Cyber Branch

1. Introduction

a. Purpose of the Cyber branch. The Cyber branch has the mission to plan, synchronize, and conduct defensive cyberspace, offensive cyberspace, and electronic warfare operations (DCO, OCO, and EW, respectively).Through the employment of precision effects, adversary capabilities are degraded, disrupted, destroyed, or manipulated while simultaneously supporting the commander's freedom of maneuver across all domains. OCO are intended to project power through the application of force in and through the cyberspace domain to create and achieve effects against adversaries in support of commanders' objectives. DCO are passive and active activities intended to preserve the ability to utilize friendly cyberspace capabilities at times and locations of our choosing, and protect data, net-centric capabilities, the Department of Defense Information Network (DODIN), and other designated weapons systems. EW operations are military actions involving the use of electromagnetic and directed energy to seize, retain, and exploit the initiative in the electromagnetic spectrum (EMS) through the execution of electronic attack (EA), electronic protection (EP), and electronic warfare support (ES) actions which deliver capabilities in support of Army and Joint, Interagency, Intergovernmental, and Multinational (JIIM) operations. Cyber officers conduct these operations to enable the commander's ability to mass effects and gain advantages in the EMS, cyberspace domain, and across all other domains during multi-domain battle in support of unified land operations (ULO) objectives. Cyber is the only branch specifically designed to engage the enemy directly within the cyberspace domain and the EMS. Cyber officers must possess a current Top Secret (TS) / Sensitive Compartmented Information (SCI) clearance to be awarded and maintain the AOC. Additionally, cyber officers must be capable of passing a counterintelligence scope polygraph (CSP) to serve in unit or mission specific AOC 17A (Cyber Operations Officer) positions.

b. Proponent information. Commandant, U.S. Army Cyber School, Fort Gordon, GA 30905-5735. For more information contact the Cyber School personnel proponent office at usarmy.gordon.cyber-coe.mbx.occ-officers@mail.mil or visit the website at https://cyberschool.army.mil.

c. Functions. Cyber officers are experts in projecting power in and through cyberspace and the EMS, and are proficient in all forms of decisive action: offense, defense, and stability operations. Cyber officers must fully understand maneuver operations to ensure synchronized, relevant, and integrated effects that enable success in an ever-changing strategic and operational environment. The Cyber Operations Officer is the primary subject matter expert for operations and employment of Cyber Mission Forces (CMF), including OCO and DCO capabilities at all echelons and support to DODIN operations. Select Cyber Operations Officers are subject matter experts for engineering, developing, managing, and integrating hardware and software solutions and network and cloud based capabilities to facilitate real-time cyberspace operations. The Cyber and Electronic Warfare Operations (CEWO) Officer is the commander's subject matter expert for all cyberspace electromagnetic activities (CEMA), including cyberspace and EW operations. At echelons corps and below, the CEWO Officer is also responsible for the planning, integrating, and synchronizing all cyberspace and EW operations in support of ULO. Cyber officers work primarily in Army and Joint cyberspace operations and maneuver units and fill a variety of key positions to perform the following functions and tasks:

(1) Execute mission command of CMF and CEMA elements during DCO, OCO, and EW missions in support of Joint, Army, and combined arms operations.

(2) Provide coordination for employment of cyberspace and EW operations capabilities at all levels of Joint, Army, and Coalition commands.

(3) Develop doctrine, organizations, and equipment for cyberspace operations' unique missions and units.

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

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

(6) Serve as cyberspace operations and EW advisors to foreign military, Army National Guard, and U.S. Army Reserve organizations.

(7) Serve in cyberspace operations roles in support of other designated systems (i.e. DODIN and weapon systems).

d. Branch eligibility. The Cyber branch is open to both male and female officers. Officers of other branches who desire to VTIP into Cyber branch should submit a request in accordance with AR 614-100, chapter 4, DA PAM 611-21 and VTIP MILPER messages.

2. Officer characteristics required

a. The core competencies and essential capabilities of Cyber officers. The Cyber branch requires officers who are, first and foremost, leaders of Soldiers and Department of the Army Civilians. They should be mentally and physically disciplined and well-versed in cyberspace operations, EW, and combined arms tactics, techniques, and procedures. They must possess the moral, intellectual, and interpersonal characteristics that will enable them to develop into agile and adaptive leaders who are flexible, critically reflective, and comfortable with ambiguity and uncertainty. They must be innovative and adaptive while competently performing in JIIM environments across the spectrum of conflict.

b. Characteristics required of all officers. Cyber officers are valued for their skills as cyberspace and EW operations and engineering leaders, trainers, and planners. The goal of the branch is to provide each officer with a series of leadership, staff, and developmental assignments, institutional training, and self-development opportunities in order to develop combined arms warriors with broad experience who can successfully operate in Cyber Operations, Cyber and Electronic Warfare, Cyber Operations Engineering, branch immaterial, and JIIM assignments.

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

(1) Mastery of knowledge related to the cyberspace domain, the EMS environment, and the DODIN, including associated doctrine, policies, statutes, and laws.

(2) Firm understanding of intelligence preparation of the battlefield/battlespace (IPB), the military decision-making process (MDMP), the Joint operation planning process (JOPP), the targeting process, and provision of valuable, relevant feedback affecting mission accomplishment and unit survivability.

(3) Outstanding performance across a wide variety of operating and generating force positions, including being a talented, flexible, and adaptive team player with a keen ability to work with diverse team members.

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

(5) Operate without direct oversight or guidance – self-motivated – and provide timely and effective technical products, effects, and solutions.

(6) Ability to gain and retain an in-depth understanding of how best to employ cyberspace and EW operations assets in support of combined arms and JIIM operations, including planning, coordinating, integrating, and assessing cyberspace and EW operations capabilities to support the combatant commander.

(7) Lead CMF teams, cyber engineering teams, EW elements, organic CEMA cells/sections, and CEMA working groups.

(8) Prepare, submit for approval, and supervise the issuing and implementation of orders/fragmentary orders for cyberspace and EW operations.

(9) Develop and maintain a current assessment of available Special Access Programs, cyberspace operations, and EW resources.

(10) Advise the commander on cyberspace and EW operations capabilities, employment, targeting requirements, limitations, and legal considerations.

(11) Serve as the area of responsibility jamming control authority when designated and deconflict EW operations with spectrum manager(s).

(12) Ability to express technical concepts clearly, concisely, and accurately – both orally and in writing – and be able to make presentations to the commander for decision-making purposes.

(13) Assist primary staff elements in developing the cyberspace, EW, and CEMA-related threat characteristics during the IPB process.

(14) Fully represent cyberspace and EW operations equities to commanders and staffs who may not understand the importance and relevance of this critical capability.

(15) Apply doctrinal knowledge and translate technical data into useable information to solve the tactical problems, and formulate and defend solutions to problems using current Army and Joint doctrine.

(16) Understand and integrate area of responsibility lessons learned in a strategic, operational, or tactical environment.

(17) Possess a baccalaureate degree, preferably in the fields of science, technology, engineering, and mathematics.

(18) Possess TS/SCI access prior to attending Cyber branch courses.

d. Unique attributes for Cyber officers. The Cyber branch requires dynamic, competent, well-trained leaders at all levels who understand how combat arms fight in order to effectively integrate DCO, OCO, and EW. Cyber officers must possess the following attributes:

(1) Terrain sense. Terrain sense is the ability to visualize, both physically and virtually, the battlefield and understand how to optimize cyberspace and EW weapon systems and the application of fires in the cyberspace domain. This includes understanding the nuances of the three cyberspace layers (physical, logical, and cyber-persona) and all warfighting domains and their impacts on conducting effective cyberspace and EW operations.

(2) Attention to detail. Cyber officers must possess and demonstrate a high degree of attention to detail to ensure timely and effective delivery of cyberspace and EW operations capabilities, especially since they control capabilities that have the potential to affect systems beyond designated targets.

(3) Joint and expeditionary mindsets. All Cyber leaders must be ready to provide cyberspace and EW operations capabilities anywhere in the world, in either long or short duration and in a flexible and adaptive manner. The application of cyberspace and EW operations includes JIIM assets that must be synchronized and synergized in support of ULO. Cyber officers must gain in-depth knowledge in the disciplines of cyberspace and EW operations, as well as, learning the nuances of JIIM planning, CEMA elements, and support to DODIN operations. This life-long learning effort starts prior to commissioning and continues throughout the officer's career. The study of foreign cultures, language skills, and formal schooling (both military and civilian) are just a few of the opportunities that will assist a Cyber officer in developing Joint and expeditionary mindsets.

3. Cyber Branch officer development

a. Cyber officer development – areas of concentration. All Cyber officers begin their career as a 17A (Cyber Operations Officer) and may obtain additional AOC and specialized technical training, as needed. Cyber officers who acquire an additional AOC may have the opportunity to leverage those skills in future assignments; however, Cyber officers must continue to successfully serve in key developmental (KD) assignments for each grade. Cyber officers can expect some permeability between the 17-series AOCs depending on availability of positions, personnel, and training, as well as, development of unique skillsets and individual professional interests by officers within all Cyber AOCs.

(1) Cyber Operations Officer (17A). All Cyber officers receive initial and advanced training as a 17A. Duties include leading, directing, managing, planning, integrating, coordinating, and conducting DCO and OCO missions and support to DODIN operations at Army and Joint levels, to include JIIM. The 17A officer is well-versed in tactics, techniques, and procedures for maneuvering in and through cyberspace to provide offensive and defensive actions. Select 17A officers receive highly specialized, technical training designed and/or designated by the Cyber Center of Excellence, Army Cyber Command, and/or U.S. Cyber Command, possibly including the Computer Network Operations Development Program (CNODP), to perform cyber operations engineering and capabilities development functions. Duties include leading, directing, managing, planning, integrating, coordinating, and conducting tool and capability development, including engineering software, hardware, network, and cloud-based solutions, to enable cyberspace operations at all echelons.

(2) Cyber and Electronic Warfare Operations Officer (17B). Following completion of 17A AOC qualification training, select promotable first lieutenants and captains will attend the Cyber Captains Career Course (CyCCC) and EW Qualification Course to become a 17B. Duties include leading, directing, managing, planning, integrating, coordinating, and conducting cyberspace and EW operations at brigade,

division, corps, Army, and Joint levels, to include JIIM. The 17B officer is skilled and knowledgeable in tactics, techniques, and procedures for providing cyberspace and EW operations effects through CEMA in ULO to support commander requirements.

b. Lieutenant development. The professional development objective for this phase of an officer's career is to develop requisite baseline Cyber branch knowledge, skills, and attributes. The focus of the Cyber lieutenant is the development of technical defensive and offensive cyberspace operations skills and the utilization of these skills in an operational assignment on or in support of a CMF team.

(1) Education. After commissioning, most Cyber officers will attend Cyber Basic Officer Leader Course (CyBOLC). A select number of lieutenants may attend ACS prior to CyBOLC; however, all officers are still required to attend CyBOLC after commissioning.

(2) Assignments. After CyBOLC, lieutenants can expect to be assigned to a CMF team for at least 12 months in order to gain leadership experience and technical competence. Ideally, lieutenants will serve as a CMF Sub-Element (or Section) Lead or Operations Officer to obtain leadership, management, and technical skills associated with DCO and OCO missions. These developmental opportunities will prepare a lieutenant to be a future CMF Cyber Defense Manager and Team Lead as a captain.

(a) Cyber lieutenants should be assigned to CMF or associated cyberspace operations positions, primarily within a Cyber Protection Team (CPT), National Mission Team (NMT), National Support Team (NST), Combat Mission Team (CMT), or Combat Support Team (CST), upon completion of CyBOLC and requisite functional training. Select lieutenants develop expertise in technologies used within the cyberspace domain (to include industrial control systems, weapons systems, etc.) and cyberspace engineering capabilities through highly specialized training designed and/or designated by the Cyber Center of Excellence, Army Cyber Command, and/or U.S. Cyber Command, possibly including CNODP.

(b) The goal of the branch is to assign lieutenants to the operational force as an initial assignment. Some of these assignments include:

Table 1 Developmental Positions for Lieutenants	
17A (Cyber Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
CMF Team Operations Officer CMF Sub-Element/Section Lead Cyber Planner CMF Team Member (OCO/DCO) CMF Analyst/Operator Watch Officer Company Executive Officer (XO) Developer Hardware/Software (HW/SW) Engineer Cloud/Network Engineer	No lieutenant assignments

(3) Self-development. Lieutenants should focus on tactical and technical cyberspace operations fundamentals, CMF work role certifications, cyber-related industry certifications, leadership skills, logistics operations, basic administrative operations, fundamentals of training management, and other technical proficiency skills.

(4) Desired experience. Each Cyber lieutenant will successfully serve in an operational Cyber unit and focus on developing team or section-level leadership skills and mastering the essential elements of the technical and tactical competencies of a cyberspace operations analyst and operator. Lieutenants should continue to build their working knowledge of conducting various types of cyberspace operations missions.

c. Captain development. The professional development objective for a captain is to expand their expertise and lead section/team level cyber missions. The focus of the Cyber captain is on the development of tactical and technical leadership and management skills to conduct and synchronize cyberspace operations at various Army, Joint, and National-level echelons.

(1) Education.

(a) Captains will attend the Cyber Captains Career Course (CyCCC). It is desirable for Cyber officers to attend CyCCC as soon as practical after promotion to captain, or as soon as possible after completing four years and prior to the seventh year of Active Federal Commissioned Service (AFCS).

(b) Select 17A Captains develop mastery of technologies used within the cyberspace domain (to include industrial control systems, weapons systems, etc.) and cyberspace engineering capabilities through highly specialized training designed and/or designated by the Cyber Center of Excellence, Army Cyber Command, and/or U.S. Cyber Command, possibly including CNODP.

(c) Captains who become 17Bs strive to develop mastery of cyberspace and EW operations capabilities through the EW Qualification Course and CyCCC, as well as, application of knowledge and development of tactical skills while supporting ULO.

(d) Company grade VTIP or branch-detailed officers transitioning into the Cyber branch must attend the Cyber Operations Officer Course (CyOOC), the EW Qualification Course (for officers selected for 17B), and CyCCC (for officers who have not completed a Captains Career Course for any branch prior to selection).

(2) PME constructive credit. Cyber officers can apply for constructive credit for military courses under AR 350–1, based on experience and other training. Constructive credit is awarded through a formal board process convened by the Commander, HRC.

(3) Technical constructive credit. Cyber officers who acquire cyberspace and EW operations related skills, knowledge, and abilities through civilian industry, education, or training may apply for 17A/B qualification training constructive credit. Approval authority for awarding 17A/B qualification training constructive credit is the Commandant, U.S. Army Cyber School. Constructive credit criteria is developed by U.S. Army Cyber School in close coordination with U.S. Army Cyber Command and U.S. Cyber Command.

(4) Assignments. Captains will normally not be assigned to positions outside of an operational unit until they have had the opportunity to achieve branch key development goals.

(a) Key developmental assignments. CMF section/team leadership positions provide a Cyber captain with the desired operational experience in small unit leadership and cyberspace and EW operations at this developmental phase. Capabilities development and research positions deepen a captain's technical expertise and provide far-reaching benefits to the CMF. Company command is also desired for captains to gain considerable experience in leading and managing small organizations and their associated training, maintenance, logistics, and administrative operations. These assignments provide a credible developmental experience in the core skill sets required of future CMF mission team leaders and key field grade positions. Captains must serve in key developmental positions for a minimum of 12 months (optimally 24 months). 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 Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
CST Team Lead Cyber Defense Manager Company Commander Senior Developer Senior HW/SW Engineer Senior Cloud/Network Engineer	Brigade Combat Team CEWO Officer Special Operations CEWO Officer Company Commander

(b) Developmental assignments. Developmental assignments for 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, such as:

Table 3 Developmental Positions for Captains	
17A (Cyber Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
Operations Planner (Brigade, Division, ARCYBER)	Active Component/Reserve Component (AC/RC)

Cyber School Instructor, Training Developer or Small Group Leader TRADOC Capabilities Developer ARCYBER staff / Army Cyberspace Operations and Integration Center (ACOIC) Instructor (USMA/ROTC) Watch Officer (JOC/ROC/AROC) CMF Sub-Element/Section Lead CMF Mission Commander Systems Architect Cyber Planner Researcher/Developer, Army Research Laboratory (ARL) / Army Cyber Institute (ACI) Systems Architect	Observer-Controller/Trainer (OC/T) Combat Training Center (CTC) Observer-Controller (OC) Cyber/CEMA Planner Centers of Excellence CEWO Officer

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

1. Advanced civil schooling
2. Training with industry
3. DoD or other interagency fellowships

(d) Self-development. Captains should continue to gain an advanced understanding of combined arms and CEMA to become proficient in DCO, OCO, EW, and support to DODIN operations related tasks. Captains should also continue to gain an in-depth understanding of MDMP and concentrate on those critical CEMA-focused tasks required to accomplish their wartime mission. These provide the foundation of knowledge required to effectively serve as a staff officer at the brigade or division-level. Military-orientated training for all designated Cyber officers include the Joint EW Theater Operations Course, Advanced Leader Cyber Operations Course, Special Technical Operations Planners Course, Joint Network Attack Course, EW Coordination Course, Space Fundamentals Course, Cyber 200 and 300, Joint Targeting Course, Joint Firepower Course, Joint Advanced Cyber Warfare Course, Joint Information Operations Planners Course, Joint Cyberspace Operations Planners Course, Military Deception Planners Course, and the NATO EW Course. Captains should pursue graduate-level education in a science, technology, engineering, or math (STEM) related discipline and/or obtain industry certifications related to information technology, networking, cyberspace operations, cybersecurity, and other pertinent disciplines as the opportunity presents itself.

(e) Desired experience. Cyber captains should have an in-depth knowledge of synchronizing and integrating cyber maneuver and effects at the CMF section and support team levels and successfully leading Soldiers at the mission team level. Captains should serve in at least one KD assignment for a minimum of 12 months (optimally 24 months) in order to gain the necessary leadership and mission-related skills and experience. It is also desirable to have exposure to experiences outside of core Cyber branch positions to provide a wider range of knowledge and skills to enhance an officer's understanding of the full spectrum of Army missions and expand the officer's awareness of other governmental agencies, units or environments.

d. Major development. The professional development objectives for a major is to expand and broaden the officer's tactical and technical experience and understanding of cyberspace operations, EW operations, and cyberspace operations engineering by leading and conducting CMF, cyber engineering team missions, EW elements, and CEMA cells/sections. Cyber majors also lead, manage, and plan organizational staff functions at the battalion, brigade, division, and corps levels. In addition, Cyber officers should focus on developing organizational leadership, management, and planning skills through a series of operating and generating force developmental assignments.

(1) Education. Military education required during this phase is completion of Intermediate Level Education (ILE) at the U.S. Army Command and General Staff College (CGSC). The Army conducts ILE selection boards in conjunction with the Major ACC Promotion Selection Board to consider officers for resident or non-resident ILE opportunities. In addition to Army's CGSC, Command and Staff College (CSC)/Intermediate Level Education (ILE) attendance opportunities may include one of the following schools: the U.S. College of Naval Command and Staff, the U.S. Air Command and Staff College, the U.S.

Marine Corps Command and Staff College, the Western Hemisphere Institute for Security Cooperation Command & General Staff Officer Course, or foreign military staff colleges which have been granted MEL 4 equivalency by the DCS, G-3. Officers may also compete to be selected for the School of Advanced Military Studies (SAMS) following the Army Operating Warfighting Course (AOWC).

(2) Constructive credit. Cyber officers can apply for constructive credit for military courses under AR 350–1, based on experience and other training. Because of opportunities available for Cyber officers to attend resident ILE and to enroll in the nonresident MEL 4 equivalent course, approval of constructive credit is restrictive. Constructive credit is awarded through a formal board process convened by the commander, HRC.

(3) Assignments. Majors will normally not be assigned to positions outside of an operational unit until they have had the opportunity to obtain branch key development goals.

(a) Key developmental assignments. Cyber mission and engineering team leadership and key CEMA-related positions provide a Cyber major with increased and advanced operational experience in synchronizing and orchestrating all functions of an entire CMF team to conduct cyberspace and EW operations missions. In addition, key leader staff positions help develop a Cyber major's expertise in leading, managing, and planning at higher-level organizational staff functions. These assignments provide a credible developmental experience in the core skill sets required of future Cyber battalion-level commanders, as well as, Army and Joint staff officers. Majors must serve in key developmental positions for a minimum of 12 months (optimally 24 months). 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 Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
Team Lead (NST/CMT/CPT) Battalion XO/S3 Engineering Team Lead/OIC Chief, On-net Development (USCYBERCOM) Chief, Capability Integration (USCYBERCOM)	BCT/Division/Corps CEWO Officer Program Manager Battalion XO/S3

(b) Developmental assignments. Branch developmental assignments for 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, such as:

Table 5 Developmental Positions for Majors	
17A (Cyber Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
Secretary of the General Staff (SGS) assignments College Chief, Instructor, or Training Developer (Cyber School) Cyber Training and Education Deputy Chief (Cyber School) Mission Manager Integration Lead Career Manager (HRC) Project Officer, Information and Intelligence Warfare Directorate (CERDEC) ASCC CEWO Planner Action Officer, PEO, IEWS Training/Exercises Officer	CTC Observer-Controller CEWO Lead Integrator College Chief, Instructor, or Training Developer (Cyber School) Cyber Training and Education Deputy Chief (Cyber School) TRADOC Capabilities Developer Asymmetric Warfare Group CEWO Officer HRC Career Manager Action Officer, PEO, IEWS ASCC CEWO Planner Senior Cyber/CEMA Planner Project Officer, Information and Intelligence Warfare Directorate (CERDEC)

Watch Officer (JOC/ROC/AROC) Branch or Division Chief (Operational Force/ACI) Senior Cyber Planner Senior Developer/Engineer Systems Architect Capability Analyst (USCYBERCOM) Project Manager (ARL) Researcher/Developer (ARL/ACI)	Researcher/Developer (ARL/ACI)

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

1. Advanced civil schooling.
2. Training with industry.
3. DoD and other interagency fellowships.

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

(e) Desired experience. Cyber majors should have an expert knowledge of synchronizing and integrating cyber maneuver and effects at the CMF team-level and successfully lead staff functions at the organizational-level.

Majors should serve in at least one KD assignment for a minimum of 12 months (optimally 24 months) in order to gain the necessary leadership and mission-related skills and experience. It is desirable to have exposure to experiences outside the Cyber branch to provide a wider range of knowledge and skills to enhance an officer's understanding of the full spectrum of Army missions and expand the officer's awareness of other governmental agencies, units or environments.

e. Lieutenant colonel development. The professional development objective for a lieutenant colonel is a demonstrated excellence in tactical skills, technical proficiency, and the ability to lead, train, motivate, and care for Soldiers in both the staff and command environments.

(1) Education. Senior Cyber lieutenant colonels may be selected for Senior Service College (SSC). SSC attendance opportunities may include one of the following schools: the U.S. Army War College, the National War College, the Industrial College of the Armed Forces, the Naval War College, the Air War College, approved SSC Fellowship, or foreign military SSCs that have been granted MEL 1 equivalency by DCS, G-3. Officers selected for Joint assignments must complete JPME II training.

(2) Assignments.

(a) Key developmental assignments. Lieutenant colonels must serve in key developmental positions for a minimum of 12 months (optimally 24 months). 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 Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
Team Lead (NMT, National CPT) Battalion Commander (CSL) Brigade Deputy Commanding Officer (post-CSL) Brigade S3 Chief, ACI/Joint Cyber Division Senior Capability Analyst (ARCYBER) Director, Special Projects/Innovation Team (ARCYBER) Chief, Experimentation Division (USCYBERCOM) Chief, Tool Development (USCYBERCOM) Chief, ACI/Joint Cyber Division	Division/Corps/ASCC/CCMD CEWO Force Planner/Integrator NATO CEWO Officer FORSCOM CEMA Integrator Battalion Commander (CSL) Brigade Deputy Commanding Officer (post-CSL) Brigade S3

(b) Developmental assignments. Branch developmental assignments for 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, such as:

Table 7 Developmental Positions for Lieutenant Colonels	
17A (Cyber Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
Director, Office of Chief of Cyber Operations Planner DCS/SGS assignments ARCYBER staff Cyber Branch Chief (HRC) Cyber Targeting Officer Training or Doctrine Developer (Cyber School) Instructor (USMA/ROTC/other) TRADOC Capabilities Developer Army Staff (AOC 17-coded assignments) Battle Captain Deputy Director, TCM Cyber/EW Branch/division chief (Army/Joint) Watch Officer (Army/Joint) Project Manager (ARL) Senior Researcher/Developer (ARL/ACI) Senior Developer/Engineer	Deputy Director, TCM Cyber/EW DCS/SGS assignments Director, Office, Chief of Cyber Cyber Branch Chief (HRC) ARCYBER staff Senior Researcher/Developer (ARL/ACI) Army Staff (AOC 17-coded assignments)

(c) Broadening assignments include:

1. PhD program, Naval Postgraduate School (NPS) or Air Force Institute of Technology (AFIT)
2. Training with Industry
3. DoD and other interagency fellowships

(3) Self-development. Lieutenant colonels not selected for resident SSC should enroll in nonresident SSC education. Other self-development includes a PhD STEM program at NPS or AFIT. The officer should also continue the development of his or her cyber operations and Joint warfighting skills and understanding of the Joint and Combined operational environment.

(4) Desired experience. NMT lead, National CPT lead, and battalion command experience are important for the Cyber lieutenant colonel population. Cyber branch offers other key leader opportunities that include increased responsibilities for leading and managing cyberspace operations and CEMA-focused organizations and capabilities at the Army and Joint levels. Cyber lieutenant colonels can expect to serve as cyberspace operations and EW subject matter experts in a wide variety of professionally challenging and personally rewarding assignments in the operating and generating forces. They will also serve in Army Staff and/or in JIIM organizations. Lieutenant colonels should serve in at least one KD assignment for a minimum of 12 months (optimally 24 months) in order to gain or refine the necessary leadership and mission-related skills and experience.

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

(1) Education. The majority of officers selected for promotion to colonel will be selected to attend SSC. Those not CSL-selected should enroll in the nonresident SSC course. Those selected to command will also attend a pre-command course. Officers serving as a TRADOC Capabilities Manager (TCM) may attend the Combat Developers Course. Other senior leader and executive courses will be considered to enhance leadership with cyberspace and EW operational units and CEMA-focused elements.

(2) Assignments. Cyber colonels contribute to the Army by serving in crucial assignments in the CMF, the Joint force, or with interagency partners. It is critical during this phase to develop the broad skills and competencies required of an agile and adaptive leader, while maintaining branch competency.

(a) Key developmental assignments. Command selection is limited for the Cyber colonel population. Therefore, Cyber branch offers other senior key leader opportunities that include increased responsibilities for leading and managing cyber operations organizations and capabilities at the Army and Joint levels. Colonels must serve in key developmental positions for a minimum of 12 months (optimally 24 months). Success in the assignments listed below (or combination of assignments) will provide opportunities for career development and future consideration for promotion (which will be primarily based on performance in one or more of the following positions):

Table 8 Key Developmental Positions for Colonels	
17A (Cyber Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
Brigade Commander (CSL) G3, ARCYBER Director, ACI/Joint Cyber Directorate ARCYBER Chief of Staff Cyber COE Chief of Staff Director, TRADOC Capability Manager Cyber/EW ACOIC Director (ARCYBER) Director, ACI/Joint Cyber Directorate Director, TRADOC Capability Manager Cyber/EW ACOIC Director (ARCYBER) Chief, Applied Research and Development (USCYBERCOM)	Director, TRADOC Capability Manager Cyber/EW CCMD Army Force Integrator Corps/ASCC CEWO Director Brigade Commander (CSL)

(b) Developmental assignments. Branch developmental assignments for 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, such as:

Table 9 Developmental Positions for Colonels	
17A (Cyber Operations Officer)	17B (Cyber and Electronic Warfare Operations Officer)
Cyber School Assistant Commandant Instructor (USMA/ROTC) Director, Cyberspace Operations Research and Development (ARL) Program Manager (DARPA) Partner Relations Government Outreach (USMA) Instructor (USMA/ROTC) Silicon Valley LNO Team Lead Branch immaterial assignments ACOM, HQDA, Joint, multinational, or combatant command staff Other JIIM or nominative assignments	Instructor (USMA/ROTC) ACOM, HQDA, Joint, multinational, or combatant command staff Branch immaterial assignments Other JIIM assignments Other Nominative assignments

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

1. Instructor positions (USMA faculty, ROTC, other branch and Service school instructors).
2. Other branch immaterial positions (recruiting command staff and AC/RC positions).
3. ACOM, HQDA, Joint, multinational, or combatant command staff.
4. Other special assignments in JIIM positions.
5. Other nominative assignments.

(3) Self-development. Cyber colonels must maintain their branch skills and keep current on all changes that affect the Soldiers they command and/or manage JIIM assignments are important during this phase.

(4) Desired experience. The well-experienced Cyber colonel will have a variety of duty assignments as operational and strategic Cyber leaders and subject matter experts in both operating and generating force organizations, Army Staff, and JIIM organizations. The Cyber colonel's knowledge and experience will provide a significant contribution to the Army and the DoD. Colonels should serve in at least one KD assignment for a minimum of 12 months (optimally 24 months) in order to gain or refine the necessary leadership and mission-related skills and experience.

Figure 1: 17A AC Officer Career Timeline

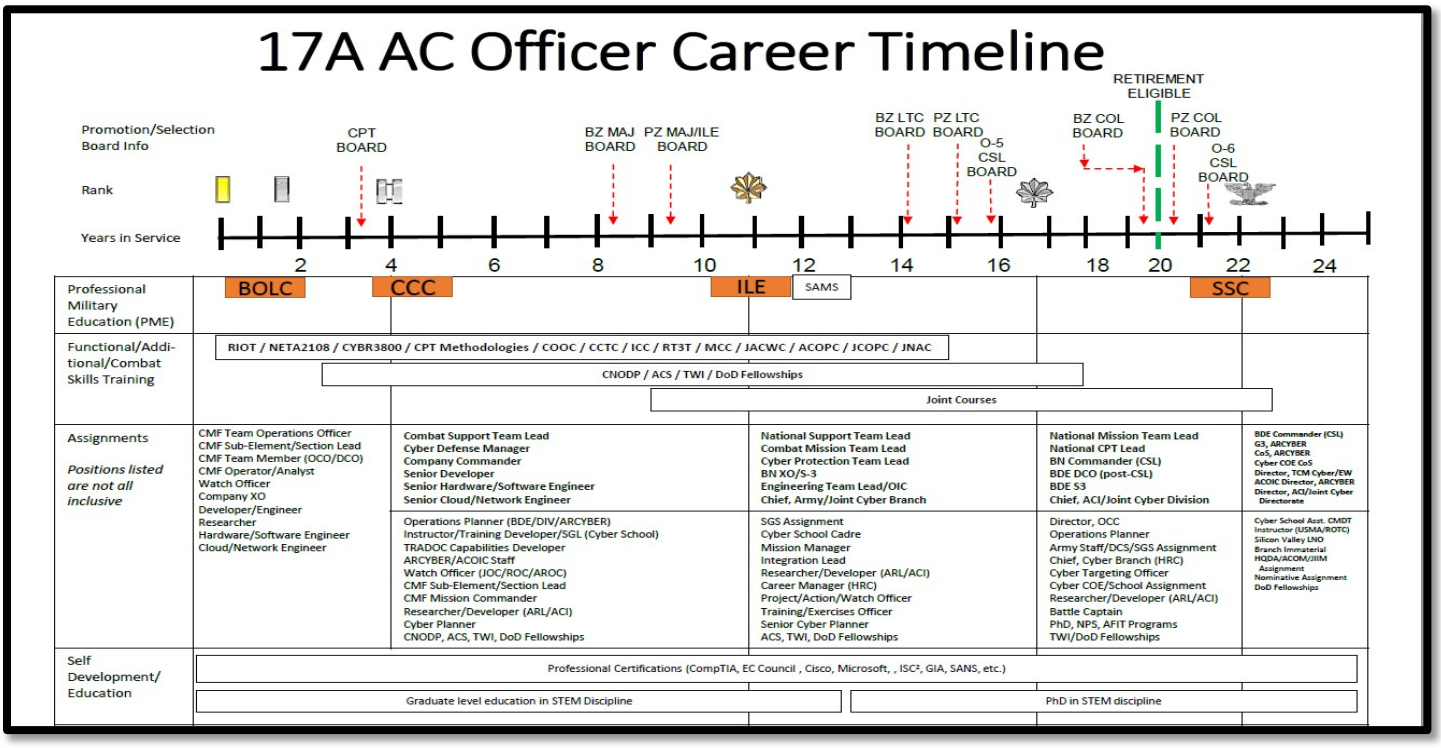
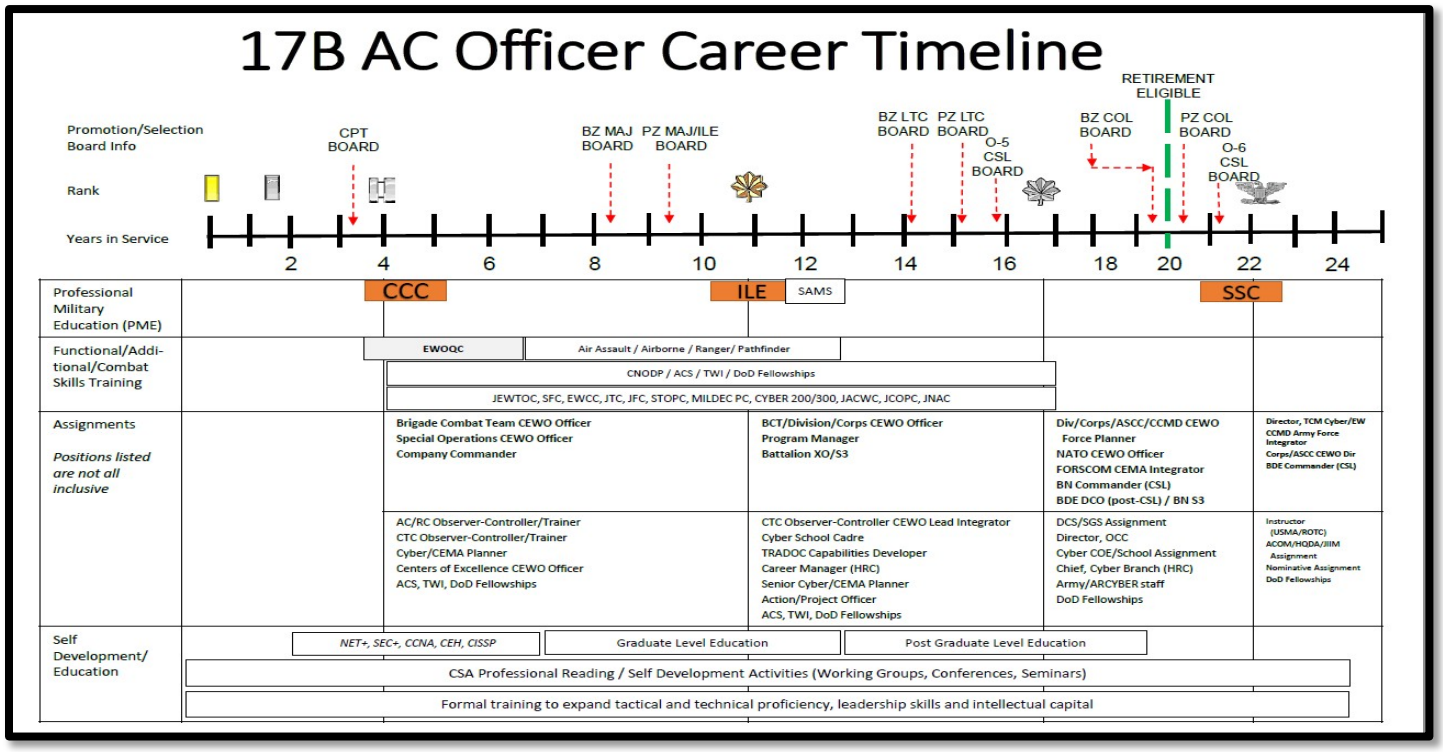


Figure 2: 17B AC Officer Career Timeline



4. Cyber Operations Reserve Component officers

a. General career development. The ARNG and USAR Cyber officers serve the same role as their Active Duty counterparts within the confines of approved RC force structures. The unique nature of the RC Soldier's role as a "citizen Soldier" poses a significant professional development challenge. To fulfill their wartime mission of leading, planning, and executing cyber operations, RC Cyber officers rely upon extensive interaction between the AC and the RC, maintaining skills through civilian education, industry organizations, professional certifications, and online collaboration tools.

b. Branch developmental opportunities. RC Cyber officers should adhere to the same standards and professional development patterns in individual training, operational assignments, and self-development as their Active Duty counterparts. RC officers should build a solid foundation in leadership, cyberspace and EW operations skills, and cyber forces operations to serve successfully in the branch. Because of geographic location or other considerations, RC Cyber officers may not have the opportunity to serve in as many cyberspace and EW operations positions as Active Duty officers. However, this issue is offset by longevity in positions that are available in Cyber forces in their geographic area.

(1) RC field grade officer standards.

(a) RC major. Majors must have completed common core ILE to be competitive for promotion to lieutenant colonel. To be best qualified, majors should seek KD duty positions as a CMF Cyber Defense Manager, CMF Team Lead, CMF Executive/Operations Officer, Cyber Protection Center (CPC) Cyber Operations Officer, detachment commander, Cyber Exploitation Team Chief, battalion XO/S3, or other unique positions of similar level of responsibility. Optimally, majors should spend 24 to 36 months in at least one of these positions.

(b) RC lieutenant colonel. Lieutenant colonels must have completed ILE common core to be competitive for promotion to colonel. To be best qualified, lieutenant colonels should seek duty positions as CMF Team Lead, Cyber Protection Center and/or Training Support Element Team commanders and deputy commanders, Army Reserve Cyber Operations Group (ARCOG), Cyber Training Support Element (CTSE), and/or Army Reserve Intelligence Support to Cyber Operations (ARISCO) operations officers, cyber effects support staff officers, battalion commanders, brigade-level XO/S3, and other staff principals. Optimally, lieutenant colonels should spend 24 to 36 months in at least one of these positions.

(c) RC colonel. Colonels serve as brigade-level commanders for ARCOG, CTSE, or ARISCO, in a variety of important staff positions to include USARC G-39, and in various Cyber branch related generalist positions at the State or National-level.

(d) RC selection board. Lieutenant colonels and colonels are selected for SSC by a RC selection board.

(2) 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.

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

(4) Branch transfers. RC Cyber officers may have to branch transfer during the course of their career due to lack of positions in their geographic area. When an officer transfers into the Cyber branch, completion of CyOOC and minimum time in a key position is required before branch qualification is complete. For AOC 17A/B, the qualification standards at each rank, as well as, PME requirements are the same as for AC officers. Commanders should closely manage branch transfer officers and assign them to a qualifying positions concurrent with enrollment in CyOOC or after completion of the course. Officers should not normally be assigned to a qualifying position prior to enrolling in or completing CyOOC.

(5) RC guidance. For further guidance on RC officer development, see Part One of DA PAM 600-3.

a. Constructive credit. RC officers (captain and above) who acquire cyberspace and EW operations related skills, knowledge, and abilities through civilian industry, education, or training may apply for 17A/B qualification training constructive credit. Approval authority for awarding 17A/B qualification training constructive credit is the Commandant, U.S. Army Cyber School. Constructive credit criteria is developed by U.S. Army Cyber School in close coordination with U.S. Army Cyber Command and U.S. Cyber Command.

Figure 3: 17A RC Officer Career Timeline

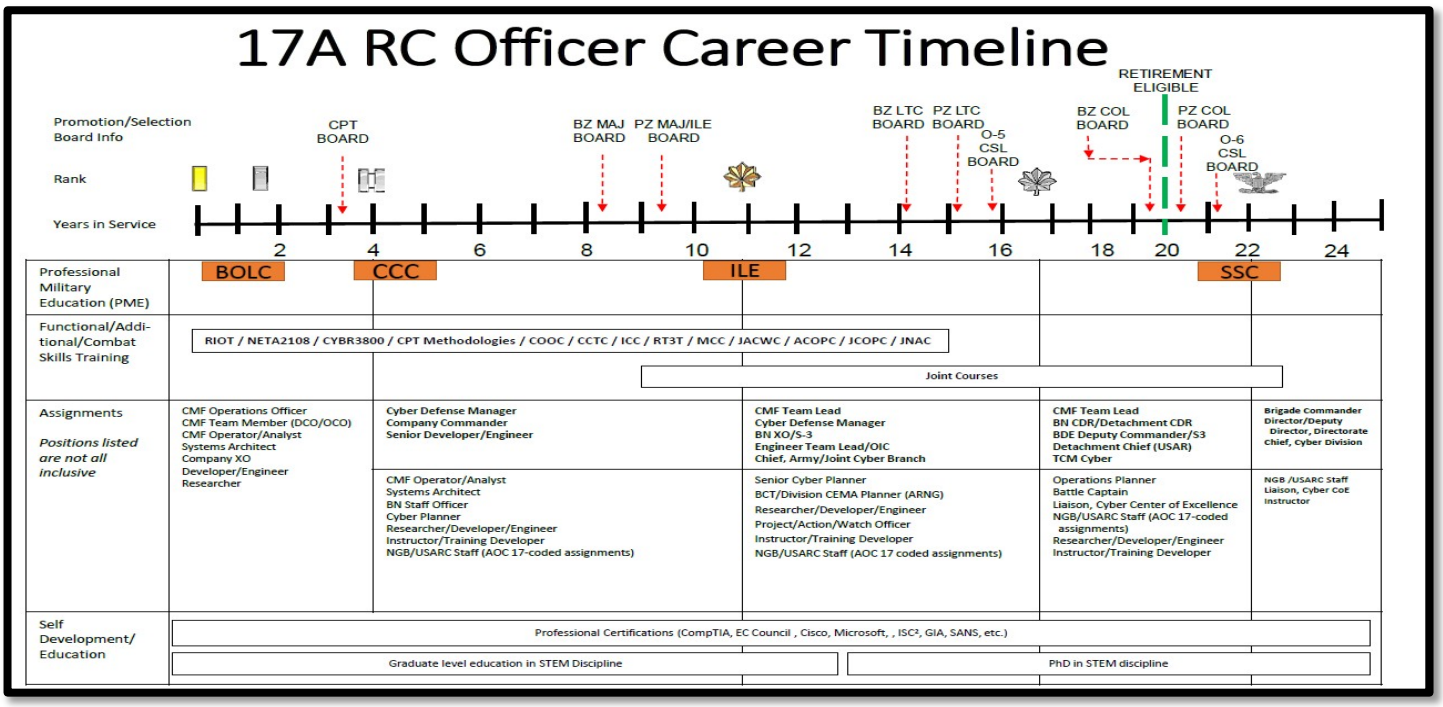
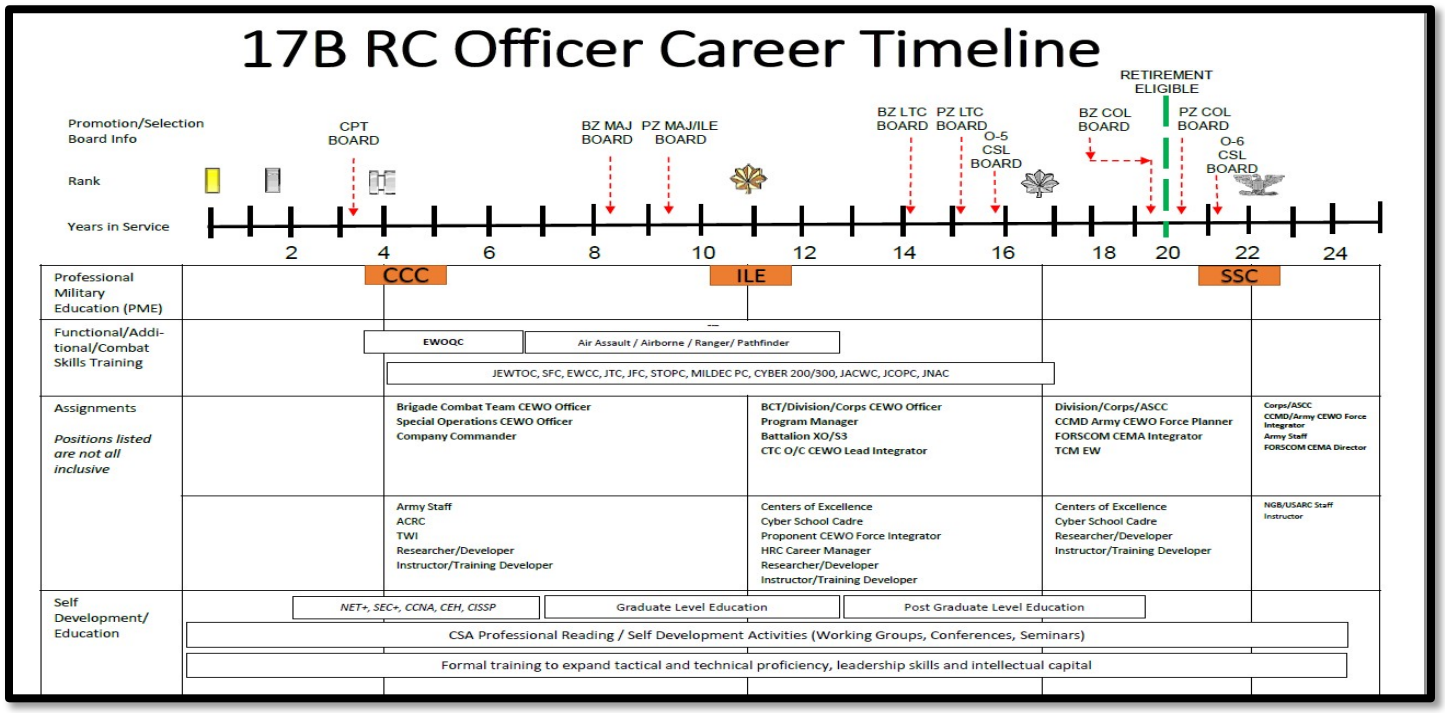


Figure 4: 17B RC Officer Career Timeline



5. Warrant officer development

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

(1) Cyber branch warrant officers are leaders and skilled technicians. They have technically-unique skills, knowledge, and attributes that require continual professional development.

(2) Cyber branch warrant officers must possess expert knowledge and skill in Cyberspace and Electronic Warfare operations supporting mission command; such knowledge and skill requires practical experience in tactics, combined arms operations and the employment of systems and processes.

(3) Cyber branch warrant officers sustain knowledge and skills through institutional training and education, duty in operational assignments and continuous self-development. Cyber branch warrant officers may deploy with units, teams, or as individuals to support Army, Joint, Interagency, Intergovernmental and Multinational (JIIM) applications of Cyberspace operations.

b. Cyber branch warrant officer military occupational specialties (MOSs). Cyber branch warrant officers are experts who provide technical and tactical expertise and experience as well as invaluable leadership throughout all levels of command. The following are MOSs for Cyber branch warrant officers: 170A - Cyber Operations Technician and 170B - Electronic Warfare Technician.

(1) 170A Cyber Operations Technician Active Component Warrant Officer development.

(a) Characteristics required of Cyber Operations Technician. Cyber Operations Technicians plan, supervise, assess and execute offensive and defensive Cyberspace operations. They lead small teams to accomplish unit objectives. They provide technical guidance, expertise and advice to commanders and their staff on the management and application of Army and JIIM Cyberspace operations. They must be consummate professionals; self-motivated and self-disciplined. They must be awarded and maintain a current TOP SECRET (TS) Sensitive Compartmented Information (SCI) clearance to maintain

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

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

(c) Assignments: Cyber Operations 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 unified land operations and multi-domain battles. Select Warrant Officers can also expect to receive assignments that broaden their experience as Cyber Operations Technicians and may serve in a generating force capacity such as the following:

1. Doctrine Writer
2. WOBC/WOAC Instructor/TAC Officer
3. Training/Course Developer
4. Army Cyber Institute Research Scientist
5. United States Military Academy Instructor
6. HRC Assignment Manager

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

1. Warrant Officer Cryptologic Career Program (WOCCP)
2. Computer Network Operations Development Program (CNODP)
3. Special Technical Operations Planners Course (V8)
4. Special Technical Operations Chief Course (V9)
5. Military Planners Courses
6. Military Targeting Courses

(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 technician.

(f) WO1/CW2 development.

1. *Entry level.* Upon warrant officer selection, all non-commissioned officers (warrant officer candidates upon arrival) will complete Warrant Officer Candidate School (WOCS). WOCS provides the basic skills necessary to prepare the warrant officer candidate to become an effective Army warrant officer. WOCS consists of two phases: Phase One is available as both distance learning (DL) and resident. Attendance at the resident phase is mandatory for all in the grade of E1 through E4 prior to entry into the program, non- PLDC/WLC/BLC (or equivalent) graduates in the grade of E5, and all prior service Air Force, Navy, or Coast Guard personnel who have not completed Army or Marine Corps basic training. All others will complete Phase One through DL. The Phase Two, five-week resident course at Fort Rucker, AL, is attended as resident training by all candidates. After graduation from WOCS and appointment to WO1, each officer will attend the 19-weeks and four days Warrant Officer Basic Course (WOBC) at Fort Gordon, GA.

2. *Education.* The 170A Cyber Operations Technician Basic Course provides Cyber Operations Technicians the education, training, and core skills necessary to successfully lead Cyberspace operations. The emphasis is for Army tactics, techniques, and procedures (TTP) to prepare the warrant officers to lead and direct the execution of authorized Cyber effects. Company grade warrant officers need to develop a basic understanding of technical integration of Cyberspace Defense; Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR); Cyberspace Surveillance and Reconnaissance (S&R) Cyberspace Operational Preparation of the Environment (OPE); and Cyberspace Attack in support of unified land operations and increase knowledge in a related special skill area to increase competitiveness. Completion of the Action Officer Development Course (AODC) is required once promoted to CW2 and prior to attending the Warrant Officer Advanced Course (WOAC). Completion of an associate's or baccalaureate degree is a recommended goal prior to becoming eligible for promotion to CW3.

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

(g) CW3 development.

1. *Education*. The 170A Warrant Officer Advanced Course (WOAC) focuses on advanced technical training and common leader development subjects designed to prepare officers for assignment in Field Grade Cyber Operations Technician positions. The residential course at the Army Cyber School at Fort Gordon, GA consists of 14-weeks of advanced technical and tactical training in Cyberspace Operations. The WOAC should be completed by the one year time-in-grade point as a CW3. The WOAC should be completed for promotion to CW4. Completion of a baccalaureate or master's degree in a related STEM discipline is also a recommended goal prior to becoming eligible for promotion to CW4.

2. *Desired experience*. CW3s must have the requisite senior-level expertise to perform one cyber work-role and should have experience in multiple work-roles prior to serving as a cyber mission force team senior technical advisor. Technical comprehension and competence in the management of Cyberspace Defense; Cyberspace ISR; Cyberspace S&R, Cyberspace OPE; and Cyberspace attack actions at the tactical and strategic-level should be mastered prior to becoming a senior warrant officer (CW4).

(h) CW4 development.

1. *Education*. The Warrant Officer Intermediate Level Education (WOILE) is a professional development course with a two-week Phase one distance learning (DL) portion, followed by a five-week resident Phase two portion taught at the Warrant Officer Career Center (WOCC), Fort Rucker, AL. 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 unified land operations through decisive action.

2. *Desired experience*. CW4s should have experience leading both offensive and defensive Cyberspace operations prior to being assigned to senior Cyber technical advisor positions. It is highly desirable that CW4s attain master-level expertise in at least one Cyber work-role, and must have

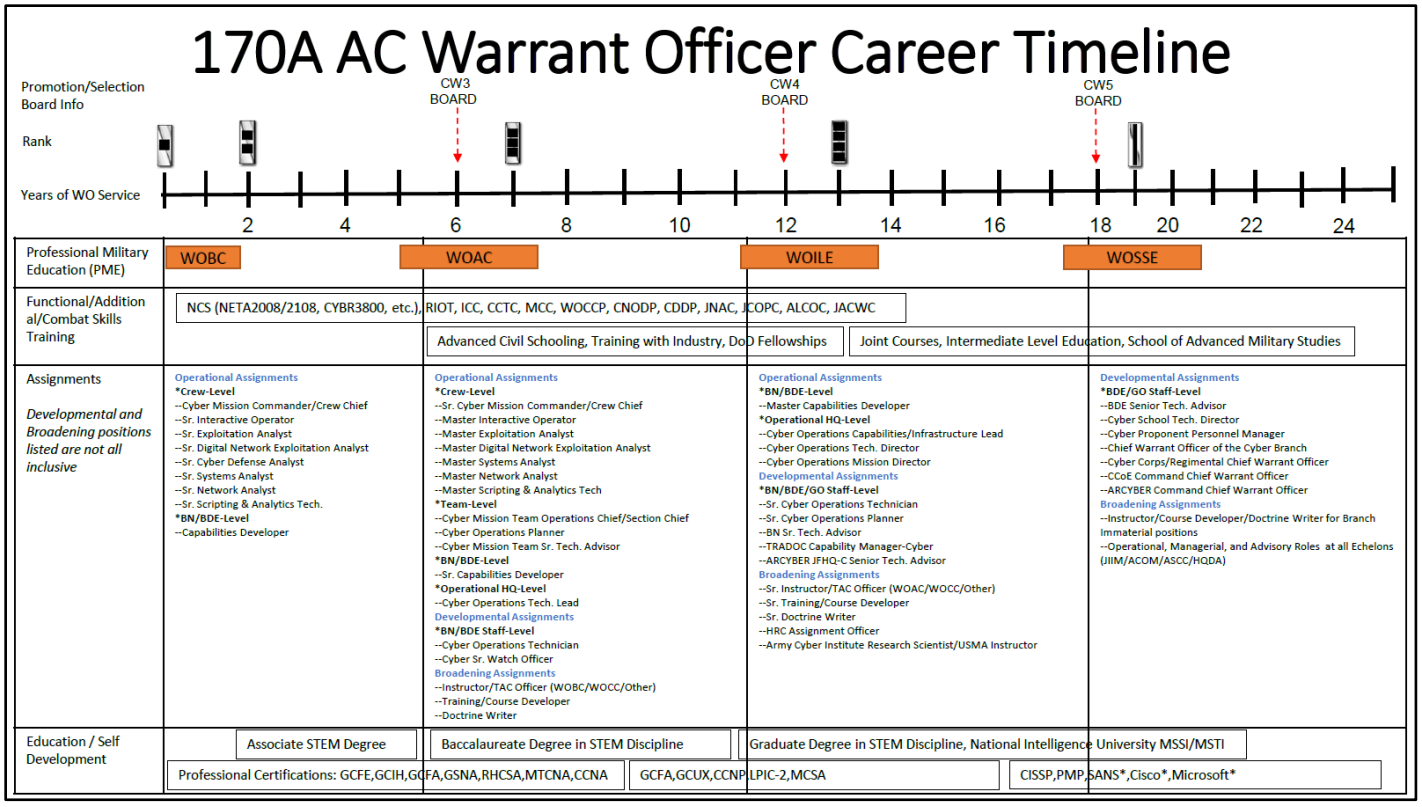
experience in multiple work-roles.

(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 in support of leaders on Army and strategic-level joint staffs during unified land operations. The WOSSE can be attended after one year time-in-grade to CW4 and should be completed by one year time- in-grade as a CW5. CW5s should continue work in an associated graduate-level field of study.

2. Desired experience. All CW5 170As should have cyber operational experience performing 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.

Figure 5: 170A AC Warrant Officer Career Timeline



(2) 170A Cyber Operations Technician Reserve Component Warrant Officer development.

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

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

(c) Training and development. Required training and recommended branch

developmental assignments by grade are as follows:

1. *Warrant officer one.* Must complete WOCS and WOBC before promotions to CW2. Assignments include team leader, and section chief. WO1 positions are concentrated in Cyber Protection Team TDA organizations within the USAR and ARNG.

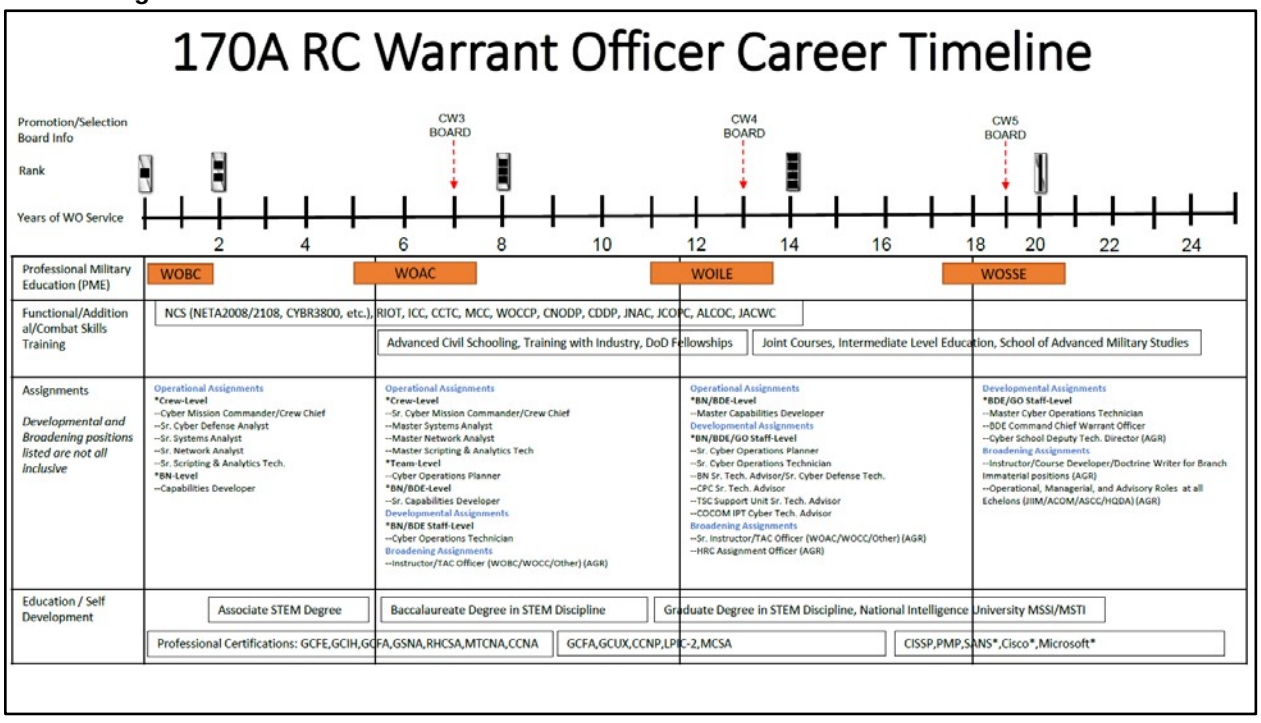
2. *Chief warrant officer two.* Warrant officer with at least one year time in grade as a CW2 can attend WOAC but must complete the course before promotion to CW3. Assignments include team leader, section chief, and operations chief. CW2 positions are concentrated in Cyber Protection Team TDA organizations within the USAR and ARNG.

3. *Chief warrant officer three.* Warrant officer with at least one year time-in-grade as a CW3 can attend WOILE but must complete the course before promotion to CW4. Assignments include, senior operations tech, systems architect, team leader, information protection technician, and instructor. CW3 positions are concentrated in Cyber Protection Team TDA organizations within the USAR and ARNG.

4. *Chief warrant officer four.* Warrant officer with at least one year time-in-grade as a CW4 can attend WOSSE but must complete the course before promotion to CW5. Assignments include senior technician, instructor, detachment commander and section or branch chief in a joint assignment. CW4 positions are concentrated in Cyber Protection Team TDA organizations within the USAR and ARNG.

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

Figure 6: 170A RC Warrant Officer Career Timeline



(2) 170A Cyber Operations Technician Reserve Component Warrant Officer development.

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

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

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

1. Warrant officer one. Must complete WOCS and WOBC before promotions to CW2. Assignments include team leader, and section chief. WO1 positions are concentrated in Cyber Protection Team TDA organizations within the USAR and ARNG.

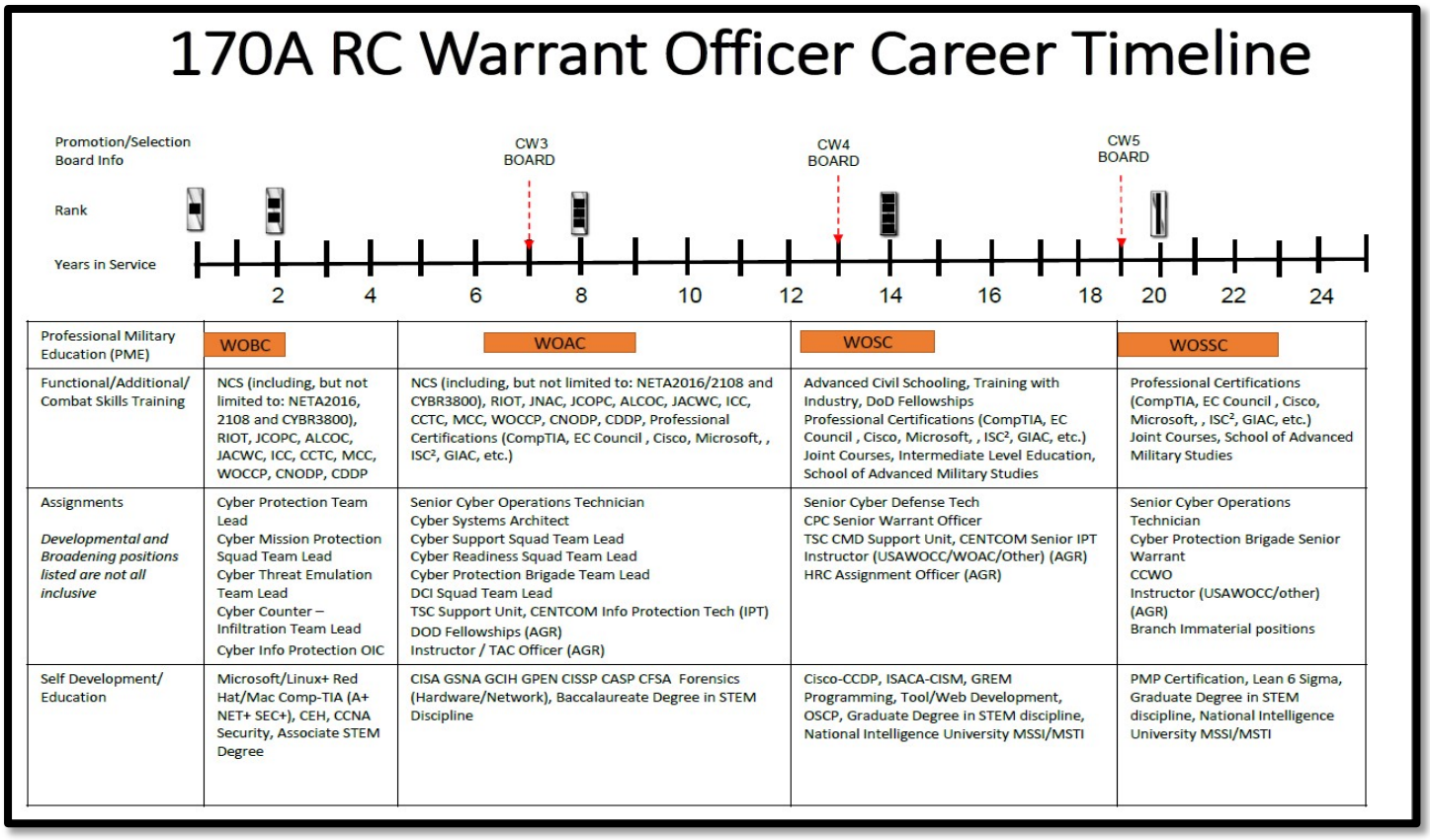
2. Chief warrant officer two. Warrant officer with at least one year time in grade as a CW2 can attend but must complete WOAC before promotion to CW3. Assignments include team leader, section chief, and operations chief. CW2 positions are concentrated in Cyber Protection Team TDA organizations within the USAR and ARNG.

3. Chief warrant officer three. Warrant officer with at least one year time in grade as a CW3 can attend but must complete WOILE before promotion to CW4. Assignments include, senior operations tech, systems architect, team leader, information protection technician, and instructor. CW3 positions are concentrated in Cyber Protection Team TDA organizations within the USAR and ARNG.

4. Chief warrant officer four. Warrant officer with at least one year time in grade as a CW4 can attend but must complete WOSSE before promotion to CW5. Assignments include senior technician, instructor, detachment commander and section or branch chief in a joint assignment. CW4 positions are concentrated in Cyber Protection Team TDA organizations within the USAR and ARNG.

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

Figure 6: 170A RC Warrant Officer Career Timeline



Professional Military Education (PME)	WOBC	WOAC	WOSC	WOSSC
Functional/Additional/ Combat Skills Training	NCS (including, but not limited to: NETA2016, 2108 and CYBR3800), RIOT, JCOPC, ALCOC, JACWC, ICC, CCTC, MCC, WOCCP, CNODP, CDDP	NCS (including, but not limited to: NETA2016/2108 and CYBR3800), RIOT, JNAC, JCOPC, ALCOC, JACWC, ICC, CCTC, MCC, WOCCP, CNODP, CDDP, Professional Certifications (CompTIA, EC Council , Cisco, Microsoft, , ISC², GIAC, etc.)	Advanced Civil Schooling, Training with Industry, DoD Fellowships Professional Certifications (CompTIA, EC Council , Cisco, Microsoft, , ISC², GIAC, etc.) Joint Courses, Intermediate Level Education, School of Advanced Military Studies	Professional Certifications (CompTIA, EC Council , Cisco, Microsoft, , ISC², GIAC, etc.) Joint Courses, School of Advanced Military Studies
Assignments *Developmental and Broadening positions listed are not all inclusive*	Cyber Protection Team Lead Cyber Mission Protection Squad Team Lead Cyber Threat Emulation Team Lead Cyber Counter – Infiltration Team Lead Cyber Info Protection OIC	Senior Cyber Operations Technician Cyber Systems Architect Cyber Support Squad Team Lead Cyber Readiness Squad Team Lead Cyber Protection Brigade Team Lead DCI Squad Team Lead TSC Support Unit, CENTCOM Info Protection Tech (IPT) DOD Fellowships (AGR) Instructor / TAC Officer (AGR)	Senior Cyber Defense Tech CPC Senior Warrant Officer TSC CMD Support Unit, CENTCOM Senior IPT Instructor (USAWOCC/WOAC/Other) (AGR) HRC Assignment Officer (AGR)	Senior Cyber Operations Technician Cyber Protection Brigade Senior Warrant CCWO Instructor (USAWOCC/other) (AGR) Branch Immaterial positions
Self Development/ Education	Microsoft/Linux+ Red Hat/Mac Comp-TIA (A+ NET+ SEC+), CEH, CCNA Security, Associate STEM Degree	CISA GSNA GCIH GPEN CISSP CASP CFSA Forensics (Hardware/Network), Baccalaureate Degree in STEM Discipline	Cisco-CCDP, ISACA-CISM, GREM Programming, Tool/Web Development, OSCP, Graduate Degree in STEM discipline, National Intelligence University MSSI/MSTI	PMP Certification, Lean 6 Sigma, Graduate Degree in STEM discipline, National Intelligence University MSSI/MSTI

(3) 170B Cyber and Electronic Warfare Operations Technician Active Component Warrant Officer development.

(a) Characteristics required of Cyber and Electronic Warfare Operations Technician. The 170B Cyber and Electronic Warfare Operations Technician (CEWOT), plans, directs, supervises, and assesses Cyberspace operations (CO) and Electronic Warfare (EW) operations. The Cyber and Electronic Warfare Operations Technicians serves as the technical and tactical EW expert prepared to organize, manage, and lead small teams to accomplish unit objectives. They provide technical guidance, expertise and advice to commanders and staffs on the management and operation of Army, Joint, Interagency, and Multinational applications of Cyberspace Operations and EW operations. They must be the consummate professional; 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 Cyber and Electronic Warfare Operations Technician. The Cyber and Electronic Warfare Operations Technician is a Subject Matter Expert (SME) on Electronic Warfare, and is a leader, trainer, and advisor to commanders at all levels. The Cyber and Electronic Warfare Operations Technician analyzes, plans, organizes, implements, monitors, integrates, and assesses EW operations, threat environment, and technical requirements. The Cyber and Electronic Warfare Operations Technician synchronizes effects with the fires cell/section to disrupt or destroy EW targets, whether by lethal or nonlethal means. The Cyber and Electronic Warfare Operations Technician provides advice on the technical and tactical employment of both organic and non-organic EW systems. The Cyber and Electronic Warfare Operations Technician should have an understanding and comprehension in general aspects of Cyberspace Operations and in the Cyber Mission Force (CMF). Cyber and Electronic Warfare Operations Technicians facilitates and manages unit maintenance, oversight, and training programs as it pertains to EW. Cyber and Electronic Warfare Operations Technicians are mainly accessed from Cyber and Electronic Warfare Operations Specialists (17E) who possess a high degree of success spanning multiple echelons and demonstrate technical expertise in all facets of EW. Cyber and Electronic Warfare Operations Technicians perform the following key functions/tasks:

1. Advise commanders on capabilities and employment of Cyberspace Electromagnetic Activities assets and capabilities.

2. Execute Electronic Attack in support of a commander's requirements.

3. Conduct Electronic Warfare Support to meet commander's requirements (geolocation, direction finding).

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

5. Monitor electromagnetic spectrum (EMS) for indications and warnings enabling immediate threat recognition and targeting.

6. Determine intelligence requirements, priorities, Target Selection Standards, attack guidance, and targeting objectives for Cyber Electromagnetic Activities.

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

8. Deconflict electronic attack/EW support with the Analysis Control Element and Collection Management in the collection process.

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

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

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

(c) Assignments: Cyber and Electronic Warfare Operations Technicians are primarily assigned to units corps and below. These assignments allow tactical commanders exposure to Cyberspace operations in support of unified land operations. Select Warrant Officers can also expect to receive assignments that broaden their experience as Cyber and Electronic Warfare Operations Technicians and may serve in a generating force capacity such as the following:

1. HRC Assignment Officer/Career Manager
2. TRADOC Capabilities Manager
3. Doctrine Writer
4. WOBC/WOAC Instructor
5. COCOM Senior CEMA Adviser
6. Army Cyber Institute Researcher
7. Battle Lab CEMA Technician

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

1. Joint EW Theater Operations Course
2. Special Technical Operations Planners Course (V8)
3. Special Technical Operations Chief Course (V9)
4. EW Coordination Course
5. Space Cadre Course (3Y)
6. Cyber 200/300
7. Joint Firepower Course
8. Joint Advanced Cyber Warfare Course
9. Military Deception Planners Course
10. Aerial Precision Geolocation Course (V3)
11. Close Access Tactical-Recon (CAT-R)
12. NATO EW Course
13. NATO Targeting Course
14. Joint Cyber Analysis Course (JCAC) (Q3)

(e) Self-development. Lifelong learning, supported by both 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 Electronic Warfare Operations Technician based on current and projected duty assignments.

(f) WO1/CW2 development.

1. Entry level. Upon warrant officer selection, all non-commissioned officers (warrant officer candidates upon arrival) will complete Warrant Officer Candidate School (WOCS). WOCS provides the basic skills necessary to prepare the warrant officer candidate to become an effective Army warrant officer. WOCS consists of two phases: Phase 1 is available as both distance learning (DL) and resident. Attendance at the resident phase is mandatory for all in the grade of E1 through E4 prior to entry into the program, non-PLDC/WLC (or equivalent) graduates in the grade of E5, and all prior service Air Force, Navy, or Coast Guard personnel who have not completed Army or Marine Corps basic training. All others will complete Phase 1 through DL. The Phase 2, five-week resident course at Fort Rucker, AL, is attended as resident training by all candidates. After graduation from WOCS and appointment to WO1, each officer will attend the 15-week Warrant Officer Basic Course (WOBC) at Fort Sill, OK.

2. Education. The 170B Cyber and Electronic Warfare Operations Technician Basic Course provides Cyber and Electronic Warfare Operations Technicians the education, training, and core skills necessary to successfully lead Cyberspace operations. The emphasis is for Army tactics, techniques, and procedures to prepare the warrant officers to lead and direct the execution of authorized effects throughout the electromagnetic spectrum. Company grade warrant officers need to develop a basic understanding of technical integration of effects of friendly and adversary EW systems on the electromagnetic spectrum, Cyberspace Electromagnetic Activities concepts, Cyberspace Operational Preparation of the Environment (OPE), and offensive/defensive Cyberspace actions in support of unified land operations. Completion of the Action Officer Development Course (AODC) is required once promoted to CW2 and before attendance to the Warrant Officer Advanced Course. Completion of an associate's or baccalaureate degree is a recommended goal prior to becoming eligible for promotion to CW3.

3. Desired experience. Junior Cyber and Electronic Warfare Operations Technicians must attain and maintain expertise on the science of signal theory, application of electronic order of battle, and the request, limitation, and application of Cyber effects for implementation at corps and below. Continuous education, training, and experience in the coordination and execution of Cyber Electromagnetic Activities operations 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 officers for assignment in Field Grade Cyber and Electronic Warfare Operations Technician positions. The residential course at Fort Sill, OK consists of 8-weeks of advanced technical and tactical training in Electronic Warfare and Cyberspace Operations. The WOAC should be completed by the one year time in grade point as a CW3. The WOAC must be completed for promotion to CW4. Completion of a baccalaureate or master's degree in a related STEM discipline is also a recommended goal prior to becoming eligible for promotion to CW4.

2. Desired experience. CW3s should have requisite journeyman-level expertise, technical comprehension, and competence in the employment of Cyberspace Electromagnetic Activities assets and capabilities at the tactical level should be mastered prior to becoming a senior warrant officer (CW4).

(h) CW4 development.

1. Education. The Warrant Officer Intermediate Level Education (WOILE) is a professional development course with a two-week Phase one distance learning (DL), followed by a five-week resident Phase two taught at the Warrant Officer Career Center (WOCC), Fort Rucker, AL. 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 unified land operations through decisive action.

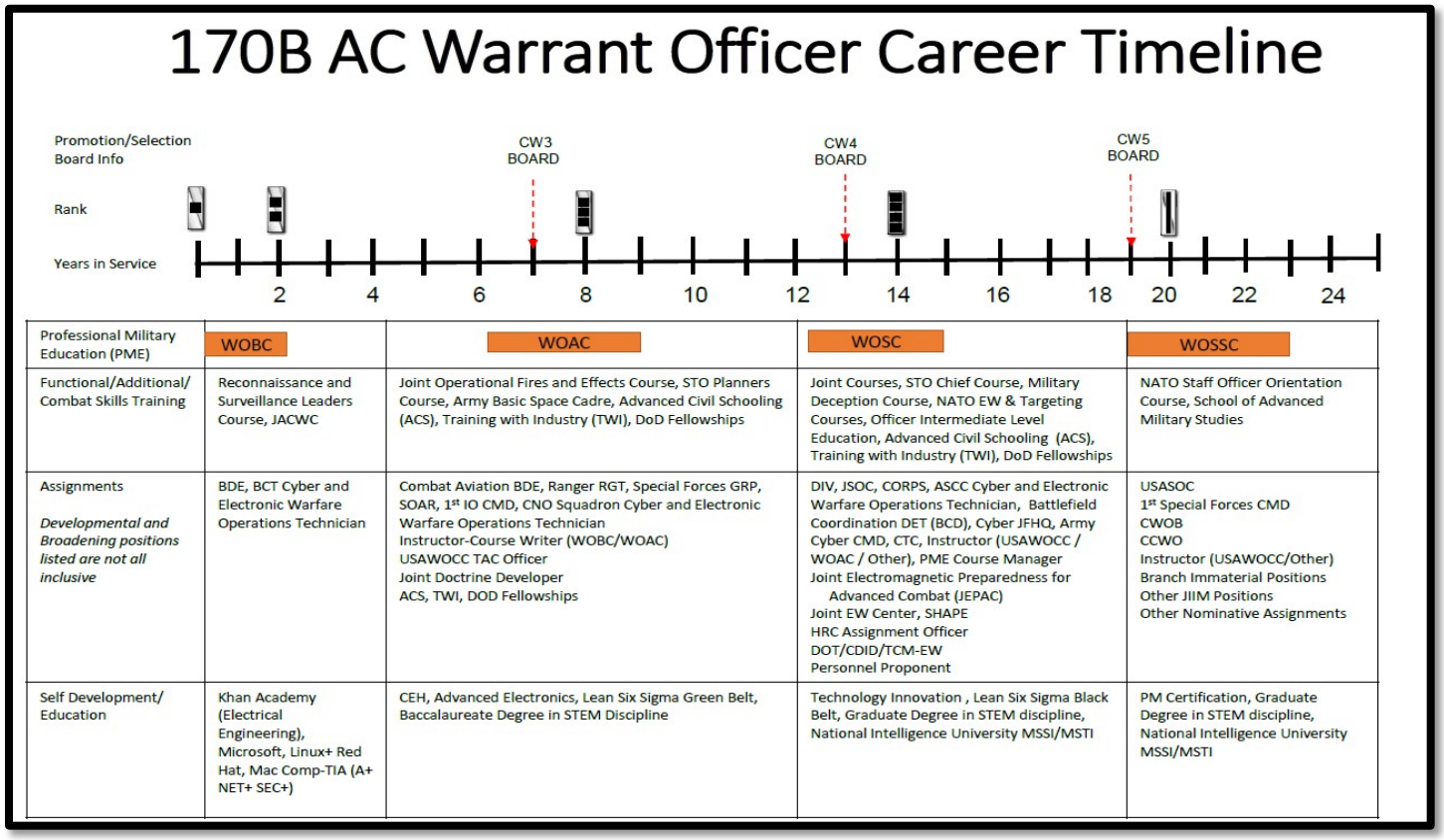
2. Desired experience. CW4s should have experience leading Cyberspace operations and Cyber Electromagnetic Activities at corps and below prior to being assigned to senior broadening or joint positions.

(i) CW5 Development.

1. Education. The Warrant Officer Senior Service Education (WOSSE) is a two phase course consisting of a Phase one (DL) followed by a four-week Phase two (resident) course attended by the Army's most senior warrant officers at Fort Rucker, AL. The educational goal is to provide senior CW4s or new CW5s with the master-level education, knowledge, and influential leadership skills necessary to apply their technical expertise in support of leaders on strategic-level joint staffs during unified land operations. The WOSSE can be attended after one year time in grade to CW4 and should be completed by one year time in grade as a CW5. CW5s should continue work in an associated graduate-level field of study.

2. Desired experience. All CW5 170Bs should have operational experience at all levels, and have attained proficiency of all critical tasks through combined experiences and career self-development in every facet of their career path.

Figure 7: 170B AC Warrant Officer Career Timeline



Professional Military Education (PME)	WOBC	WOAC	WOSC	WOSSC
Functional/Additional/ Combat Skills Training	Reconnaissance and Surveillance Leaders Course, JACWC	Joint Operational Fires and Effects Course, STO Planners Course, Army Basic Space Cadre, Advanced Civil Schooling (ACS), Training with Industry (TWI), DoD Fellowships	Joint Courses, STO Chief Course, Military Deception Course, NATO EW & Targeting Courses, Officer Intermediate Level Education, Advanced Civil Schooling (ACS), Training with Industry (TWI), DoD Fellowships	NATO Staff Officer Orientation Course, School of Advanced Military Studies
Assignments *Developmental and Broadening positions listed are not all inclusive*	BDE, BCT Cyber and Electronic Warfare Operations Technician	Combat Aviation BDE, Ranger RGT, Special Forces GRP, SOAR, 1st IO CMD, CNO Squadron Cyber and Electronic Warfare Operations Technician Instructor-Course Writer (WOBC/WOAC) USAWOCC TAC Officer Joint Doctrine Developer ACS, TWI, DOD Fellowships	DIV, JSOC, CORPS, ASCC Cyber and Electronic Warfare Operations Technician, Battlefield Coordination DET (BCD), Cyber JFHQ, Army Cyber CMD, CTC, Instructor (USAWOCC / WOAC / Other), PME Course Manager Joint Electromagnetic Preparedness for Advanced Combat (JEPAC) Joint EW Center, SHAPE HRC Assignment Officer DOT/CDID/TCM-EW Personnel Proponent	USASOC 1st Special Forces CMD CWOB CCWO Instructor (USAWOCC/Other) Branch Immaterial Positions Other JIIM Positions Other Nominative Assignments
Self Development/ Education	Khan Academy (Electrical Engineering), Microsoft, Linux+ Red Hat, Mac Comp-TIA (A+ NET+ SEC+)	CEH, Advanced Electronics, Lean Six Sigma Green Belt, Baccalaureate Degree in STEM Discipline	Technology Innovation , Lean Six Sigma Black Belt, Graduate Degree in STEM discipline, National Intelligence University MSSI/MSTI	PM Certification, Graduate Degree in STEM discipline, National Intelligence University MSSI/MSTI

(4) 170B Cyber and Electronic Warfare Operations 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 electronic warfare technical assignments that yield the same developmental opportunities as their AC counterparts.

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

1. Warrant officer one. Must complete WOCS and WOBC before promotions to CW2. Assignments include EW technical advisor and team chief. WO1 positions are concentrated in brigade level MTOE organizations.

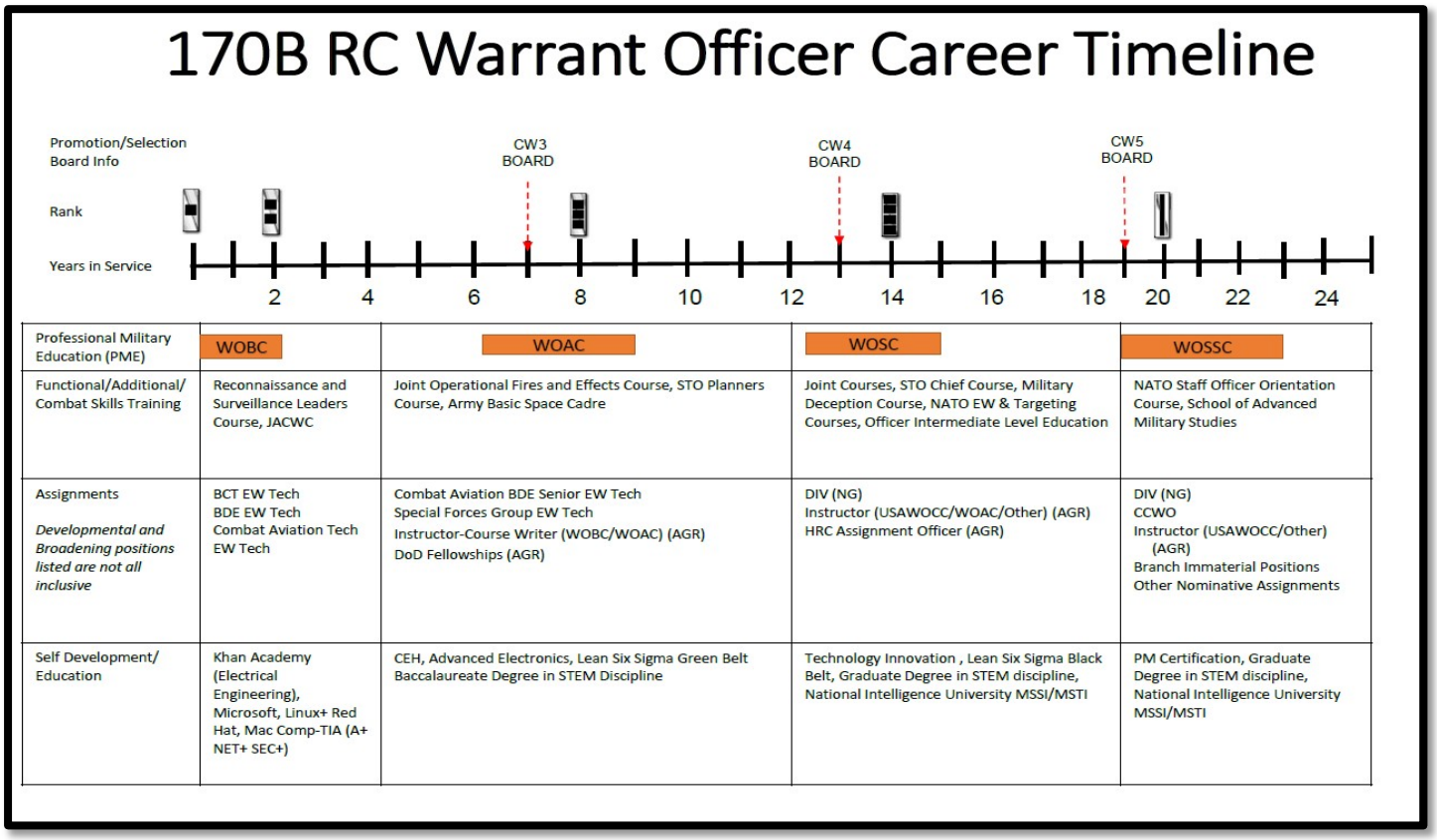
2. Chief warrant officer two. Warrant officer with at least one year time in grade as a CW2 can attend but must complete WOAC before promotion to CW3. Assignments include technical advisor, team chief, section chief, and platoon leader. CW2 positions are concentrated in brigade level MTOE organizations.

3. Chief warrant officer three. Warrant officer with at least one year time in grade as a CW3 can attend but must complete WOILE before promotion to CW4. Assignments include EW technical advisor, team chief platoon leader, and instructor. CW3 positions are concentrated in brigade level TDA organizations within the USAR and the ARNG.

4. Chief warrant officer four. Warrant officer with at least one year time in grade as a CW4 can attend but must complete WOSSE before promotion to CW5. Assignments include senior EW technical advisor and instructor. CW4 positions are concentrated in division level TDA organizations within the USAR and ARNG.

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

Figure 8: 170B RC Warrant Officer Career Timeline



Professional Military Education (PME)	WOBC	WOAC	WOSC	WOSSC
Functional/Additional/ Combat Skills Training	Reconnaissance and Surveillance Leaders Course, JACWC	Joint Operational Fires and Effects Course, STO Planners Course, Army Basic Space Cadre	Joint Courses, STO Chief Course, Military Deception Course, NATO EW & Targeting Courses, Officer Intermediate Level Education	NATO Staff Officer Orientation Course, School of Advanced Military Studies
Assignments *Developmental and Broadening positions listed are not all inclusive*	BCT EW Tech BDE EW Tech Combat Aviation Tech EW Tech	Combat Aviation BDE Senior EW Tech Special Forces Group EW Tech Instructor-Course Writer (WOBC/WOAC) (AGR) DoD Fellowships (AGR)	DIV (NG) Instructor (USAWOCC/WOAC/Other) (AGR) HRC Assignment Officer (AGR)	DIV (NG) CCWO Instructor (USAWOCC/Other) (AGR) Branch Immaterial Positions Other Nominative Assignments
Self Development/ Education	Khan Academy (Electrical Engineering), Microsoft, Linux+ Red Hat, Mac Comp-TIA (A+ NET+ SEC+)	CEH, Advanced Electronics, Lean Six Sigma Green Belt Baccalaureate Degree in STEM Discipline	Technology Innovation , Lean Six Sigma Black Belt, Graduate Degree in STEM discipline, National Intelligence University MSSI/MSTI	PM Certification, Graduate Degree in STEM discipline, National Intelligence University MSSI/MSTI