Information & Security

N. Georgieva
vol. 46, no. 3 (2020): 311-320
https://doi.org/10.11610/isij.4623

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Comparison between the Cyber Operations Majors in the United States Naval Academy and the Bulgarian Naval Academy

Nikoleta Georgieva

Nikola Vaptsarov Naval Academy, Varna, Bulgaria, www.naval-acad.bg/en

ABSTRACT:

This study is about the comparison between the Cyber Operations majors in both the United States Naval Academy and the Bulgarian Naval Academy. It compares the goals of the major, the length of study for the degree, the courses, the lab hours, and their respective learning objectives to conclude.

ARTICLE INFO:

RECEIVED: 08 JUN 2020
REVISED: 17 Jul 2020
ONLINE: 15 AUG 2020

KEYWORDS:

cybersecurity, cyber operations, Navy, US Naval Academy, analysis, academic major

Introduction

The motivation of this study is to compare the degrees in both military institutions. Since the Bulgarian Naval Academy has introduced this major in 2019 with the first graduating class to be in 2024, it is important to compare, see and analyze the positives and the negative sides of its creation. In this way, the major will always develop in creating a better suited Cyber Officers in the future to defend and protect Bulgaria. The methods used in this study is to compare the major matrixes between the United States Naval Academy, their credit hours, their contents, and length of education and goals.

✉ Tel.: +359882416801; E-mail: nikolethag@gmail.com

Methods

To fully understand how and why both military academies have created the major, this paper is going to compare the year of the creation of the major, the class and courses offered, summer trainings and the end objectives of their respective Navies.

Analysis

1. United States Naval Academy:

a. History and Background:

United States Naval Academy was established in 1850, starting with around 300 midshipman per class, with recently of having a minimum of 1,000 midshipman. Currently there are 29 majors offered with 6 language minors. One of these majors is Cyber Operations and was introduced in 2012, with the first class to graduate with 27 midshipmen in 2016. Every year the interest in this major has grown exponentially, given the growing interest and popularity of the subject. That last class that graduated, the class of 2020, had 76 midshipmen with the Cyber degree. The length of study is four years and to satisfy the United States Navy's needs, every midshipman must also graduate with a Bachelor of Science degree as well as their major. This means that even if a midshipman has chosen an English Degree, they have to take Chemistry, Physics, Leadership, Thermodynamics and Electrical Engendering courses to satisfy the requirements of earning a Bachelor of Science Degree. This in a way hinders the actual majors because to not overload the midshipman with so many courses, there are more courses of non-major classes compared to major ones. Every year the Cyber Operations major has involved with every graduated class to fill out forms and do four-year comprehensive exams for the professors to evaluate each class and to get suggestions of every class that has finished all of their courses. In the last couple of years there is an option of choosing an Honours route of the major which requires more courses to be taken.

During their third year of being at United States Naval Academy, every midshipman must choose and be selected into their respective community in order to serve in the United States Navy and Marine Corps for the next five years. There are, currently, 24 communities that midshipman can serve in, with the biggest being Surface Warfare Community, where they serve on Navy Ships, Submarine Community, Navy Pilot and Marine Air/Ground. The combination of these five brings around 90.4 % of midshipman and the other 9.6% choose to serve in smaller communities.[1] One of these small communities is the IWC, which stands for Information Warfare Community. The mission of the Information Warfare Community is to "gain a deep understanding of the inner workings of our adversaries, develop unmatched knowledge of the battlespace, provide our operating forces with sufficient over-match in wartime command and

[1] See https://www.usna.edu/NewsCenter/2019/11/NAVAL_ACADEMY_CLASS_OF_2020_OBTAIN_CAREER_ASSIGNMENTS.php.

control, and project power through and across the network,"[2] The biggest take-away of their mission is that they protect and defend the Navy's networks and deal with information across the domain. Cryptologic Warfare and Cryptologic Warfare Engineer community are included inside IWC. Out of 1,021 midshipman that graduated in class of 2020, only 17 were selected for CW (Cryptologic Warfare) and CWE (Cryptologic Warfare Engineer).

After graduating, newly commissioned officers in the CW community start their training to prepare for their five years of service in the community. First they go to a Division Officer Leadership Course for 1 week, then Information Warfare Basic Course for 3 weeks, and finally to a Cryptologic Warfare Officer Basic Course for 8 weeks. Even if a certain new officer does not know anything about cyber and computers, those courses are highly intense and provide enough understanding in order for them to excel in their respective jobs. A CW officer in the United States Navy has a department of enlisted personnel that work for him or her. This means that their job is to understand what they are doing, why they are doing it and to know how to lead their enlisted and trust that the enlisted would know how to accomplish their certain mission. In other words, in the United States Navy, the officers are only the managers and leaders while the enlisted are the ones that do all the technical parts of their respective jobs. This is worth mentioning because with knowing how the United States Navy works, it explains how they have created the Cyber Operations Bachelor's degree. Their officers must have a broad understanding of every topic in the cyber domain, they must lead, but they do not need to know how to do an actual attack. This is the reason why the Cyber Operations major is more theoretical and broad, compared to a more practical approach.

b. Courses of Cyber Operations Major:

The first Cyber course that is offered to every midshipman is SY110 – Cyber Security I. This course is introduced during the first year of studying in either the first or second semester. The learning objective of this course is to introduce midshipman to the "use, function, and operation of computer, networks and applications with an emphasis on cyber security." [3] It has 3 credits with 2 lecture periods and 2 lab periods every week. During SY110, midshipman learn the five cyber domains, the OSI model, learn how to convert and calculate binary numbers, the basic components inside the computer, firewalls and computer privacy and basic cyber-attacks with an emphasis of phishing attacks. It is taught to every midshipman, because future officers need to know the basics of cyber domain and need to know what a cyber-attack looks like and have to know how to protect their personal and work computers.

The first course of the Cyber Operations major is SY201 – Cyber Fundamentals I. It teaches midshipman the basics of programming starting with defining variables and loops to classes and switches. It is taught in Python and introduces the Linux Operating system. It is four credits, with 3 lecture hours and 2 lab

[2] https://www.usna.edu/CyberCenter/_files/documents/idc/IDC_Overview.pdf.

[3] https://www.usna.edu/CyberDept/Academics/CyberCourses.php.

periods every week. During this course, midshipman learn problem solving skills and basic coding with labs and projects for them to program.

The next course offered is SY202 – Cyber Systems Engineering. It is 3 credits with 2 lecture hours and 2 lab hours per week. This course teaches different types of cyber physical systems and infrastructures, such as SCADA and embedded systems. The goal of this class, is to understand the "entire communication cycle as it pertains to the cyber physical and communications controls systems."[4] The students learn Matlab and they try to hack the controllers of a small SCADA elevator to give wrong calibrations and control its movement. The biggest takeaways from this course is for midshipman to understand how vulnerable industrial systems are due to the fact that most of them were created before the cyber era and have very little protection against such attacks.

The next course offered is SY204 – Systems Programming and OS Fundamentals. This course is 4 credits, meaning 3 lecture hours and 2 lab hours per week. The learning objective of this course is to learn system programming by introducing C language and to understand the features and the design of operating systems. This course has multiple labs and projects, where midshipman design cyber tools for network monitoring and listening, work with the Linux filing system, learn memory allocation, forks and pipes.

The next course offered is SY301 – Data Structures for Cyber Operations. This course is 4 credits, with 3 lecture classes and 2 lab periods. Midshipman learn complex data types and how to sort and analyze them. The topics are a range from simple data types, their algorithms to probability calculations and sorted and unsorted trees. During the lab hours, students write programs and algorithms in python like merge sort with linked lists and tree sorts to fully understand all the topics.

The next course offered is SY303 – Applied Cyber System Architecture which is 4 credits and has 3 lecture hours and 2 lab hours per week. This course is project-oriented where Midshipman learn computer logic gates to design a simple computer ALU and CPU with the proper combination of those gates. By the end of the semester, they design an assembler, virtual machine and a compiler. This course is created for midshipman to understand low-level programing and functions.

The next course offered is SY304 – Information Operations, Social Engineering, and Hacktivism which is 3 credits with 3 lecture hours per week. This course is non-technical and examines the "human factor" of cyber operations, it teaches human behaviors and the types of social engineering and different approaches of gaining advantage. During the lab hours, midshipman learn how to pick locks with five pins and they have a course project to pick a store or an organization and find ways to get inside the building and its network without having any technical expertise.

The next course offered is SY306 – Web and Database Cyber Operations which is 3 credit hours with 2 lecture hours and 2 periods of labs. During this

[4] https://www.usna.edu/CyberDept/Academics/CyberCourses.php.

course midshipmen learn how to create and maintain websites. They learn basic HTML, JavaScript, MYSQL database, Python with CGI, web authentication and how to operate their own server to host a website. They also focus on common cyber-attacks such as XSS, SQL injection, etc.

The next course offered is SY308 – Security, Fundamental Systems which is 3 credits with 2 lecture hours and 2 lab periods. In this course students learn fundamental principle of security, basic cryptography such as symmetric and asymmetric encryption mechanism, the math behind them and focus on buffer overflow attacks, rainbow table attacks and write programs to create and defend against such attacks.

The next course offered is SY310 – Networking and Mobile Computing which is 4 credits with 3 lecture hours and 2 lab periods every week. This course is an introduction of wired and wireless communications, where Midshipman learn basic signals and their transmission. Also, it is focused on the TCP/IP model and learn what each layer is comprised from and how the layers communicate between each other. During their lab periods, they have labs about hacking a RC car, looking at different networks in Wireshark and learning about APR poisoning and other network based cyber-attacks and how to defend against them.

The next course offered is SY401 – Cyber Operations I with 3 credit hours that comprises of 2 lecture hours and 2 lab periods every week. This is one of the final courses of the Cyber Operations Major, where midshipman tie everything together. They learn what it requires to be a Cyber Operator and the course is designed to teach end-to-end Offensive Cyber Operations, from Reconnaissance to the actual attack. Their labs are inside a virtual environment where they safely test different tools and attacks such as zero-day vulnerability, CVEs, DDOS attacks, etc.

The next course offered is SY403 – Cyber Planning and Policy which is 3 credits and has 3 lecture hours. This is a non-technical course to deepen the understanding of critical infrastructures vulnerabilities and the growing dependency upon them. It is designed for midshipman to understand the gap inside the private sector, and how much private companies spend on cyber security and their priorities. There are multiple exercises that cover ransomware and ransomware attacks, where midshipman must find ways to protect a company against themselves and their attackers. They also create plans for minimizing the risks of cyber-attacks to a private and government entity.

The next course offered is SY402 – Cyber Fundamentals II, which is 3 credits with 2 lecture and 2 lab hours. This course is focused of understanding risks and how to build and defend large networks. It talks about Intrusion Detection and Prevention Systems, it uses Snort and writing Snort rules and other tools for network monitoring and detection. It is the second course of the major that its goal is to teach what it is like to be a Defensive Cyber Operator.

The last course of the Cyber Operations major is SY406 – Cyber Law and Ethics which is 3 credit hours and 3 lecture hours each week. This course is designed to study United States Cyber Laws and the issues behind those laws. The course

starts by studying the US Constitution and the Amendments and various computer and cyber laws. This course is non-technical but important for the future officer, because a Cryptologic Warfare Officers must know the laws behind their cyber operations and must always protect and defend the constitution and must know what is legal and what is illegal.

c. Conclusion:

This is the summation of the Cyber Operations Major at the United States Naval Academy. Every year, the courses are modified and changed and this paper follows the plan and matrix of the class that graduated in the year 2020. In conclusion, this major provides the basic understanding of Cyber Operations and has a variety of technical and non-technical courses but by no means provides enough education for someone to graduate and be ready to be an expert in the field. The reason for that is the goal of the Naval Academy. Since midshipman that later serve in the Cryptologic Warfare Community have to do 3 month of intense studying and training, having the fundamentals of Cyber Operations is enough to reach their goals and mission.

2. Bulgarian Naval Academy:

a. *History and Background*:

The Bulgarian Naval Academy was created 1881 in Ruse, Bulgaria and later in 1900 was moved to its current location in Varna, Bulgaria. At the beginning there were only 30 cadets per class with a total number of 150 cadets inside the Academy. Currently there are 168 cadets, however the Academy keeps expanding and there will be more in the future. The majors that are offered are Navigation, Mechanical Engineer, and Radio Communications and Cyber Security. Cyber Security is the newly found major and the first class to graduate with it will be the class of 2024. In the future, cadets that graduate with the Cyber Security major will work in the Communication Information Systems Department and in the newly developed Cyber Center at the Bulgarian Naval Academy. The Cyber Security major was introduced, because of the growing interests of that field and the need and importance for the Navy to have officers that are equipped to protect and defend the nation's networks.

At the Bulgarian Naval Academy, the length of study is five years, compared to four at the United States Naval Academy and midshipman choose their majors at the beginning of their first year. These majors are going to represent what they would be working in the future in the Bulgarian Navy. During the course of five years, cadets acquire two degrees one military which is Organization and Military Tactics, modified by their selected major and their civilian degree. After graduation they do not have to attend more courses and trainings when the cadets commission they would go straight to the fleet and start their future jobs.

b. Courses of Cyber Operation Major:

The Bulgarian Naval Academy as previously mentioned offers two degrees one military and one civilian. In the military Cyber Degree, the cadets study cyber security principles specifically for the Bulgarian Navy. They study defensive and

offensive cyber operations, how the Communication Information Systems Department works, what encryption schemes it uses and how communications are set inside the military network. They also study NATO and EU laws and documentations and etc. The purpose of this report is not going to be the military Cyber Security, but the civilian one.

The first course that is offered is Basics of Web Design. The course is 7 credits which is equivalent to 3.5 US credits and it teaches cadets basic HTML, CSS, JavaScript and JQuery. At the end of this course cadets will develop their own interactive website that included all of the topics previously mentioned.

The next course that is offered is Basics of Computer Technology and Communications. This course is an introduction to computers and computer technology and cadets learn binary and arithmetic binary calculations, they read and develop logic gates and schemes, logic registers and counters. The course is 6 Bulgarian credits, which is equivalent to 3 US credits.

The next course is Computer Architecture and Peripheral Devices. The course is 6 EU credits, which is equivalent to 3 US credits. In this course, cadets learn the structure of a computer systems and their separate components, types of computer architectures, peripheral devices and also during lab hours, cadets practice the installation and diagnostics of various components in the computer system.

The next course is Windows Operating System. This course is 6 credits which is equivalent to 3 US credits. In this course cadets learn the difference between the different versions of the Windows Operation Systems, ways of configuring the Windows Server and Windows 10, the different roles of Windows Server and must know how to install a Windows Operating System and how to use Server Manager. This is a very practical course that enables cadets to deepen their understanding of Windows machines and how it works.

The next course offered is Basics of Cyber Security. This course is 5 credits, which is equivalent to 2.5 US ones. This course as the title suggests discusses various Cyber Security topics in high level. It discusses topics likes vector attacks, basic vulnerabilities of vector attacks, audit programs, types of Penetration Testing, social engineering techniques, basic Web attacks, network analyzation and protection, firewalls, malware and worms. It offers cadets basic understanding of cyber security and lays the foundation.

The next course is Introduction to Network Systems. This course is the first out of four that teaches cadets about networks. It is 6 credits which are equivalent to 3 US credits. They learn the 5 layers TCP/IP model and how the different layers communicate between each other, CIDR. Cadets will also learn to work with crossover cables and create a wired network, how to configure TCP/IP protocols, and learn how to run diagnostics in a network and fix issues.

Another course that is offered at the Bulgarian Naval Academy is Object-Oriented Programming. This course is 6 credits, which is equivalent to 3 US credits. Cadets learn how to program in C++ and start from defining variables, loops, and classes to developing more complicated programs. This course is highly lab-based.

The next course is the second Networking course which is focused on Routes and Switches. It is 5 credits which are equivalent to 2.5 US credits. Cadets learn how to configure and control routers, the algorithm of RIP and OSPF protocols, the typed of VLAN, and the difference between the public and private IP addresses. During their lab hours, they learn how to configure NVRAM memory, TFTP server, RIP protocol, OSPF, VLAN, DHCP, NAT, to do Password Recovery.

The next course is Linux Operation Systems. It is 5 credits, which is equivalent to 2.5 US credits. During this course, cadets learn the basics of the Linux Operation System, file organization, how to configure Linux machines, and learn common issues regarding the OS and how to operate in a Linux environment.

The next course is Data Bases, which is 5 credits. During this course, cadets learn how to work and configure and maintain a SQL database, learn common attacks and how to defend against them, how to install SQL Developer, Data Manipulation Language, Data Definition Language, etc.

The next course is Penetration Testing. It is 5 credits in which cadets learn the way common cyber-attack work and how to counter them, what are the consequences of allowing those attacks to happen on your network and how to prevent them from happening. They must learn how to use network monitoring tools and how to do attacks successfully.

The next course is the third Networking Course – Scaling Networks. It is 6 credits where cadets learn how switches work, how to configure them and ways to control them. They learn the algorithm of Spanning Tree Protocol, Virtual Trunking Protocol, types of VLAN, and know-how to configure a local wireless network.

The next course is Windows Server Administration and it is 6 credits. In this course, cadets learn how to install and work on Windows Server, types of directories and their policies, how to install a domain controller, and its functions. Cadets must also learn how to operate different accounts and profiles in an active directory.

The next course is Big Data, which is 5 credits. Cadets must know unstructured databases such as NoSQL and how to work with Nadoor and how to sort information from those unstructured databases.

The next course is Cryptography and Cryptanalyst, which is 4 courses. It teaches basic Cryptographic techniques, their algorithms, basic stenography methods, digital signatures, and methods of protecting emails.

The next course is the last network class – Connecting Networks, which is 6 credits. In this course, cadets learn in-depth WAN, ways to perform diagnostics and fix errors in the systems, how to configure and use Frame Relay, HDLC, DHCP, and how to work with Security Device Manager.

The next course is Mobile App Development, which is 5 credits. Cadets learn how to do back-end and front-end mobile apps and secure them using Java. This is a very heavy lab course, whereby at the end of the semester every cadet must make their own mobile Android App in their liking.

During their last years, cadets have multiple classes on network, web, database, mobile app security, and reengineering.

c. Conclusion:

Since the Bulgarian cadets study five years, most of the courses in the later years are very practical and not only theoretical. This provides educated officers that do not need to attend future courses and training and are ready to hit the fleet. Part of the reason, why this is more technical is because the Cyber Degree is very new and there is a need of very qualified officers in the Bulgarian Navy.

Major Matrix

Class: 2020 Major: SCY CYBER OPERATIONS

Total Matrix Credit Hours: 142

	NS101, 2	NE203, 3	NN210, 2	NN310, 2	NL310, 3	NL400, 2	NS43X, 2
SI110, 3	NL110, 2						
CHEM1, 4	CHEM2, 4	SP211, 4	SP212, 4			ES300, 3	
CALC1, 4	CALC2, 4	SM223, 4	SM230, 3	EE301, 4		ES360, 1	
HE111, 3	HE112, 3	HH2XY, 3	HH216, 3	HM SS1, 3	HM SS2, 3		
HH104, 3	FP130, 3					EM300, 4	EA/N4XY, 4
		SY201, 4	SY202, 3	SY301, 4	SY304, 3	SY403, 3	SY406, 3
			SY204, 4	SY303, 4	SY306, 3		
					SY308, 3	SY4XX, 3	SY4XY, 3
					SY310, 4	SY401, 3	SY402, 3
[17]	[18]	[18]	[19]	[17]	[19]	[19]	[15]

Figure 1: Cyber Operations Major Matrix at the United States Naval Academy.

Conclusions

In Conclusion, when comparing the Cyber Degrees both at the Bulgarian and the US Naval Academy, it shows that the Bulgarian Naval Academy focuses more on practical skills, compared to theoretical and it's due to the fact that the length of the degree is different and their respective Navy's needs are also different. In both Academies, their degrees accomplish their goals and missions and provide qualified officers but in different ways.

References

1. Yuliyan Tsonev and Milen Sotirov, "Implementation of Gamification in the University Classrooms," *Conference proceedings of seventh national conference "E-learning in higher education," Sofia,* 2018, pp. 232-236.
2. United States Naval Academy Official Website, https://www.usna.edu/CyberDept/Academics/ [accessed June 2020].
3. United States Cyber Science Department, https://www.usna.edu/CyberDept/ Assessment/SCYStudentOutcomes.php [accessed June 2020].
4. Yuliyan Tsonev and Marin Marinov, "Nyakoi osobenosti na metodikata pri obuchenieto za izpolzvane na slozjni programni produkti," *Morski nauchen forum Tom 2, Varna*, *1996*, pp.225-230.
5. Bulgarian Naval Academy Official Website, http://www.naval-acad.bg/education/bachelor/cybersecurity [accessed June 2020].

About the Author

ENS Nikoleta **Georgieva** is from Silistra, Bulgaria and joined the Bulgarian Navy in 2016. She attended one year the Bulgarian Naval Academy and later transferred to the United States Naval Academy. She majored in Cyber Operations and graduated in May 2020, and then returned to serve in the Bulgarian Navy.