Report 1337.1

A Proposed Army Information Dominance Officer Education Model

David R. Raymond

Department of Electrical Engineering & Computer Science
United States Military Academy
West Point, NY 10996
{david,raymond} @usma.edu

Vol 1337 No. I
30 September 2013

ACI
Army Cyber Institute

A Proposed Army Information Dominance Officer Education Model

LTC David R. Raymond, Ph.D.
Army Cyber Center
30 September 2013

Abstract

Success in cyberspace operations requires strong leaders with expertise spanning the domains of communications, information technology, signals intelligence, and electronic warfare. The Army's cyber operators are currently a mixture of basic branch and functional area officers and Soldiers from the Signal and Military Intelligence (MI) Corps, as well the newly emerging Electronic Warfare (EW) functional area (29 Series). Analysis is underway by key stakeholders to determine the best way forward for the Army's cyber force. One possible way ahead, suggested by General Alexander, Commander of U.S. Cyber Command and Director of the NSA, is for a new Cyber Corps to emerge from and possibly replace the Army's Signal Corps, MI Corps, EW Corps, and current cyber operators.[1] This approach has the potential to focus the Army's cyber security efforts and increase efficiency in facilities and training programs. I will refer to this new group as the Information Dominance Corps, a term currently used by the U.S. Navy. This paper proposes an education plan for Army Information Dominance officers during their entire career, with a special emphasis on immediate post-commissioning education and training. This plan is designed to produce officers that can function across the cyber and kinetic domains and integrate information technology, signals intelligence, and electronic warfare capabilities so they are prepared to employ cyberspace systems, information, and capabilities to achieve military objectives and to deny adversaries the ability to do the same.

1. Introduction

Herein we propose an overview of Information Dominance officer education from pre-commissioning through the rank of Colonel based on Army training policy and on an analysis of the education currently provided officers in the Signal, MI, and electronic warfare (EW) career fields. We assume that the Information Dominance (ID) Officer Corps will replace and incorporate the Signal corps including basic branch 25 (Signal), functional areas 24 (Telecommunications Engineering) and 53 (Information Systems Management), the Signals Intelligence (SIGINT) specialty from the Military Intelligence corps (and perhaps the entire MI branch), and the Electronic Warfare functional area. Education for these officers must, therefore, incorporate sufficient signal and intelligence topics for officers to be successful in roles that require those skills, plus it must include cyber operations coverage to tie these domains into one coherent whole. This paper focuses on ID officer education. Similar analyses must be done with the ID Warrant Officer, NCO, and enlisted Military Occupational Specialties.

Specific emphasis is given to immediate post-commissioning officer training. While an overview of an ID Captain's Career Course is given, the training that newly commissioned ID officers should receive to prepare them for their futures in this new career field receives much more detailed coverage. Officer branch designation is currently not predicated on undergraduate area of study, however, the ID corps would be best served by officers with a technical background and a firm grounding in computer science,

[1] R. Ackerman, "Cyber Command Redefines the Art," 1 June 2013. [Online]. Available: http://www.afcea.org. [Accessed 9 July 2013].

information technology, computer engineering, electrical engineering, or other cyber-related disciplines. To maximize the value of the Army's investment in undergraduate education programs and avoid squandering the limited pool of available talent, we advocate creating a strong linkage between cyber-related undergraduate degrees and a newly commissioned officer's selection as an ID officer. A technical, cyber-related education at the undergraduate or graduate level may even become a prerequisite for entry into some of the more specialized, hands-on ID sub-fields.

The doctrinal basis for U.S. Army officer education is Army Regulation (AR) 350-1, Army Training and Leader Development.[2] Section IV of this regulation lays out the general guidelines for officer education spanning an officer's career and specifies the system's goal.

> *The goal of the [Officer Education System] is to produce a corps of leaders who are fully competent in technical, tactical, and leadership skills, knowledge, and experience; are knowledgeable of how the Army runs; are prepared to operate in Joint, interagency, intergovernmental, and multinational (JIIM) environments; demonstrate confidence, integrity, critical judgment, and responsibility; can operate in an environment of complexity, ambiguity, and rapid change; can build effective teams amid organizational and technological change; and can adapt to and solve problems creatively.*
>
> AR 350-1, Paragraph 3-26

The education plan for ID officers presented in this document is in line with these goals.

We begin with a proposed ID Officer Education Strategy that provides a roadmap for ID officer training and education from pre-commissioning through Colonel. We then discuss education for ID lieutenants in detail. An overview of ID captain's education follows. Appendix A proposes a program of instruction (POI) for the ID Basic Officer Leader's Course (BOLC) and subsequent appendices provide POIs for assignment-specific courses following the common BOLC course taken by all ID officers.

2. Information Dominance Officer Education Strategy

Each Army branch and functional area has a two-digit identifier. In this education strategy discussion, we use 26 as the basic branch designator for the Information Dominance corps. The 2 represents the intelligence functions generally carried out by a unit S2, G2, or J2, and the 6 represents the telecommunications responsibilities of the S6, G6, or J6. Since the ID corps largely subsumes the signal and MI corps, we add one-character area of concentration (AOC) identifiers and skill identifiers (SI) to indicate specialized skills, some derived from current Signal, MI, and other AOCs. Figure 1, which visually depicts the sequence of ID officer courses, also indicates AOCs and SIs obtained in various training courses.

As per AR 350-1 and TRADOC Regulation 350-36, Basic Officer Leader Training Policies and Administration[3], all Information Dominance officers will complete Basic Officer's Leader Course, part A (BOLC-A) as part of the pre-commissioning training at the United Stated Military Academy, in the Reserve Officer Training Corps, or during Officer Candidate School. BOLC-A provides a basis of Army

[2] Headquarters, Department of the Army, *Army Regulation 350-1: Army Training and Leader Development,* Washington, DC, 18 Dec. 2009.

[3] U.S. Army Training and Doctrine Command, *TRADOC Regulation 350-36: Basic Officer Leader Training Policies and Administration,* Fort Eustis, VA, 19 Oct. 2012.

training and professional development to prepare lieutenants for commissioning and for success in BOLC-B. BOLC-A outcomes include an understanding of Army values, ethics, professionalism, officership, and personal development, along with technical and tactical competence and leadership experience required of newly-commissioned officers.

The first branch-specific cyber operations education ID officers will receive is IDBOLC-B. We recommend that the Cyber Center of Excellence (CoE) at Ft. Gordon be the proponent for this course. IDBOLC-B will begin with a 16 week course that trains all lieutenants in a single baseline Area of Concentration (AOC) and awards AOC 26C, Cyber Operations Officer. This course incorporates the BOLC-B common core critical task list specified in TRADOC Reg 350-36, plus relevant communications, information technology, SIGINT, and EW topics from the U.S. Army Intelligence Center of Excellence (USAICoE), the U.S. Army Cyber CoE (USACCoE), and the Fires COE. Additional coverage of cyber operations beyond those currently included in a BOLC is also part of this new course.

An ID officer will graduate IDBOLC-B with the skills and expertise necessary to serve as a successful battalion intelligence collection coordinator (BICC) or battalion signal officer (S6), as a platoon leader in a Signal or MI battalion, as an electronic warfare staff officer, or as a computer network operations or defense team leader in a cyber operations organization such as the 780th MI brigade, the 1st Information Operations Command, or the National Security Agency. To maximize their potential and make ID officers true experts in the skills required for their initial assignments, we recommend that officers attend follow-on courses after the common IDBOLC-B course. This is a common approach used across the Army. For example, an Armor officer may attend follow-on courses to serve as a Battalion

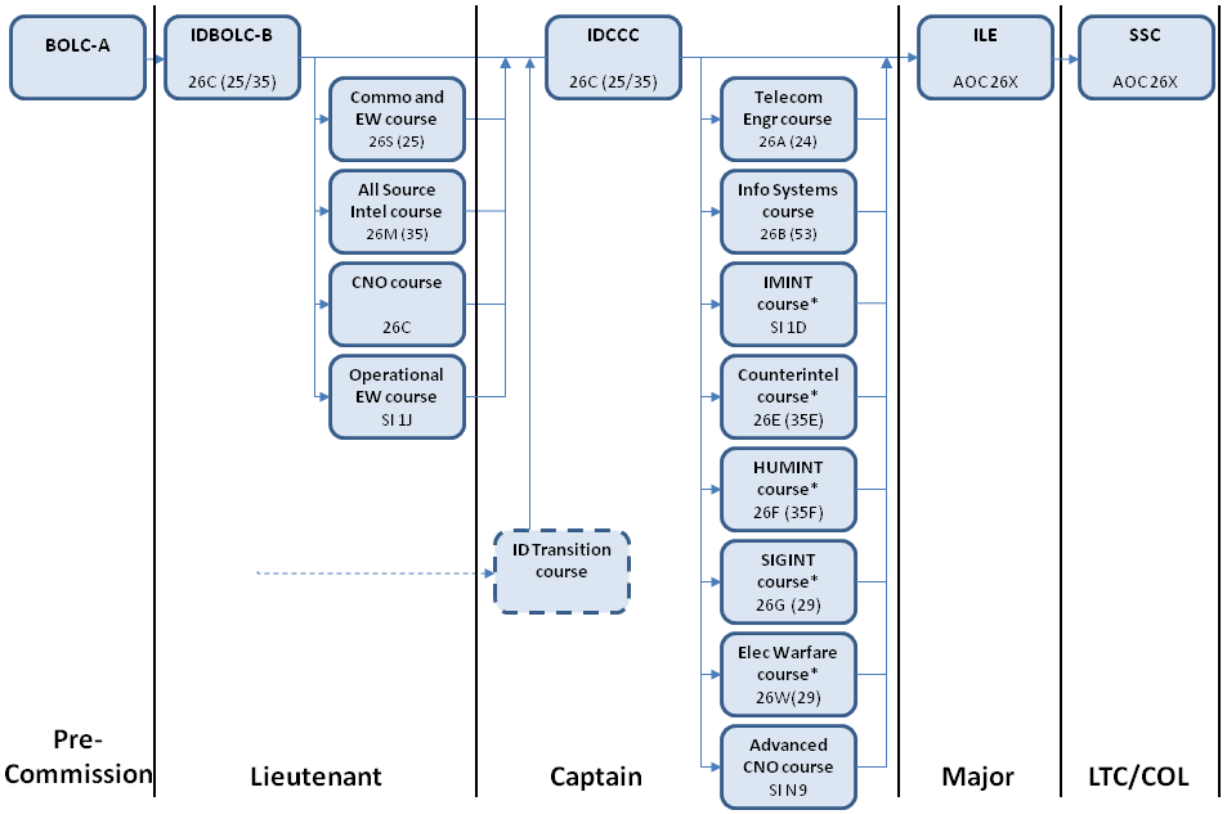

*Figure 1. Proposed ID Officer Training System. Each box represents a course and graduates will be awarded the AOC or SI shown. Numbers in parenthesis are the corresponding AOCs under the current branch and functional area numbering system. AOC 26X is used to refer to any 26-series officer. In rare instances, ID Lieutenants may take Captain-level courses indicated with *.*

Maintenance Officer or Scout Platoon leader. ID officer training will be aligned functionally to reduce duplication of effort between the Cyber (formerly Signal) and Intelligence Centers of Excellence much like the way the Maneuver Center of Excellence (MCoE) at Fort Benning has realigned officer training for Armor and Infantry officers along functional lines.[4]

After their common BOLC-B experience, ID officers should attend 4 to 7 weeks of additional training to prepare them for their first assignments. Most of this training will be functionally aligned with the Cyber and Intelligence CoEs and will take place at either Fort Gordon or Fort Huachuca. Officers destined for assignments as battalion communications officers or platoon leaders in a Signal unit will attend the Cyber Officer's Communications and Electronic Warfare functional training course and will be awarded AOC 26S, Communications-Electronics Operations. Those assigned to serve as battalion intelligence coordinators or platoon leaders in an MI Battalion should attend the Cyber Officer's All Source Intelligence functional training and be awarded AOC 26M, Cyber Intelligence Officer. This functional training is designed to ensure officers are successful in their initial assignments and does not permanently relegate them to the communications or intelligence functional areas. It should be possible to earn qualifications in multiple AOCs, thus it is possible for an officer with appropriate training to be qualified as both a 26S and a 26M. This model has proven successful in the past, for example, Military Intelligence Officers could be qualified as both a 35D (Tactical Intelligence Officer) and 35G (Signals Intelligence Officer) and serve in either type of position. This is not an exhaustive list of potential follow-on courses for Information Dominance officers after BOLC-B. There are likely other follow on courses, such as the Joint Network Attack Course (JNAC) offered by U.S. Cyber Command's Center for Information Dominance at Corry Station in Pensacola, FL, for ID lieutenants destined for computer network operations (CNO) assignments[5] and the Army Operational Electronic Warfare Course offered by the Fires COE at Fort Sill, OK. Courses such as these can be used to assign skill identifiers to provide assignments officers and organizations higher resolution in requesting and assigning desired personnel.

To maximize promotion potential and benefit to the Army, ID officers are encouraged to serve assignments spanning the cyber domain, including the communications, electronic warfare, intelligence, and computer network operations domains. As the ID officer management model matures, future changes may be made as desired to front-load certain types of training and operational experiences earlier in an officer's career. As an example, it may make sense for officers to first serve in a network operations role before taking on an offensive cyber operations assignment.

After graduating IDBOLC-B, any follow-on courses, and completing their first assignments, ID Officers will attend the Information Dominance Captain's Career Course (IDCCC). ID officers may attend other branch captain's career courses by exception. Non-ID officers transitioning into the ID Corps must complete the Information Dominance Transition Course before attending IDCCC. The transition course model has long been used successfully by the Military Intelligence branch as they accept transfers who served their first tour in other branches. After completion of IDCCC, branch detailed officers will be awarded the AOC 26C. Following IDCCC, officers may again attend functional courses specific to their next assignment in Advanced Communications-Electronics Operations (AOC 26S), Signals Intelligence (AOC 26M), Electronic Warfare (AOC 26T), Imagery Intelligence (SI 1D), Counterintelligence (AOC 26E),

---

[4] L. Egan, "Maneuver Center of Excellence to use university model to maximize efficiency," 1 May 2013. [Online]. Available: http://www.army.mil/article/102358/. [Accessed 22 July 2013].

[5] MARDET Corry Station, "Joint Network Attack Course (JNAC)," 2013. [Online]. Available: https://www.mcis.usmc.mil. [Accessed 12 July 2013].

Human Intelligence (AOC 26F), Signals Intelligence (AOC 26G), Telecommunications Engineering (AOC 26A), Information Systems Management (AOC 26B), Electronic Warfare (AOC 26W), or an advanced CNO course that will award the Computer Network Operations Planner skill identifier (SI N9). Again, it is possible, and perhaps likely that officers will become qualified in multiple AOCs.

Mid-career ID officers will attend Intermediate-Level Education with their peer group to update them on Army warfighting doctrine and provide learning opportunities to help them develop as self-aware and adaptive leaders. Senior officers will attend senior service college (SSC) to prepare them for positions of senior leadership in the joint community. In addition to Army education, advanced civil schooling (ACS) is a critical component of ID officer's training. ACS opportunities with utilization tours at USMA, the Army Cyber Center, U.S. Cyber Command, U.S. Army Cyber Command, the National Security Agency, or the Intelligence CoE or Cyber CoE, should be made available. Opportunities for training with industry (TWI) will also be an important part in ID officer education. Figure 1 shows the progression of ID officer education. The following paragraphs describe each phase in detail.

3. Information Dominance Lieutenant Training and Education.

The POIs proposed in this section draw on the BOLC Common Core and on modules taught during the Signal and MI BOLC-B courses. By relying mostly on existing POIs, we draw on well-developed lesson plans and minimize the start-up time required to initiate these new courses. We would expect POIs to evolve rapidly based on input from the field and on student feedback.

a. Information Dominance Basic Officer Leader Course, Part B.

IDBOLC-B trains ID officers who can conduct and lead cyber operations in support of tactical operations. IDBOLC-B graduates also could, by exception and particularly if coupled with an appropriate undergraduate degree, serve in operational or strategic assignments. ID Lieutenants will normally begin BOLC-B within 90 days of commissioning. The proposed course uses 8 modules to train tasks critical to the success of an ID lieutenant. In each module, IDBOLC-B will incorporate three core competencies that each ID officer must demonstrate to be successful regardless of the operational environment. The first core competency is critical thinking. ID officers must be able to analyze a situation and distill it down to its essential elements in order to communicate them to superiors and subordinates alike. Second, ID officers must be creative problem solvers. They will often find themselves in unique situations that require innovative solutions to unforeseen problems. Due to the nature of the ID discipline, which directly and uniquely supports the Mission Command warfighting function, ID officers often have a direct impact on mission success. The third core competency, which supports and informs the first two, is technical and tactical proficiency within their chosen area. We note that tactical proficiency includes proficiency in both land and, importantly, cyberspace operations. All components of our proposed ID officer training support these three core competencies. A basic POI providing training hours devoted to each task in modules listed below is provided at Appendix A.

1) Module A. The purpose of module A is to train basic warrior tasks and leadership skills in accordance with the BOLC Common Core Task List specified in TRADOC Regulation 350-36. This task list is common among all branch BOLC courses and provides a baseline for officer education. It includes administrative tasks such as training management, supervising Preventive Maintenance Checks and Services (PMCS) on Army equipment, property accountability, Sexual Harassment and Assault Response and Prevention (SHARP), and resiliency training. Tactical tasks are an important part of module A and include marksmanship, land navigation, tactical convoy planning, and small unit operations and tactics.

Other common leader tasks that round out module A include composite risk management, cultural awareness, analysis of the operational environment (OE), and combatives training.

2) Module B. This module teaches ID officers administrative and troop leading tasks that are not part of the BOLC common core. Effective oral and written communication are critical to success in the ID field and these are included in this module. Lessons on subordinate counseling, Non-Commissioned Officer Evaluation Report and Officer Evaluation Report preparation, and leader development are also part of this module. Tactical troop leading tasks included in this module are to plan a tactical movement, prepare for and react to an IED, and care of combat casualties.

3) Module C. Module C consists of core information technology (IT) and networking knowledge and tasks that form the foundation of tactical cyber operations. Starting with an overview of networking and the Internet, this module delves into network protocols and the Open Systems Interconnect (OSI) model, network planning, configuring network equipment, Voice over IP operations, and secure network deployment, administration, and monitoring. It also includes training on how Army and Joint forces plan and conduct cyberspace operations. During this module, students take the CompTIA Security+[6] Certification Examination and the Network Operations Examination.

4) Module D. This module trains officers for proficiency in communications and electronic warfare topics necessary for success in information dominance. Topics include basic electronics, telecommunications concepts, power distribution, wave propagation, communications security (COMSEC), and spectrum management. It also covers topics in electronic warfare and capabilities of line of sight (LOS) and beyond line-of-sight (BLOS) systems. Finally, module D trains ID officers on the employment of tactical radio systems and introduces TACSAT employment and ABCS systems.

5) Module E. Module E teaches basic staff roles and functions, command post operations, and delves into the fundamentals of tactical intelligence. It covers intelligence tools available on the Secret Internet Protocol Router Network (SIPRNet), an introduction to security programs available through the Defense Security Service (DSS), and an introduction to the cyber threat. This module also covers the intelligence process, introduces intelligence specialties such as Geospatial Intelligence (GEOINT) and Human Intelligence (HUMINT), and delves deeply into the field of Signals Intelligence (SIGINT).

6) Module F. Module F covers introductory material and provides a foundation for Electronic Warfare (EW) in Army operations. After covering the evolution of EW and Joint and Army EW doctrine, this module analyzes EW threats and principles of electronic attack. It then covers radar systems principles and radar system attack, an overview of Army EW systems, and provides hands-on instruction on planning EW support to operations.

7) Module G. Having covered the BOLC common core, warrior tasks, leadership skills, and the fundamentals of cyber operations in terms of communications, signals intelligence, and EW, module G gives students the opportunity to further develop their critical thinking skills, then teaches the Military Decision Making Process (MDMP), where they can put their newfound skills to use as they solve a series of increasingly complex military problem sets. This module requires ID officers to analyze a situation, develop and compare courses of action, and prepare appropriate annexes and appendices of operations orders to address the cyber component of Army operations, in particular the ability to bring cyber effects to bear in both cyber-only and combined cyber/kinetic operations.

[6] "CompTIA Security+," CompTIA, Inc., 2013. [Online]. Available: http://certification.comptia.org. [Accessed 9 July 2013].

8) Module H. A one-week field training exercise (FTX) serves as the capstone event, where ID officers will demonstrate their ability to lead troops in a series of situation training exercises (STXs) that mimic situations they will encounter as lieutenants across the range of potential information dominance assignments. These exercises will include integration of cyber planning and cyber effects into tactical Army operations.

9) Module I. This module captures administrative tasks such as in- and out-processing, course introduction and after-action review, and graduation.

b. Cyber Officer's Communications and Electronic Warfare Course.

The Cyber Officer's Communications and Electronic Warfare Course will build on the cyber security, kinetic warfighting, and leadership foundation provided by IDBOLC-B to prepare lieutenants to serve as communications officers in tactical units and as platoon leaders in Signal battalions and will award AOC 26S. Graduates of this course will also be prepared to serve in cyber-electromagnetic activities (CEMA) elements at the brigade and higher levels.[7] The proposed course will consist of three modules. A task list with contact hours for the modules is provided at Appendix B.

1) Module A. This module will cover TACSAT employment as well as the integration and defense of Force XXI Battle Command Brigade and Below (FBCB2) systems into tactical networks. It will also cover development of a signal network plan and communications support coordination with supported and supporting units.

2) Module B. Here we cover information technology topics necessary for an ID officer serving as a tactical battalion signal officer or staff officer to supervise administration and security of the unit's IT infrastructure. It will include courses on the Windows operating system, computer components, and an introduction to computer repair. This module will conclude with the CompTIA A+ Certification Examination.[8]

3) Module C. This module covers employment and defense of Army communications-electronics systems such as the Promina NX-1000 IP Access Switch, the Joint Network Node (JNN), the Single Shelter Switch (SSSv3), the Command Post Node (CPN) and Multi-Channel Tactical Satellite. It also covers development of a signal network plan.

4) Module D. Module D covers the integration, management, and protection of Army Battle Command systems such as Maneuver Control System (MCS), Tactical Operations Center Intercommunications (TOCNET), Command Post of the Future (CPOF), and Command Post Platform (CPP).

c. Cyber Officer's All Source Intelligence Course.

Upon completion of BOLC-B, ID lieutenants destined to serve as tactical battalion intelligence coordinators or as platoon leaders in Military Intelligence units will become qualified for those jobs by

[7] W. Grigsby, J. Howard, T. McNeill and G. Buehler, "CEMA: A key to success in unified land operations," Army Magazine, pp. 43-46, June 2012.
[8] "CompTIA A+," CompTIA, Inc., 2013. [Online]. Available: http://certification.comptia.org. [Accessed 9 July 2013].

taking the Cyber Officer's All Source Intelligence Course. This proposed course consists of two modules. Specific tasks and hours for each module are provided at Appendix C.

1) Module A. The first module covers intelligence support to MDMP and targeting in significant depth, along with coverage of intelligence collection.

2) Module B. This module covers tools available in the Distributed Common Ground System-Army (DCGS-A), preparation of the intelligence estimate (IE), and detailed coverage of Intelligence, Surveillance, and Reconnaissance (ISR) planning.

4. ID Captain Training and Education.

The Information Dominance Captain's Career Course (IDCCC) will be a multi-disciplined cyber operations officer's course that trains ID officers in TRADOC common core and in cyber operations support to brigade through division, corps, and joint organizations. The course will also prepare ID captains for company command and for key and developmental assignments as a cyber operations officer at all echelons, with focus on corps and below. ID officers will generally attend IDCCC as a permanent change of station (PCS) course between the 4th and 7th year of service. Following IDCCC, officers can expect to attend functional training in preparation for their next assignment.

Branch specific instruction includes communications systems tactics and doctrine; digital and analog communications systems and networks planning; cyber preparation of the battlespace; cyber targeting; electronic warfare; and the MDMP. Similar to other Army CCCs, IDCCC will include modules on Army operations doctrine, common and collective staff procedures, problem solving, communication skills, staff coordination techniques, agile leadership, personnel administration, property accountability, training management, force integration, military justice, cultural awareness, decision making, negotiations, simulations, Operations Security (OPSEC), and Sexual Harassment and Assault Response and Prevention (SHARP).

To keep the course consistent with other captain's career courses, the planned IDCCC will last approximately 20 weeks and will prepare officers for success across the spectrum of cyber operations assignments, including company command and other command positions. Recommended functional training will follow IDCCC to prepare officers for specific follow-on positions such as battalion or brigade Intelligence Officer (S2) or Signal Officer (S6). The Intelligence CoE will continue to offer courses in Imagery Intelligence (ASI 1D), Counterintelligence (AOC 26E), Human Intelligence (AOC 26F), and Signals Intelligence (AOC 26G) for officers entering those intelligence specialties. The Cyber CoE at Fort Gordon will continue to train officers in Telecommunications Engineering (AOC 26A) and Information Systems Management (AOC 26B). We anticipate that those courses will be updated to include appropriate cyber content and experience efficiency gains due to material being covered in IDBOLC-B and IDCCC.

5. Conclusion.

Bold steps are necessary if we are to gain the upper hand in the cyber domain. This is but one of many potential approaches for the Army's way forward in cyber operations, but one that we think has great potential. The combination of the Signal, MI, and EW communities is likely to be controversial. If this merger comes to pass, it is important that Soldiers, NCOs, and officers in this new combined branch are properly trained and educated for the Army to be successful in the cyber domain. We propose an officer training plan that we feel will provide the Army with officers that are ready to lead our cyber

operations efforts into the future. We furthermore give a detailed roadmap for Lieutenant training, including BOLC-B and follow-on courses that will build the foundation of officer education in this new branch.

Acknowledgements.

I would like to thank the following individuals for their key insights, valuable input, and careful review of this paper.

COL Gregory Conti
Army Cyber Center

COL Robert Fanelli
U.S. Cyber Command

COL Tom Cook
Army Cyber Center

LTC Michael Nowatkowski
Army Cyber Center

MAJ Todd Arnold
Cyber Research Center, USMA Department of Electrical Engineering and Computer Science

The views expressed herein are those of the author and do not reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.

Appendix A. Proposed Information Dominance BOLC-B Program of Instruction

This POI includes 726.5 hours of training, or 16 weeks at 45 hours per week. All task numbers provided here are notional and do not correspond with task numbers in current signal or MI officer training plans. Contact the author for a mapping of tasks to the BOLC-B required task list, Signal BOLC-B, MI BOLC-B, or EW (FA29) qualification course where they exist.

Module A	**Common Core (BOLC-B)**	**119**
IDBOLCB-A01	Role of Military History for Leaders in Profession of Arms	6
IDBOLCB-A02	Manage training at platoon level	3
IDBOLCB-A03	Supervise PMCS	2
IDBOLCB-A04	Fundamentals of property accountability	4
IDBOLCB-A05	Apply Concepts of the Army Profession to Leader Situations	2
IDBOLCB-A06	Implement SHARP program	3
IDBOLCB-A07	Composite Risk Management	2
IDBOLCB-A08	Plan a tactical convoy	9
IDBOLCB-A09	Identify EW capabilities in full-spectrum ops	2
IDBOLCB-A10	Marksmanship	40
IDBOLCB-A11	Land Navigation	10
IDBOLCB-A12	Cultural awareness	1
IDBOLCB-A13	Effective explain the OE	1
IDBOLCB-A14	Basic foundational combatives	10
IDBOLCB-A15	Basic tactical combatives	10
IDBOLCB-A15	Resiliency training	10
IDBOLCB-A16	Employ small unit operations and tactics	4
Module B	**Troop Leading**	**43.5**
IDBOLCB-B01	Communicate In Writing	4
IDBOLCB-B02	Counsel a Subordinate	4
IDBOLCB-B03	Produce a Noncommissioned Officer Evaluation Report (NCOER) Counseling Report	4
IDBOLCB-B04	Develop An Officer Evaluation Report (OER)	4
IDBOLCB-B05	Write Favorable Personnel Actions	4
IDBOLCB-B06	Manage Self and Organizational Development as a Leader	4
IDBOLCB-B07	Present an Information Brief	7
IDBOLCB-B08	Tactical Combat Casualty Care	1
IDBOLCB-B09	React to an IED	2
IDBOLCB-B10	Plan Mounted/Dismounted Movement	3.5
IDBOLCB-B11	Prepare for an IED Prior to Movement	6
Module C	**Info Technology and Networking**	**128**
IDBOLCB-C01	Living in a Network Centric World	3
IDBOLCB-C02	Communicating over the Network	2.9
IDBOLCB-C03	Application Layer Functionality and Protocols	3
IDBOLCB-C04	OSI Transport Layer	4
IDBOLCB-C05	OSI Network Layer	3
IDBOLCB-C06	Addressing the Network – IPv4/IPv6	6
IDBOLCB-C07	OSI Data Link Layer	3
IDBOLCB-C08	OSI Physical Layer	3
IDBOLCB-C09	Ethernet	6
IDBOLCB-C10	Planning and Cabling Networks	4.1
IDBOLCB-C11	Configuring and Testing Your Network	6
IDBOLCB-C12	Basic Networking Examination	4

IDBOLCB-C13	General Security Concepts	3.8
IDBOLCB-C14	Identify Potential Risks	5
IDBOLCB-C15	Infrastructure and Connectivity	6.1
IDBOLCB-C16	Monitoring Activity and Intrusion Detection	4.4
IDBOLCB-C17	Implementing and Maintaining a Secure Network	3.7
IDBOLCB-C18	Securing the Network and Environment	3.9
IDBOLCB-C19	Cryptology Methods and Standards	4.4
IDBOLCB-C20	Security Policies and Procedures	2.6
IDBOLCB-C21	Security Administration	4.9
IDBOLCB-C22	Security + Examination	1.2
IDBOLCB-C23	WIN-T Network Architecture	2
IDBOLCB-C24	Battalion Command Post Node (BNCPN) Overview	3.5
IDBOLCB-C25	Configure a VPN router	3
IDBOLCB-C26	Introduction to Detailed Planning & Engineering (DPEM)	1
IDBOLCB-C27	SNMPc 7.0 Workgroup	7
IDBOLCB-C28	SolarWinds Engineer's Edition 7.1	6
IDBOLCB-D29	Conduct VOIP Ops	16
IDBOLCB-C30	Network Operations Examination	1.5
Module D	**Signal Core**	**68**
IDBOLCB-D01	Fundamentals of Basic Electronics	5
IDBOLCB-D02	Develop Power Distribution Plan	9
IDBOLCB-D03	Concepts of Telecommunications	7
IDBOLCB-D04	Basic Electronics, Power Distribution, and Telecommunications Exam	3
IDBOLCB-D05	Wave Propagation	4
IDBOLCB-D06	COMSEC	4
IDBOLCB-D07	Spectrum Management	4
IDBOLCB-D08	Switching Theory	2
IDBOLCB-D09	Component Device Introduction	2
IDBOLCB-D10	Signal Flow and Integration	2
IDBOLCB-D11	Introduction to PROMINA/NX-1000	4
IDBOLCB-D12	Employ PRC-148	2
IDBOLCB-D13	Install SINCGARS Radio	4
IDBOLCB-D14	Employ AN/PRC-150	4
IDBOLCB-D15	Introduction to TACSAT Radio employment	2
IDBOLCB-D16	Employ AN/PRC-152	2
IDBOLCB-D17	Introduction to ABCS systems: CPOF/MCS/DCGS-A	8
Module E	**Intelligence Core**	**51**
IDBOLCB-E01	Staff Roles and Functions	2
IDBOLCB-E02	TOC Operations	2
IDBOLCB-E03	SIPR Tools	10
IDBOLCB-E04	Cyber Threat	2
IDBOLCB-E05	Security Programs - DSS	9
IDBOLCB-E06	Signal Intelligence (SIGINT)	10
IDBOLCB-E07	Geospatial Intelligence (GEOINT)	4
IDBOLCB-E08	Intelligence Process/Disciplines	6
IDBOLCB-E09	Intelligence Oversight/HUMINT/Legal	6
Module F	**Electronic Warfare**	**40**
IDBOLCB-F01	Army Electronic Warfare (EW) Vision	1
IDBOLCB-F02	Evolution of Electronic Warfare (EW)	2
IDBOLCB-F03	Joint Electronic Warfare (EW) Doctrine	1

IDBOLCB-F04	Army Electronic Warfare (EW) Doctrine	3
IDBOLCB-F05	Current Electronic Warfare (EW) Threats	2
IDBOLCB-F06	Analyze Electronic Warfare (EW) Threats	3
IDBOLCB-F07	Commercial Antenna Types	1
IDBOLCB-F08	Principles of Communications Electronic Attack (EA)	1.5
IDBOLCB-F09	Fundamentals of Radar Systems	3.5
IDBOLCB-F10	Principles of Radar Electronic Attack (EA)	2
IDBOLCB-F11	Overview of EW systems	12
IDBOLCB-F12	Plan EW support to operations	8
Module G	**Targeting and MDMP**	**139**
IDBOLCB-G01	Critical Thinking	19
IDBOLCB-G02	Military Decision Making Process (MDMP)	80
IDBOLCB-G03	Cyber Targeting	40
Module H	**FTX**	**106**
IDBOLCB-H01	FTX	90
IDBOLCB-H02	Recovery	16
Module I	**In/out processing and admin**	**32**
IDBOLCB-I01	In processing	16
IDBOLCB-I02	Out processing / Graduation	16
	Total hours	**726.5**

Appendix B. Proposed Cyber Officer's Communications and Electronic Warfare Course POI

This course includes 184.5 hours of training; 5.3 weeks at 45 hours per week. Course numbers correspond with those used for similar courses in the Signal BOLC POI and skill identifier 1J course.

Module A	**Combat Net Radio (CNR)**	**34**
113-SBOLBC07	Employ TACSAT Radios	8
113-SBOLBC09	Integrate FBCB2 into BCS	8
113-SBOLBC10	Employ FBCB2 Greenbox	8
113-SBOLBC11	Analyze Terrain Using SPEED Software	4
113-SBOLBC12	Coordinate Signal Support With The Supporting Unit	4
113-SBOLBC13	CNR Exam	2
Module B	**Information Technology**	**49.5**
113-OAP11A00	Understanding Windows	3.4
113-OAP11A01	Personal Computer Components	7.1
113-OAP11A02	Working with Windows	7.6
113-OAP11A03	Input/Output Devices	7.3
113-OAP11A06	Complete PC Tech	16
113-OAP11A07	A+ Exam	2.1
113-OAP11D01	Microsoft Office SharePoint Server 2007	6
Module C	**Communications-Electronics Systems**	**75**
113-SBOLBF01	Signal Corps Modularity	2
113-SBOLBF06	Signal Flow Using PROMINA/NX-1000	8
113-SBOLBF07	Construct a PROMINA/NX-1000 Diagram	2
113-SBOLBF08	Components of JNN	6
113-SBOLBF09	CPN Capabilities	2
113-SBOLBF10	Tactical Hub Node	6
113-SBOLBF11	Single Shelter Switch (SSSv3)	6
113-SBOLBF12	Switching Demo	2
113-SBOLBF13	Capabilities Of Multi-Channel Tactical Satellite	3
113-SBOLBF14	Capabilities of LOS and BLOS System	3
113-SBOLBF16	VSAT/SNAP/SPOP Overview	4
113-SBOLBF17	Global Broadcast System (GBS)	1
113-SBOLBF18	Design A Signal Network Plan	26
113-SBOLBF19	Switching and Transmission Hands-on Exam	4
Module D	**Army Battle Command Systems**	**26**
113-SBOLBG01	Prepare Overlays Using MCS/ABCS Workstation Capabilities	8
113-SBOLBG02	Command Post Of The Future (CPOF)	8
113-SBOLBG03	TOCNET	4
113-SBOLBG04	Employ Command Post Platform (CPP)	4
113-SBOLBG05	Conduct Online Meeting Using Defense Connect Online	2
Module E	**Electronic Warfare Systems and Operations**	**59**
TSOC-E01	EW Systems Review	4
061-EWK70311	Manage CREW Systems	20
061-EWK70312	Army Reprogramming Analysis Team (ARAT)	1.5
061-EWK70313	Electronic Warfare (EW) Reprogramming	2
061-EWK70314	Electronic Warfare (EW) Databases	2
061-EWK70315	CREW Testing Procedures	1.5
061-EWK70316	Electronic Warfare (EW) Modeling and Simulation Tools	8
TSOC-E02	Advanced Electronic Warfare Support to Operations	16
TSOC-E03	Electronic Warfare Systems and Operations Exam	4
	Total hours	**243.5**

Appendix C. Proposed Cyber Officer's All Source Intelligence Course Program of Instruction

This course includes 281 hours of training, or 6.3 weeks at 45 hours per week. Course numbers correspond with numbers used for similar courses in the MIBOLC POI.

Module A	**Unified Land Operations**	**129**
35D1B03L	Information Collection (IC)	35
35D1B04T	Intelligence Annex B Test	1
35D1B05L	Desert Lightning	8
35D1B02L	Intel support to MDMP	40
35D1B06L	Intelligence Support to Targeting	40
35D1B07T	Intelligence Support to Targeting Test	5
Module B	**Operation Unbreakable/SIPR Tools**	**152**
35D1C01L	DCGS Analytical Tools	12
35D1C02L	Operation Unbreakable	27
35D1C03T	Operation Unbreakable Test	36
35D1C09T	Route Threat Analysis Assessment	8
35D1C10L	GRINTSUM and Intelligence Estimate (IE)	17
35D1C11L	ISR Art of Warfare	44
35D1C13L	Current Conflict Case Study	8
	Total hours	**281**

MAPO Dec. 4, 2013

MEMORANDUM FOR DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE; ATTN: LTC DAVID R RAYMOND, UNITED STATES MILITARY ACADEMY, WEST POINT, NEW YORK 10996

SUBJECT: Manuscript Clearance: "A Proposed Army Information Dominance Officer Education Model"

1. In the interest of academic freedom, members of the staff and faculty who prepare manuscripts for publication in a private and unofficial capacity may express their views in such materials, as long as those views do not disclose classified or operations security information. It has been determined by appropriate USMA authority that the subject manuscript meets the requirements of para 6-1, AR 360-1, dated 25 MAY 2011 in that it does not contain classified or operations security information.

2. Accordingly, the manuscript is returned for publication. Should the manuscript be submitted in a private capacity for publication, an appropriate disclaimer will accompany each manuscript. The following is considered an appropriate disclaimer:

> "The views expressed herein are those of the author and do not reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense."

Francis J DeMaro Jr.
Media Relations Branch
U.S. Military Academy
Public Affairs Office
West Point