Cyber Education via Mathematical Education

Professor Chris Arney
Major Natalie Vanatta
Major Thomas Nelson

ABSTRACT

Cyber is more than programming 1s and 0s, it is an interdisciplinary domain that involves elements of many disciplines of science, engineering, and humanities. Understanding mathematics is critical to understanding the cyber domain. At the United States Military Academy (USMA), the Mathematical Sciences Department is contributing to cadets' cyber education. The Military Academy CYBER Education Working Group produced initial thoughts on how to educate in this domain.[1] Using this construct, this article identifies the knowledge, skills, and attributes that are elements of USMA's core mathematics, network science minor, or mathematics major. The intent is to help prepare future military officers for leadership roles in the cyber-affected world in three tiers: (1) what all officers should know, (2) what highly technical officers should know, and (3) what cyber leaders should know.[2] All officers should have a broad professional cognizance of cyber operations, while highly technical officers and cyber leaders could benefit from a more in-depth understanding of mathematics relative to cyberspace.

INTRODUCTION

> *"If I were again beginning my studies, I would follow the advice of Plato and start with Mathematics."* – Galileo Galilei[3]

Jeff Immelt, Chairman of the Board and CEO of General Electric, recently reinforced Galileo's quote at *Business Insider's* IGNITION 2015 conference when he remarked that his most valuable qualification was his undergraduate mathematics degree. He said, "I use my math major every day—I don't use the MBA quite as much." He went on to say that running a company is about problem-solving. That's something he learned about in his undergraduate studies, due to "the inherent intellectual curiosity around

Brigadier General (Retired) Chris Arney is a Professor of Mathematics at the United States Military Academy and former Head of the Department of Mathematical Sciences. He holds a Ph.D. in Mathematics and M.S. Degrees in Computer Science and Mathematics from Rensselaer Polytechnic Institute. He also holds a B.S. in Engineering from the United States Military Academy. A career Military Intelligence officer, he has served in numerous tactical assignments, teaching assignments at USMA, NASA Langley Research Center, and the Army Research Office. His current research includes cooperative game theory, applications of network science, and mathematical applications to cyberspace.

Major Natalie Vanatta is a Cyber Officer currently serving as an Academy Professor with the Army Cyber Institute at West Point, NY. She has worked from the tactical to the operational level in the signal arena while also teaching/researching in the cyber field. She holds a Ph.D. in Applied Mathematics from the Naval Postgraduate School (NPS), an M.S. in Systems Engineering from NPS, an M.S. in Mathematics from Stevens Institute of Technology, and a B.E. in Computer Engineering from Stevens Institute of Technology. MAJ Vanatta has completed multiple tours in Operation Iraqi Freedom (OIF) and her research interests are in encryption, malware detection, active cyber defense, and human behavior.

Major Thomas Nelson is a Cyber Officer and currently the Operations Officer for the 782d Military Intelligence Battalion (Cyber) at Fort Gordon, GA. He most recently served as an Assistant Professor of Mathematics at the United States Military. He holds a M.S. degree in Applied Mathematics from the University of North Carolina-Chapel Hill, and a B.S. in Mechanical Engineering from the United States Military Academy. Commissioned in the Infantry, he served in numerous positions with the 82nd Airborne Division and 4th Infantry Division in Iraq and Afghanistan. His research interests include Computational Fluid Dynamics and Anomaly-Based Intrusion Detection Systems.

math and physics." [4] That same intellectual curiosity and problem solving is expected of all officers, particularly those entering the Cyber Mission Force (CMF).

At the United States Military Academy (USMA), the Department of Mathematical Sciences is contributing to cadets' cyber education. Cyber is more than programming 1s and 0s, it is an inter-disciplinary domain that involves elements of many disciplines of science, engineering, and humanities. Initial thoughts on how to educate in this domain were produced by the Military Academy CYBER Education Working Group. [5] Using their construct, this article identifies the knowledge, skills, and attributes that are elements of the core mathematics, network science minor, or mathematics/operations research majors at USMA. Ultimately, the intent is to help prepare future military officers for leadership roles in the cyber-affected world in three tiers: (1) what all officers should know, (2) what highly technical officers should know, and (3) what cyber leaders should know. [6] We believe all officers should have a broad professional cognizance of cyber operations, of which USMA's core mathematic program contributes. Highly technical officers will benefit from the math department's network science minor, and some cyber leaders would benefit from mathematical sciences major. Additionally, the military services provide numerous opportunities for graduate work in mathematics that contributes to the cyber domain.

Two core objectives of the mathematics education at USMA is to acquire a body of knowledge, and to develop a fundamental understanding of the basic tenets of mathematics, science, and engineering.

WHAT ALL OFFICERS SHOULD KNOW: BROAD PROFESSIONAL COGNIZANCE OF CYBER OPERATIONS IN THE CORE MATHEMATICS PROGRAM

There are two terminal objectives of the core mathematics education at USMA: to acquire a body of knowledge, and to develop thought processes fundamental to understanding the basic tenets of mathematics, science, and engineering. A cadet's mathematical journey affords them opportunities to develop as life-long learners capable of formulating intelligent questions and researching answers independently and interactively. Central to the entire USMA program is the concept of problem-solving through modeling. [7] All cadets take a modeling course (MA103 or MA153), a calculus course (MA104 or MA255), and a statistics course (MA206). Officers in the Cyber Branch and those doing cyber-related work in other branches will be required to model and solve problems. Several lessons throughout the core mathematics program lend

themselves to ensuring all officers have a basic understanding of the math behind cyber operations.

MATHEMATICAL MODELING (MA103)

This course emphasizes applied mathematics through modeling. Students develop effective strategies to solve complex and often ill-defined problems. The course exercises a wide array of mathematical concepts while nurturing creativity, critical thinking, and learning through activities performed in disciplinary and interdisciplinary settings. A block of the instruction in the course is on modeling with matrix algebra. In this block a lesson is taught on cryptology with all students taught the role of cryptology in military history and the basics of the encryption and decryption processes. Students use a transformation matrix for encryption and the inverse of the transformation for decryption. In this lesson students are taught, "the design of the encryption algorithm, and the mathematics required to support the decryption process is where the art and science of cryptology lies. Its sophistication ranges from simple procedures such as the matrix algebra presented in this section, to far more advanced techniques that leverage complex machines and the computational power of computers. Much like network science, the study of cryptology is extensive; entire courses, as well as entire careers of study and research, are dedicated to it." [8] In the lesson, students role play a WWII scenario encrypting and decrypting message intercepted from a German courier.

The mathematics modeling course also teaches two lessons on networks (one on network flow and the other on network centrality). The lesson on network flow discusses rules for network flow processes, applies the mathematics to military networks, and introduces problems to quantify the flow between nodes using linear algebra. The lesson on network centrality discusses the conception of social networks, internet structure and process, and how network analysis determines the most important node. Examples include Facebook and Google's page rank algorithm. This ensures all cadets receive a basic understanding of networks, network science, and the major domain and tools of cyberspace during the core mathematics curriculum.

SINGLE VARIABLE CALCULUS (MA104)

The goal of this course is to foster knowledge and understanding of single variable calculus, including the concept of the derivative and the integral, and to apply these concepts to model and solve problems, and to interpret and communicate the results in context. During the calculus applications block, the course covers several topics that are loosely related to cyber including rates of change in the natural and social sciences, exponential growth and decay, optimizations, Newton's method, applications to physics and engineering, and probability.

One lesson specifically addresses "applications to cyber operations." This lesson gives the students a background on information theory and Claude Shannon's interpretation of entropy. Students are given a scenario where they need to use integral calculus to determine the entropy of several different systems used in communications and secrecy systems. Using this information they communicate an argument as to which encryption algorithm a bank should use for their website. Students then learn about several government and military applications of cryptographic systems to include the one-time pad. This lesson and the other applications provide students a broad understanding of how math is used in the cyber domain.

PROBABILITY AND STATISTICS FOR ENGINEERING AND THE SCIENCES (MA206)

This course helps students use mathematics to model real-world variation and assess the likelihood of events. The course shows students to use statistical tools to help draw appropriate conclusions from data. It also teaches reliability analysis of independent systems with component diagrams and it works through reliability of systems/components in series and parallel. The current textbook example focuses on the reliability evaluation of solar photovoltaic arrays in series-parallel and total-cross-tied. Theses to arrays are set up very closely to the ring and mesh network topologies of computer networks. The same analysis on the solar arrays can be applied to predicting the system lifetime of computer networks.

The course then models uncertainty in the context of several different probability distributions—discrete and continuous. In this block, cadets execute a mini-project focused on the phases of network penetration. Cadets are required to program and conduct Monte Carlo Simulations on the probability of an attacker gaining access to the system within a certain timeframe and/or at a certain cost in resources. These are statistical simulations utilize sequences of random numbers to replicate real-world scenarios. Cadets not only build Monte Carlo simulations in Excel or R, but also interpret the results, and answer probability and analysis questions.[9] The statistical modeling in this course also gives cadets the ability to write, debug, and use a mathematical computer code to a real life scenario. Statistical and uncertainty models can be used to model other applications in the cyber domain.

> Cyber is more than programming 1s and 0s, it's an interdisciplinary domain that involves elements of science, engineering, and humanities.

NETWORKS FOR CYBER OPERATIONS (MA490)

Networks for Cyber Operations is a course intended to serve as an integrative experience for cadets of all majors and fields of study.[10] This course was formally known as Application Problems for Mathematics, Science, and Engineering. This specific offering of the course is new to academic year 2016 and focuses on networks for cyber operations. The seven-course blocks are as follows: Network Science, Cryptography, Cyber Mission Forces, Internet of Things, Social Sciences, Data Analytics and Science, and Tactical Cyber (Support to Corps and Below). The course enables students to confront cyberspace issues by modeling, solving, analyzing, and understanding problems involving cyber processes and structures on networks. The students learn about networks, perform complex modeling, work on a topic associated with this subject, write a book review, produce a poster, and give a presentation to the class.

All cadets taking the course complete a semester long project and presentation for USMA Projects Day in one of the following domains: Cyber and Social Movements, Cyber and Social Media, Security of the Internet, or Infrastructure Vulnerability. Although taught by USMA Department of Mathematical Sciences instructors, the course leverages the experience, knowledge, and expertise of the Army Cyber Institute (ACI), and other partner organizations (such as Combatting Terrorism Center, Department of Social Sciences, and FBI) for several guest lectures. The current section consists of 12 cadets (11 are math majors and one is a computer science major) that upon graduation will be commissioned into the Army's Cyber, Armor, Aviation, Military Intelligence, Air Defense Artillery, Field Artillery, Engineer and Infantry branches.

Network Science is an inherently interdisciplinary academic field which studies complex networks such as telecommunications, computer, biological, cognitive, and social networks.

WHAT (SOME) HIGHLY TECHNICAL OFFICERS SHOULD KNOW: NETWORK SCIENCE MINOR

Network Science is an inherently interdisciplinary academic field which studies complex networks such as telecommunications, computer, biological, cognitive, and social networks. Network representations of these systems lead to predictive models and insights into how networks behave and evolve. Students who minor in Network Science graduate with an enriched understanding of the interrelationships and influences that drive the formation and evolution of systems. They also learn to formalize and measure several different aspects of an individual's importance to a system, as well as to formalize and

measure various characteristics of the system itself, such as its size, sensitivity to change, and topology (such as its shape and pattern of connectivity).[11]

To earn the network science minor, students take the following five courses to earn the Network Science minor: Fundamentals of Network Science, a theory course, a modeling course, an applications, and a capstone course. Some of the cyber-related skills cultivated in this sequence of courses are how to categorize network types, understand the limitations and challenges associated with network security, build network models to address network security, and identify critical actors in a network. Students will understand the structures associated with various ways network nodes act in the network, formulate processes and structures that degrade, disrupt, and destroy a network, and understand cascading effects of actions in the cyber domain. Students will also learn to understand network sensitivity and understanding cause and effort of network modifications, analyze the influences of human relationships on information, discuss cognitive perceptions and their impact through network interdependencies, and understand the cascading implications of cyber effects on different and common/conflicting mission goals.

WHAT (SOME) CYBER LEADERS SHOULD KNOW: MATHEMATICAL SCIENCES MAJOR

The Mathematical Sciences Major offers abundant opportunities for study in a broad range of mathematical subjects. Courses such as differential equations, linear algebra, mathematical modeling, analysis, numerical computation, statistics, provide a sound mathematical foundation in the science and engineering fields. Also, follow-on courses such as graph theory and networks, linear optimization, combinatorics, and advanced individual study provide both depth in understanding the foundations of mathematical theory, as well as the opportunity for study and research in a selected subject. Whenever possible, cyber is emphasized to extend the knowledge required for the consideration of realistic and challenging problems of today's world.[12]

The Mathematical Sciences department also presents applied mathematical topics and network science needed for success in cybersecurity. We have organized our topics into three areas: modeling large networks, cyber threat discovery, and network dynamics. These topics areas associated with cyber security are challenging and understanding these topics can provide the foundation for many cyber issues. The topics include modeling large networks, discovering cyber threats, and network dynamics.

Modeling Large Networks is covered in the Network Science course (MA394). Here students learn the development of mathematical network models that accurately emulate real-world, multi-layered networks and reflect the dynamics of these real networks. They also use statistical techniques for comparing networks and their properties, and develop methods for efficient computing of network measures. Students learn methods for discovering interesting sub-networks or clusters and optimization and statistical

methods for parameter fitting. The course also covers statistical numerical methods for likelihoods of properties.

Discovering Cyber Threats is covered in the Network Science and Optimization courses (MA394, MA481). Students learn about machine learning methods for finding and understanding features for data with evolving characteristics. Students also learn techniques for optimization of properties when using data sampling and data analysis of networks with missing values or attribute uncertainty. They learn how to detect anomalies that do not conform to models to develop understanding the mathematics malicious code detection and understand the aggregation of information (locally and across networks).

The Mathematical Sciences department also presents applied mathematical topics and network science needed for success in cybersecurity.

In the Network Science course, students will also learn network dynamics. They learn how to model flow or the spread of infections or ideas on a network. They also learn game theoretic or dynamical systems techniques for the evolution of cyber threats. Finally, they learn how to employ mathematical models for the emergence of a behavior on networks.

MATHEMATICS SENIOR HONORS THESIS (MA498/MA499)

These two courses provide a year-long thesis option for all math majors. During the year students will produce a research proposal, literature review, midyear report, written thesis, conference presentation, and poster presentation at USMA's projects day. Currently there are four cadets math majors completing year-long honors theses in Cyber related research. Their work includes:

(1) Comparing Statistical Approaches to Anomaly-Based Intrusion Detection Systems, (2) Implementing an Anomaly-Based Intrusion Detection System—Focus on Internal Threat, (3) Finding invariants for the equivalence of quantum error correcting codes, and (4) Investigating the properties of asymmetric key encryption schemes and the effects of transposing the method to different finite groups or elliptical curve space. These yearlong research projects allow cadets to learn a depth of knowledge in a cyber related topic that aligns with their interests.

Past cyber domain related honors thesis topics have also included: (1) The past, present, and the future of wireless security: an analysis of Wi-Fi protected access, (2) Hunting the Zodiak: Attacking the Z340 Cipher with Hybrid Methods, (3) Cryptographic Graphs: A look at the Cryptographic Applications of *Hard* Problems from Graph Theory, (4) Developing an Arithmetic Processor for Elliptical Curve Cryptography and (5) Randomness Properties Found in De Bruijn Sequences.

CYBER EDUCATION BEYOND USMA

The Cyber Branch pilots a program, which affords newly commissioned Cyber officers the opportunity to earn a graduate degree in a cyber-related field before attending their Cyber Basic Officer Leadership Course (CBOLC). It is estimated that ten of the thirty newly commissioned Cyber officers will go immediately to graduate school. Additionally, officers can compete for elite national and international scholarships for additional opportunities to attend graduate school. For example, a current senior cadet was awarded the Churchill Scholarship and will attend Oxford University to earn a one-year Masters of Science degree in Applied Mathematics.

> It is essential that all officers understand how mathematics affect the rapidly developing cyber domain.

The Naval Postgraduate School (NPS) currently offers an applied mathematics education in support of US Army Cyber Command junior officer development. The NPS department of Applied Mathematics has outlined a fully accredited, one year degree program for recent USMA and US Army ROTC graduates that focuses on discrete mathematics and cyber related course work. Students can take optional elective courses in computer science, electrical engineering or operations research. All students will earn graduate certificates in Secure Communications and Network Science. Participants may also be able to earn a third certificate in either Cyber Warfare,Cyber Security Fundamentals or Cyber Security Defense from the Electrical & Computer Engineering or Computer Science departments. [13]

The Air Force Institute of Technology (AFIT) offer graduate programs through its Graduate School of Engineering and Management in engineering, applied science, and management disciplines. It offers masters and doctoral in applied mathematics and operations research: “The aim of the master's degree program is to provide a balanced foundational education in mathematical and statistical analysis, an understanding of appropriate applications of the theory, and some depth in an area of specialization.” [14]

Currently, the Army is offering Advanced Civil Schooling (ACS) opportunities for officers. This fiscal year Advanced Civil Schooling (ACS) is offering fifteen opportunities for Cyber and Electronic Warfare (EW) commissioned officers and warrant officers to broaden their experience and professional career. The target schools are AFIT, Massachusetts Institute of Technology, Texas A&M University, Carnegie Mellon University, NPS, University of California, Berkeley, Georgia Tech, Stanford University, and Virginia Tech. The targeted Graduate Degrees are Computer Science, Applied Math, Information Technology Strategy, Electrical Engineering, Engineering Science, Defense Analysis–Information Operations, and Cyber Operations.

CONCLUSION

There are numerous opportunities for the *Cyber Math* education at USMA, and graduate studies beyond USMA. It is essential that all officers understand how mathematics affect the rapidly developing cyber domain. The USMA Department of Mathematical Sciences is committed to developing an effective mathematics curriculum that attempts to foresee the mathematical needs of tomorrow's students. Emphasis is placed on achieving intellectual discipline, mastery of reasoning, understanding of mathematical concepts, skill in practical applications of mathematics and appreciation for the role of mathematics in the military. The USMA math department produces math majors and network science minors to be strong candidates for Cyber and other technical branches while providing a broad professional cognizance of cyber operations for all students.

NOTES

1. Military Academy CYBER Education Working Group. "Draft Cyber Body of Knowledge." Access on February 10, 2016 form http://computingportal.org/sites/default/files/CEWG%20-%20Draft%20Body%20of%20Knowledge.pdf.
2. Sobiesk, Edward, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor, "Cyber Education: A Multi-Level, Multi-Discipline Approach", SIGITE'15, September 30-October 3, 2015, Chicago, IL, 109-114. Accessed on January 18, 2016 from http://dx.doi.org/10.1145/2656450.2656478.
3. BrainyQuote. "Galileo Galilei Quotes." Accessed January 18, 2016 from http://www.brainyquote.com/quotes/quotes/g/galileogal381323.html.
4. Portia Crowe. The CEO of GE explains why his math degree is more useful than his MBA, Business Insider, 9 December 2015, Accessed January 18, 2016 from http://www.businessinsider.com/jeff-immelt-on-math-and-mba-degrees-2015-12.
5. Military Academy CYBER Education Working Group. "Draft Cyber Body of Knowledge".
6. Sobiesk et. el. Cyber Education: A Multi-Level, Multi-Discipline Approach.
7. USMA Department of Mathematical Sciences, Core Mathematics: Academic Year 2016. Accessed January 21, 2016 from http://www.westpoint.edu/math/SiteAssets/SitePages/Core%20Math/CMB-2015_16.pdf.
8. USMA Department of Mathematical Sciences, Modeling in a Real and Complex World, August 2016, 319.
9. Geisler, Trent. Discussion with author. January 26, 2016.
10. Office of the Dean. "USMA Academic Program (Redbook): Class of 2016." United States Military Academy, West Point, NY. Accessed January 21, 2016 from http://www.usma.edu/curriculum/siteassets/sitepages/course%20catalog/redbook_gy2016_20140509.pdf.
11. USMA Department of Mathematical Sciences, Network Science Minor, Accessed January 21, 2016 from http://www.westpoint.edu/math/SitePages/NetworkScience.aspx.
12. USMA Department of Mathematical Sciences, Mathematical Sciences Major, Accessed January 21, 2016 from http://www.westpoint.edu/math/SitePages/Math.aspx.
13. Naval Postgraduate School, Applied Mathematics Education in Support of US Army Cyber Command Junior Officer Development. Accessed January 26, 2016 from http://www.nps.edu/Academics/Schools/GSEAS/Departments/Math/.
14. Air Force Institute of Technology, Graduate Studies in Applied Mathematics, Department of Mathematics and Statistics Brochure, 2015-2016. Accessed January 21, 2016 from http://www.afit.edu/docs/Brochure2015-16%20with%20cover.pdf.