tech	Senior EW Tech	
	Broadening Opportunities	Operating Force		OC/T EW Tech OPFOR EW Tech	EW Tech Lead OC/T EW Tech Senior OC/T EW Tech	EW Tech Director Senior OC/T EW Tech EW STA	EW STA ASCC CCWO
		Generating Force		Advanced Civil Schooling Training with Industry DoD Fellowships	Instructor/Writer Advanced Civil Schooling Training with Industry DoD Fellowships	Senior Instructor/Writer EW Career Program Manager WO Assignment Mgr (HRC) Advanced Civil Schooling Training with Industry DoD Fellowships	Cyber CWOB
Institutional Domain	PME		WOBC	WOAC	WOILE	WOSSE	
	Functional Training		ASBC, COPC, JOFEC, JEWTOC, NATO EW COURSE, STO PLANNERS COURSE, CYBER 200, BRIGHTON, TOUCHSTONE			Joint Targeting, MILDEC, JCOPC, ALCOC, CYBER 300	
Structured Self-Development			Associates Degree	Associates Degree	Baccalaureate Degree	Baccalaureate Degree Graduate Degree	Graduate Degree
Guided Self-Development						Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies	Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies
Assignment Locations				BCT SFAB MDEB Combat Aviation BDE Cyber Warfare Battalion Ranger Regiment Special Forces Command Combat Training Center US Army WO Career College	BCT DIV MDEB SMDC GO Staff Cyber Warfare Battalion Civil Affairs BDE Special Forces Command Theater Fires Element Combat Training Center US Army Cyber School Army Cyber Institute Army Futures Command	DIV CORPS ASCC Expeditionary MI BDE Threat Fires Element US Army Cyber School Army Futures Command Cyber Center of Excellence	ARCYBER FORSCOM US Army WO Career College Army Futures Command

Figure 8: 170B AC Warrant Officer Career Map

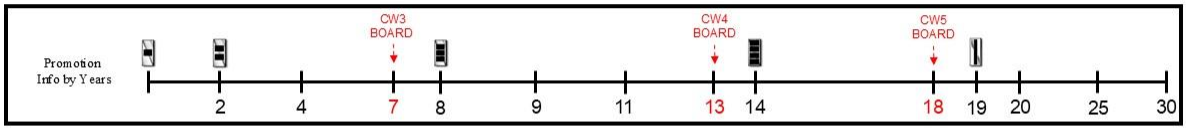
6. **170B Electromagnetic Warfare Technician Reserve Component Warrant Officer Development.**

(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. For details, reference AR 135-155.

170B RC Warrant Officer Career Timeline



			WO1	CW2	CW3	CW4	CW5
Operational Domain	Developmental		EW Tech	EW Tech	EW Tech Senior EW Tech	EW Tech Senior EW Tech	
	Broadening Opportunities	Operating Force					
		Generating Force		DoD Fellowships	DoD Fellowships	DoD Fellowships	
Institutional Domain	PME		WOBC	WOAC	WOILE	WOSSE	
	Functional Training		ASBC, COPC, JOFEC, JEWTOC, NATO EW COURSE, STO PLANNERS COURSE, CYBER 200, BRIGHTON, TOUCHSTONE			Joint Targeting, MILDEC, JCOPC, ALCOC, CYBER 300	
Structured Self-Development			Associates Degree	Associates Degree	Baccalaureate Degree	Baccalaureate Degree Graduate Degree	Graduate Degree
Guided Self-Development						Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies	Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies
Assignment Locations				BCT SFAB Combat Aviation BDE Special Forces Command	DIV Maneuver Enhancement Brigade	DIV Joint Force Headquarters	

Figure 9: 170B RC Warrant Officer Career Map

7. **170D Cyber Capability Developer Technician Active Component Warrant Officer development.**

(a) Characteristics required of Cyber Capability Developer Technician. Cyber Capability Developer Technicians develop and implement software capabilities that support offensive and defensive Cyberspace Operations and Electromagnetic Warfare Operations. Their software 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 Capability 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 Capability Developer Technician. The Cyber Capability Developer Technician is a Subject Matter Expert (SME) on developing and implementing software capabilities and is a leader, trainer, and advisor to commanders at all levels. The Cyber Capability Developer Technician is a versatile, highly trained individual responsible for analyzing system vulnerabilities, product research, capability development, documentation, and implementation of software capabilities that operate in and through Cyberspace and EMS and serve as a force multiplier for maneuver forces. The Cyber Capability 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 Capability Developer Technicians must operate without direct oversight or guidance, be self-motivated, and provide timely and effective technical products and solutions. Cyber Capability 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 Capability Developer Technicians perform the following functions/tasks:

1) Analysis of system vulnerabilities.

2) Software and hardware capability research.

3) Software capability development and documentation.

4) Software capability implementation.

(c) Assignments: Cyber Capability 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 multidomain operations. Select Warrant Officers who have completed the PME commensurate with their rank/grade (W2/WOAC, W3/WOAC, W4/WOILE, W5/WOSSE) can also receive broadening assignment opportunities that extend beyond the scope of their core technical skills to support command initiatives within the operating or generating force, as reflected on the career map.

(d) Proficiency Standards: Upon graduation from the Warrant Officer Basic Course, Cyber Capability Developer Technicians are certified in the Cyber Capability Developer work role, at the basic level. From there, 170Ds will be assessed at one or both of the following proficiency standards to determine increased experience level.

Senior	Considered fully qualified. Completed all training required to execute the tasks for one (1) of the specialty tracks listed below and possesses the experience and judgement to operate without supervision. An individual with Senior proficiency may train and supervise an individual with Basic proficiency.
Master	All Senior level requirements and must complete all training required to execute the tasks for a second (2) specialty track. An individual with Master proficiency may train and supervise training and qualification of unit personnel on execution of unit tactical and operational missions with their respective work roles. Master level proficiency includes advising leadership on mission challenges, direction, and risk mitigation strategies; development, oversight, and implementation of training to address technical competence shortfalls; evaluation of mission effectiveness; and providing recommended solutions and implementing strategies to address gaps during mission execution.

(e) Specialty Tracks:

1) Windows Access

2) Windows Persistence

3) Unix Access

4) Unix Persistence

5) Embedded

6) RF

7) Data Science

8) Infrastructure

(f) Military Oriented Training: In addition to Professional Military Education, military-orientated training for all Cyber Capability 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 Capability Developer Technician.

(f) WO1/CW2 development.

1) Entry level. Upon Warrant Officer selection, all Noncommissioned 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 Eisenhower, GA. The 170D Cyber Capability Developer Technician Basic Course provides Cyber Capability Developer Technicians with the education, training, and core skills necessary to develop software capabilities that successfully support Cyberspace Operations. The training emphasizes developing and implementing capabilities to prepare the Warrant Officers to support authorized non-lethal 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 Cyberspace Operational Preparation of the Environment (OPE), and Cyberspace Attack in support of EW operations. Completing an associate's or baccalaureate degree is a recommended goal before becoming eligible for promotion to CW3.

3) Desired experience. Junior Cyber Capability Developer Technicians must attain and maintain basic- level certification as a capability developer. 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 Capability 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 Capability Developer Technician is responsible for completing assigned tasks and modules with guidance and supervision from a Senior or Master Basic-level Cyber Capability 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 Capability Developer Technician positions. At the Army Cyber School at Fort Eisenhower, GA, the residential course consists of 19 weeks of advanced technical and tactical training in software 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 Capability 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 operator’s 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 Capability Developer Technician also provides oversight and direction to Basic- level Cyber Capability Developer Technician working under their tutelage. They are also responsible for decomposing projects into components assigned to Basic-level Cyber Capability 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 Novosel, AL and a final five-week Phase three taught at the Cyber School, Fort Eisenhower, 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 Capability 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.

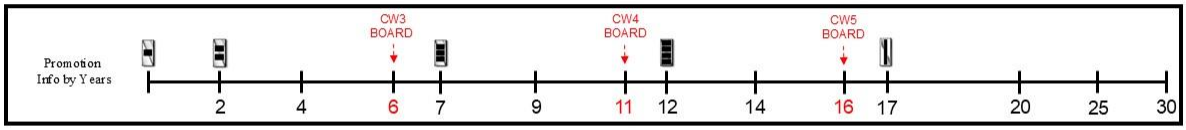
2) Desired experience. A CW4 Cyber Capability Developer Technician has mastered their specialty and is responsible for providing guidance and technical direction over multiple projects in this specialty. Additionally, they mentor Senior-level Cyber Capability Developer Technicians as they progress to the Master-level. Master Cyber Capability 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 multidomain 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 Capability Developer Technicians 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



			WO1	CW2	CW3	CW4	CW5
Operational Domain	Developmental		Cyber Capability Developer Tech	Cyber Capability Developer Tech	Cyber Capability Developer Tech Senior Cyber Capability Developer Tech	Senior Cyber Capability Developer Tech Capability Developer Tech Advisor	Capability Developer Tech Director
	Broadening Opportunities	Operating Force				Cyber STA	Cyber Tech Director (TWC)
		Generating Force		ASVE (Cyber) Advanced Civil Schooling Training with Industry DoD Fellowships	ASVE (Cyber) Advanced Civil Schooling Training with Industry DoD Fellowships	Instructor/Writer ASVE (Cyber) DoD Fellowships	
Institutional Domain	PME		WOBC	WOAC	WOILE	WOSSE	
	Functional Training		CLP-C, PCPP-21-1XX, PCPP-32-2XX, CSSLP			CISA, GSNA, GCIH, GPEN, CISSP, CASP, CHFI, GREM, CCFE, CCNP, OSCP, CNODP	
Structured Self-Development			Associates Degree	Associates Degree	Baccalaureate Degree	Baccalaureate Degree Graduate Degree	Graduate Degree
Guided Self-Development						Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies	Joint Courses Senior Level Education How the Army Runs Course Advanced Military Studies
Assignment Locations				Army Futures Command	Team BN/BDE MDEB US Army Cyber School Army Futures Command	BN/BDE US Army Cyber School Army Futures Command	ARCYBER

Figure 10: 170D AC Warrant Officer Career Map