NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

CYBERSECURITY EDUCATION FOR MILITARY OFFICERS

December 2017

By: **Andrew Bardwell**
Sean Buggy
Remuis Walls

Advisors: **Douglas Brinkley**
Raymond Jones

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** MBA professional report

4. TITLE AND SUBTITLE CYBERSECURITY EDUCATION FOR MILITARY OFFICERS	**5. FUNDING NUMBERS**
6. AUTHORS Andrew Bardwell, Sean Buggy, Remuis Walls	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Cyber threats are a growing concern for our military, creating a need for cybersecurity education. Current methods used to educate students about cyber, including annual Navy Knowledge Online training, are perceived to be ineffective. The Naval Postgraduate School developed an "All hands" pilot cybersecurity course with the objective of increasing military officers' cybersecurity awareness. The three of us participated in the ten-week course to assess the delivery of the curriculum. This MBA project is a culmination of our critiques that support whether the course objectives were effectively met. Observations of the course were supplemented with a literature review on cybersecurity education. We found the course did increase our general cybersecurity awareness and introduced us to cyber terminology and concepts. The lectures of the pilot course included excessively in-depth discussions that were not at an "All hands" level and lab sessions of limited value. Our recommendations include restructuring the course to a maximum of four units by eliminating the lab portion and centering military-relevant discussions on cyber-defense management. For MBA students specifically, we recommend either scheduling this course during quarter one or moving a Joint Professional Military Education course to quarter one and filling the vacated time with the cybersecurity course. The ideal situation for MBA students is if the Graduate School of Business and Public Policy can create and deliver a Business School–tailored version of the cybersecurity course that fulfills the requirements of taking an "All hands" cybersecurity course.

14. SUBJECT TERMS cybersecurity, cybersecurity education, cyber-curriculum development	**15. NUMBER OF PAGES** 89
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

CYBERSECURITY EDUCATION FOR MILITARY OFFICERS

Andrew Bardwell, Lieutenant, United States Navy
Sean Buggy, Lieutenant, United States Navy
Remuis Walls, Lieutenant Commander, United States Navy

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2017

Approved by: Douglas Brinkley, Ed. D.

Raymond Jones

Don Summers
Academic Associate
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

CYBERSECURITY EDUCATION FOR MILITARY OFFICERS

ABSTRACT

Cyber threats are a growing concern for our military, creating a need for cybersecurity education. Current methods used to educate students about cyber, including annual Navy Knowledge Online training, are perceived to be ineffective. The Naval Postgraduate School developed an "All hands" pilot cybersecurity course with the objective of increasing military officers' cybersecurity awareness. The three of us participated in the ten-week course to assess the delivery of the curriculum. This MBA project is a culmination of our critiques that support whether the course objectives were effectively met. Observations of the course were supplemented with a literature review on cybersecurity education. We found the course did increase our general cybersecurity awareness and introduced us to cyber terminology and concepts. The lectures of the pilot course included excessively in-depth discussions that were not at an "All hands" level and lab sessions of limited value. Our recommendations include restructuring the course to a maximum of four units by eliminating the lab portion and centering military-relevant discussions on cyber-defense management. For MBA students specifically, we recommend either scheduling this course during quarter one or moving a Joint Professional Military Education course to quarter one and filling the vacated time with the cybersecurity course. The ideal situation for MBA students is if the Graduate School of Business and Public Policy can create and deliver a Business School–tailored version of the cybersecurity course that fulfills the requirements of taking an "All hands" cybersecurity course.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AERB	Advanced Education Review Board
APT	Advanced Persistent Threat
CAE	Centers of Academic Excellence
CENC	Commission on Enhancing National Cybersecurity
CEO	Chief Executive Officer
COA	Course of action
DHS	Department of Homeland Security
DOD	Department of Defense
DON	Department of the Navy
GSBPP	Graduate School of Business and Public Policy
IOT	Internet of Things
ITACS	Information Technology and Communication Services
JPME	Joint Professional Military Education
MBA	Master of Business Administration
MRI	Magnetic resonance imaging
NICCS	National Initiative for Cybersecurity Careers and Studies
NKO	Navy Knowledge Online
NPS	Naval Postgraduate School
NWC	Naval War College
SIEM	Security Information and Event Management
TOR	The Onion Router
USNA	United States Naval Academy

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

As cyber threats become more prevalent in our society, the need for cybersecurity education has increased in importance. Several studies and reports have shown the importance of cybersecurity and the millions of dollars that companies are losing to cyber-attacks. It is estimated that in 2017, the average cost to a company of a data breach was $3.62 million (Ponemon Institute, 2017). The Chief Executive Officer (CEO) of AT&T sums it up well, “Every company either has been breached or will be breached” (Morgan, 2017, para. 2). Cybersecurity has become such a huge issue in recent years with damaging attacks on companies like Home Depot, Target, and Equifax, as well as severe interference into politics.

We think that everyone can agree there is a need for cybersecurity education, especially for our military officers because the military is a priority target for our adversaries. While the private corporations listed previously are concerned with cybersecurity, an even more dangerous problem facing the military is cyberwarfare. The vast majority of our current forces have very little knowledge of cybersecurity, let alone cyberwarfare. As revealed in a 2012 *New York* Times article by Elisabeth Bumiller and Thom Shanker, then Secretary of Defense Leon Panetta brought to light a grim truth: the nation is vulnerable to computer hackers and a “Cyber-Pearl Harbor” is a very genuine possibility (para. 1). Cyber-attacks can be used against us by state and non-state aggressors. Bumiller and Thom’s article warned that the country’s infrastructure is at risk as power grids, public transportation, financial institutions, and other assets can be targeted by foreign adversaries (para. 1). Their article further notes that Panetta was particularly concerned with a cyber-attack “On our critical infrastructure… in combination with a physical attack,” which shifts the discussion to our military (para. 7). With the new emphasis on conducting cyberwarfare combined with the lack of cyber training for our military officers, a crucial gap remains. It is evident that our military officers of today and the future need cyber education.

In response to the need for cyber education, the Naval Postgraduate School (NPS) created a prototype "All hands" cybersecurity course. The prototype course was six-units: four lecture units and two lab units. The course met on Tuesdays and Thursdays from 1500 to 1700, with the labs on Fridays from 1000 to 1200. The course requirements were to write a weekly cyber journal, consisting of 500 or more words, that summarized what we learned during the previous week's lectures and lab, and to provide feedback to the instructors. Course journals were due each Tuesday. Each of our course journals is included in this project as appendices one through three. Our course journals provide an in-depth review of the course and support our analysis and recommendations.

B. PURPOSE

NPS offered the prototype course for the first time in summer quarter of 2017. The NPS Cyber Working Group designed the course and tested it on students from a variety of departments, including the three of us from the Graduate School of Business and Public Policy (GSBPP). The NPS Cyber Working Group is gathering feedback from the students who attended the course to help shape the content and delivery for future course offerings. The intent is to expand this program and to require "All hands" at NPS to pass the general cybersecurity course. We were recruited to attend the pilot course as representatives of GSBPP then complete this Master of Business Administration (MBA) project in which we provide a critique of the course, give recommendations for improvement, and provide recommendations specifically for MBA students who may be required to take this course in the future.

The requirement for cybersecurity education at NPS is being driven by top leadership in the Navy, specifically Admiral Bill Moran, the Vice Chief of Naval Operations (Department of the Navy, 2016). During an Advanced Education Review Board (AERB) meeting on 14 November 2016, Admiral Bill Moran "directed the NPS Cyber Working Group to develop COAs to recommend a way ahead to implement the All-Hands Cyber Course into graduate education curricula for all Navy Officers at NPS" (S. Jasper, personal communication, September 14, 2017). The results of the pilot program were to be presented to the AERB in November 2017 (S. Jasper, personal communication, September

14, 2017). The purpose of the "All hands" cybersecurity course is to make cybersecurity a priority in our Navy's education system and to increase the cybersecurity knowledge of military officers.

C. PROBLEM

The problem is that current methods used to educate students about cyber is ineffective. There is a perception that the annual Navy Knowledge Online (NKO) course is not increasing cyber awareness enough to mitigate the growing cyber threat.

D. RESEARCH QUESTIONS

Here are our research questions:

- What is the most effective way to deliver cyber education?
- Does the NPS prototype course replicate the most effective delivery method?

E. SCOPE

This project analyzes the prototype cybersecurity course offered by NPS in summer quarter of 2017. The three of us went through the course to gain a first-hand experience of the delivery and content. We are examining the effectiveness of the delivery method that NPS has chosen. Our focus is on the "All hands" cybersecurity course offered at NPS in summer quarter of 2017, and attempting to influence future iterations of the course.

F. METHODOLOGY

Our MBA project is unique in that the majority of our "research" consisted of attending the pilot cybersecurity course. We attended the course for the duration of the summer quarter and kept notes on what our experience was like and what we were getting out of the course. Upon completion of the course, we supplemented our observations of the course with literature reviews on cybersecurity education and data on cyber-attacks. We researched basic cybersecurity statistics to put the need for cybersecurity education into perspective. We also researched how civilian universities are delivering cybersecurity education, although we could not find any organizations that require "All hands" to complete a cybersecurity course.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

We did a limited amount of research on civilian universities and their methods for delivering cybersecurity education. From our preliminary analysis, we cannot identify a civilian university that has the equivalent of an "All hands" cybersecurity course as a graduation requirement for a degree. Several civilian universities offer cyber education courses, degrees, and certificates; none of them appear to be required for all students. The National Initiative for Cybersecurity Careers and Studies (NICCS) is an initiative managed by the Department of Homeland Security (DHS) and serves as a national resource hub for cybersecurity education (Department of Homeland Security, 2017a). The National Centers of Academic Excellence (CAE) program, sponsored by the DHS, designates more than 200 colleges and universities that have robust cybersecurity degree programs, with a goal of linking up cybersecurity professionals with the right set of skills to jobs in the civilian and public sectors (DHS, 2017b).

Most academic institutions focus on degree programs, but these 200 colleges offer a variety of courses, certificates, and professional accreditations (Newsweek Educational Insight, n.d.). We found several colleges offering a Bachelor of Science or Master's of Science in Cybersecurity with various specializations. We could not find a university that required all students to go through a cybersecurity course. The University of California school system President has recently required all staff and faculty to complete annual cybersecurity training consisting of a one-hour online training program, but students are not required to complete it (Jones, 2017). This instruction seems similar to the Navy's required annual NKO course on cybersecurity.

Harvard University is offering cybersecurity certificates, executive programs, and an eight-week online cybersecurity course. Harvard's cybersecurity certificate program includes entire courses on Big Data and the Internet of Things (IOT), Protocols and Internet Architectures, Risk in Information Security, Cloud Security, Cryptography, Networks, and Cyberspace and International Security (Harvard Extension School, 2017a). In the NPS pilot course, each of these topics was given approximately one or two hours of lecture time; for a Harvard cybersecurity certificate each of these topics is a

semester long course. We understand that the goal of the NPS program is not to provide advanced certificates to students, but the contrast between our pilot course and Harvard's certificate programs illustrates the limitations of only taking one course. Perhaps civilian universities do not require a cybersecurity course for graduates because there is no way that you can condense all the material down into a single course.

Further research into what is taught explicitly in these civilian programs is beyond the scope of this research paper, but a comparison to the NPS prototype may exist with Harvard's eight-week online short course titled: Cybersecurity: Managing Risk in the Information Age (Harvard Extension School, 2017b). According to the course's prospectus topics of the course include: cybersecurity risk, threats to an organization, managing cyber risk, understanding technology, cyber law, incident response and accountability, and mitigation strategies (Harvard Extension School, 2017b). On the surface, this class seems similar to the material that we have covered during the pilot cyber course at NPS, except online delivery. An alternate approach to delivering the course content could be an online class, in which case this Harvard course would be worth looking into for a comparison.

Due to NPS' intention to rollout an "All hands" cybersecurity course to military students, we have chosen to review the previous efforts of the United States Naval Academy (USNA). The military consists of many different backgrounds and experience levels, regardless of age. As the U.S. military continues to be more technologically advanced, the majority of its members are not as cyber savvy as one might think. Many members can be classified as non-technical users, meaning someone who has "Either no or minimal exposure to computer-security concepts, and who does not believe they use computers in their daily lives more than average" (Zepf, 2013, para. or p. 29).

As revealed in a 2012 USNA report by Brown, Crabbe, Doerr, Greenlaw, Hoffmeister, Monroe, ... & Standard, a May 2009 Cyberspace Policy Review by President Obama sparked the leadership of USNA to create a committee charged with formulating the cyberwarfare curricula for Midshipmen, or undergraduate students (p. 303). The report states that in August of 2009, a recommendation was drafted that would require a mandatory cyberwarfare lab oriented course be taken by all students regardless

of academic major, and the prototype course began in 2011 when it was administered to 50 percent of the incoming student body, eventually educating all newcomers to the Academy (p. 303 - 304). Following the initial rollout, the committee moved to a two-course, technically-oriented sequence. The Brown et al. report explains that this phasing approach was instituted to address non-technical users with the second course to instill advanced learning about cyber concepts and applications towards more technical career fields (p. 303 - 304). Notably, the four year programs of the USNA allowed the option of scheduling the mandatory courses in the first and third year of education (p. 303 - 304). What we found interesting, despite the large influx of 1200 students each year, is that the USNA overcame the challenge of teaching this course without making the students' schedules more burdensome (p. 304). By overcoming various challenges and aligning clear objectives, the USNA's Center for Cyber Studies has been able to create cyber savvy leaders ahead of other institutions across the Department of Defense (DOD) who will be required to keep pace. In addition to USNA efforts, other service academies are working towards similar programs.

During our literature review, we also came across government initiatives on cybersecurity. On December 2, 2016 President Barak Obama released a statement through the Office of the Press Secretary on the creation of a nonpartisan Commission on Enhancing National Cybersecurity (CENC) to assess cybersecurity in the nation and make recommendations on how to boost cybersecurity for the public and private sectors. The statement detailed a 35% increase in spending for Federal cybersecurity assets in the 2017 President's budget (para. 2). All of these changes were part of President Obama's cyber strategy to increase cybersecurity defense, deter malicious activity, and effectively respond to cyber incidents (para. 3).

In December 2016, the CENC presented a report on securing and growing our economy in the digital world. They identified six imperatives to focus on, which are:

- Protect, defend, and secure today's information infrastructure and digital Networks.
- Innovate and accelerate investment for the security and growth of digital networks and the digital economy.

- Prepare consumers to thrive in a digital age.
- Build cybersecurity workforce capabilities.
- Better equip government to function effectively and securely in the digital age.
- Ensure an open, fair, competitive, and secure global digital economy. (Commission on Enhancing National Cybersecurity, 2016)

These imperatives apply to our research. Cybersecurity education will help to accomplish three of the CENC's imperatives: protect and secure our digital networks, prepare consumers to thrive in a digital age, and build cybersecurity workforce capabilities (CENC, 2016). It seems like nearly every organization, whether civilian, government, or military, understands the need for increased cybersecurity and recognizes that education plays a role. The CENC report states, "There was much to readily agree on, including … the need for greater awareness (and) education" (2016, p. 1). This illustrates the root problem; current cybersecurity methods are insufficient to mitigate the growing cyber threat, and there does not appear to be a standard method of teaching cyber education.

III. DATA

The Ponemon Institute conducts an annual study on the cost of data breaches to global companies. According to the Ponemon Institute's 2017 study, the average cost of a data breach was $3.62 million, with each compromised record costing $141. The study also found that it took companies an average of 191 days to identify a data breach and 66 more days to contain the breach (Ponemon Institute, 2017). As revealed in a 2016 *Forbes* article by Steve Morgan, Dell's annual report shows the number of malware attacks has increased to more than 8 billion. Morgan further noted an AT&T report showing a "458% increase in the number of times hackers searched Internet of Things connections for vulnerabilities" (2016, para. 2).

Cyber threats may never be totally eradicated; therefore, we must learn to manage them to an acceptable level of risk. Developing a successful cyber risk strategy should involve a multipronged educational approach that aligns the business and technical arenas. "The risk calculus some private sector entities employ does not adequately account for foreign cyber threats or the systemic interdependencies between different critical infrastructure sectors" (Clapper, Lettre, & Rogers, 2017, p. 2). Currently, the U.S. Cyber Command serves as the leading office for the nation and seeks to increase cybersecurity. The aspect of national security and the threats that serve to uproot the stability within the United States or any other part of the world are quite pervasive. The events of September 11th attacks continue to represent a painful reminder that our adversaries will not operate by traditional means nor publicize the exact details of their next treacherous plot. We must keep our eyes open for the strategic threat of the future but also endow future leaders with cybersecurity knowledge and a strategy for defense.

The United States will continue to be subjected to cyber-attacks. Cyberspace is the latest dimension of a global commons, and we will likely become more vulnerable to global threats as hackers grow their computing power and take advantage of cyberspace (Williams, 2014, para. 5). The insecurity of cyberspace has increasingly threatened the United States in recent years. Following the hacking of the Office of Personnel Management, 21 million DOD personnel had their information stolen (Sciutto, 2015).

This event led to a requirement where all federal agencies were required to assess the security vulnerabilities within their networks.

It appears that the lack of security went deeper than initially assumed. The most recent U.S. Presidential election is believed to have been influenced by cyber operations. America's entire cyber infrastructure is vulnerable if our political processes are susceptible to manipulation. Every breach similar to what occurred at Equifax earlier this year jeopardizes the information of several million people. These attacks seek to weaken our future position by creating instability throughout the global market.

The physical and social borders of nation-states continue to stretch beyond their sovereign limits via new technologies (Reveron & Mahoney-Norris, 2011). This growth in technological advancement has led to transnational problems that create dilemmas for national security across multiple domains. Meanwhile, the U.S. military will continue with a strategy that emphasizes a globally networked approach to deterrence and warfare with fewer resources (Department of Defense, 2012). The previously mentioned situations are only a small snippet of what is to come if cyberwarfare continues to breach the strategic network of national security and demonstrates why employing the attributes of cybersecurity education is a strategic move in the right direction.

The NPS prototype course is one attempt to supply cybersecurity education, and our analysis will examine the effectiveness of the delivery of course content and whether it will address the problems of a lack of cyber knowledge in the military. We will now look at data that pertains specifically to the NPS prototype cybersecurity course. The prototype course is the method that NPS came up with to increase the cybersecurity awareness of military officers to mitigate the growing cyber threat. The course included the following lecture topics, in the order they were presented: cyber concepts; network and system technologies; IOT; cyber surveillance; computation and big data; machine learning and data analytics; cyber-crimes, weapons, and attacks; attribution, anonymity, authentication, and encryption; system and network monitoring; human factors and configuration; acquisition of security products and services; cybersecurity for supply chain operations; cybersecurity management; international law, ethics, and standards; military cyber operations; and cyber policy and strategy. The following lab topics were

included: Cyberstrike Wargame; CyberCIEGE Wargame; IOT demonstration; attack methods; attribution, anonymity, authentication, and encryption techniques; cybersecurity incidents; Information Technology and Communication Services (ITACS) field lab; and Russo-Georgian War and wrap up. Twelve different professors gave lectures during this course, and all lectures were video recorded.

The course objectives, as provided in the course syllabus, are as follows:

1. Demonstrate your understanding of cyber operations by making judgments regarding mal intent and true accidental incidents in a before and after wargame.
2. Compare the differences and relationships between cyber operations and military operations.
3. Identify internal and external threats and countermeasures as well as opportunities for risk management.
4. Assess how the Department of the Navy (DON) can improve resiliency from normal accidents, malicious attacks, and provide high reliability by using your understanding of various theories such as network theories, information systems theories, or electrical and engineering theories.
5. Predict potential future capabilities, tools, trends, and possible shocks or disruptions resulting from cyber-evolution. (S. Jasper, class notes, July 5, 2017)

The NPS Cyber Working Group created these course objectives based on guidance from the AERB (S. Jasper, personal communication, September 14, 2017). These objectives are attempting to provide a framework for the prototype course that will result in the most effective delivery of the content. Of note, the course syllabus also states, “This course does not assume a technical background in cyber or computer systems. This course intends to provide a broad scope of the cyber domain and to help students understand the implications of cyber threats, as well as opportunities” (S. Jasper, class notes, July 5, 2017, p. 1). The working group designed these objectives for students without a technical background in cyber or computer systems.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DISCUSSION AND ANALYSIS

A. PROS OF CURRENT NPS PROTOTYPE

We will now identify three pros of the prototype course. These pros illustrate the benefits we got out of the course.

1. Increased Cyber Awareness

Before taking this course, the three of us did not have any experience in cybersecurity or computer science. Cybersecurity was not a point of emphasis during our officer training pipeline; the only formal training that we have received was an annual NKO course. After taking this course, we developed a completely different mindset on cyber and now possess a much better understanding of cyberspace concepts and terminology. We have a vague understanding of how the Internet works, how organizations conduct cyber operations, and the actors involved in cyber space. What we do not know about cybersecurity remains very humbling, and we are more aware of just how complex cyber space is and how vulnerable our society and military have become. We all believe this cyber "turn of mind" will really benefit us during future tours in the military.

Specifically, some key themes that we are taking away from this course are the rise of technology, the offensive advantage, and the difficulty of attribution and responding due to the complexities of cyber space. We were exposed to a lot of new technology, such as IOT, which really illustrated how far advanced cyber has become and how much our regulations are lagging. With our increasing reliance on billions of electronic devices, it is amazing how productive we can be but also astounding how vulnerable we have become to cyber-attacks that could cripple our nation. After taking this course, we are more aware of the vulnerabilities that can be applied to electronics during manufacturing. In the acquisition community, we need to be mindful of where our hardware and software are coming from at all times. No subcontracting of parts or lines of code can be allowed by our contractors unless a program manager knowingly accepts the possible cyber risks of those modifications or substitutes.

Our professors established that offensive attacks have a clear advantage over defensive measures. Attackers are working in microseconds, or at the speed of computers, while defenders are operating at human speed and can take months or years to figure out what happened. This leads us to our need for defense in depth and active defense: making our defenses automatic and just as fast as our attackers is the only chance we have for mitigating the damage that attackers can do. The difficulty of attribution reiterated several times in the course, which really characterizes the complexities of cyber space. It is incredibly difficult to attribute attacks to an organization or state in an appropriate amount of time to respond to an attack. We got into many legal issues that underscored how complex cyber operations can be, and how the U.S. is held to different standards than non-state actors. Finally, we increased our knowledge of cyber just enough to hear about an incident and distinguish reality from fiction. We know enough to discern when other people have no idea what they are talking about from a fundamental cyber perspective. We now have an informed opinion, but not nearly enough to be an expert or to conduct any cyber operations.

2. Range of Instructors

A unique aspect of this pilot course was the range of instructors we had. Twelve different professors gave lectures during this course, which gave the students a variety of perspectives and opinions. We had professors who were very negative toward our cybersecurity abilities and others who were quite positive about our security. Many of the professors shared their personal experiences in cyber space and the impacts that different attacks had on them. The personal experiences of being hacked ranged from a breach of credit card data from Target to a work computer being hacked via a Magnetic Resonance Imaging (MRI) machine. The advantage of having multiple professors give lectures is that professors can stick to their area of expertise and give informed lectures on things that they are passionate about and work on regularly. Having different people lecture kept us a little more engaged during the lectures, instead of listening to the same person talk for three months.

3. Personal Cybersecurity Improvements

During this course, we covered several attack vectors that our adversaries utilize for cyber-attacks. This awareness has led us to make changes in our personal cybersecurity. We discussed phishing attacks in detail and saw several examples, and now know what is suspicious and what is not suspicious when checking emails from unknown sources. In our lectures we discussed that a significant portion of cyber-attacks are from phishing, so this significantly reduces our risk of an attack. During the lecture on encryption, we learned that the length of our personal passwords is the most important factor for password strength. The lecture showed the math behind the possible combinations of passwords of different lengths, and made the recommendation to increase your password to 18 characters in length; it would take several years for a computer to determine your password of this length. After this lecture, one of us went home and changed the password for all critical accounts, including retirement and investment accounts, bank accounts, and email account. We made our personal cybersecurity much stronger based on what we learned in this course.

B. CONS OF CURRENT NPS PROTOTYPE

Next, we will discuss the cons of the prototype course and our critique. The three of us each commented on these aspects of the course in our journals.

1. Discussions Went Excessively in Depth

The pilot course did not contain a representative sample of students from across campus; there were far more computer science students than there would be in a representative sample. In the pilot course, we had several students that had extensive knowledge of computer science and ample cyber experience, and a handful of students that had no cyber experience. If this course expands to “All hands” at NPS, then future iterations of this course will include students from all departments across campus. The typical student attending this course will not have a strong background in computer science, and each section of the course may only have one or two students with a computer science background. For the pilot course, we had several such students, which

is understandable given that computer science savvy students would be more likely to sign up for a pilot course on cybersecurity.

The result of having so many students with extensive knowledge of computer science is that when we had discussions in class, the discussions often went very deep and were very complicated. As students without any cyber experience, most of these discussions went well over our head and we did not get a lot out of them. The discussions had no structure and were often driven by the student's questions and opinions. This led us to lengthy talks that did not reinforce the lecture material, and we would usually discuss topics that were well beyond the scope of this course. For example, during one discussion prompted by a student we started talking about quantum computing, which is way beyond the scope of this course, and understandably we were lost. Once the course is mandatory for all students at NPS, the professors should tailor the discussions to individuals with no computer science experience. This will enable everyone in the class to participate in the discussion and make the class time spent on discussions more productive. The more participation in a discussion, the more people will share opinions and ideas, and everyone will have a chance to take something away from it.

2. Exclusive Use of PowerPoint

Every lecture revolved around a PowerPoint presentation. The presentations gave us a broad understanding of the cybersecurity concepts, but made them all very abstract and theoretical. There was very little, if any, practical instruction in the class. The objective is to understand cyber operations and not to make us into cyber operators, however, some concrete examples of computer coding, vulnerabilities, attacks, and defenses would have reinforced the material we were learning. The objective is not to make students capable of operating a network or conducting a cyber-attack, but more practical computer instruction would allow us to apply the material we learned and could potentially deepen our understanding of the concepts we cover in the lecture material.

3. Labs of Limited Value

The labs were unorganized, with the schedule constantly changing, and we do not believe that the labs reinforced the lectures. Most of the labs were just a continuation of

lectures, while some included a game or a tour. It would be possible to accomplish all of the things we did in these labs during normal lectures. The two labs that were the most beneficial were the Cyberstrike game and the ITACS field lab. The Cyberstrike game did a great job of reinforcing themes of the lectures, including the complexity of cyberspace, non-state actor's cyber activities, political implications, and difficulty on attribution and responses. We expected to play Cyberstrike again at the end of the course to show how much we have learned. In fact, it was stated in the course objectives that we were to demonstrate our "Understanding of cyber operations by making judgments regarding mal intent and true accidental incidents in a before and after wargame" (S. Jasper, class notes, July 5, 2017, p. 1). We were never given the opportunity to play the game a second time. The lab that we had scheduled to play Cyberstrike for the second time was instead spent playing a different game, again illustrating how the labs were unorganized and the schedule was constantly changing. The ITACS field lab was worthwhile and allowed us to think through how the concepts we had learned in class apply to running a complex network at a military installation such as NPS. Other than these two labs, most of the others did not take up the full two hours scheduled and ended up being additional lectures or an unnecessary use of class time.

4. Scalability Concerns

The concern with having multiple professors teach different topics is scalability. This class met on Tuesdays and Thursdays from 1500 to 1650, and there were no other classes scheduled during this time. The lack of scheduling conflicts for the professors made it easier for them to come in and give a lecture, however, once this class is expanded to "All hands" we are not sure if this set up will remain feasible. The scheduling of future classes will be during normal class hours, which will inevitably cause scheduling conflicts with instructors. If it is not feasible to have multiple professors come in to give lectures, then future classes will miss the benefits listed in our pros section. If this class expands to multiple sections, then it is likely that one professor will be assigned to each section and be responsible for teaching all of the material.

Maintaining this number of instructors will hinder scalability and is also a sign of how the content for the course has become too advanced. If one person cannot teach the course, then the information being presented is too advanced or too in depth for an "All hands" course. Keeping the material simple and focusing on the significant points will enable one professor to cover all of the lectures. Having multiple professors who are subject matter experts may lead to the content becoming too detailed and may take away from the learning experience. This is a ten-week course for "All hands," mostly non-technical students; professors should focus on the basic information that will increase students' cyber awareness and not go in so much detail. If future courses continue to use multiple professors, then one additional concern is consistency. This was not an issue for us because the course was graded pass/fail, but for future courses that are graded, the method for evaluating students should take into account this inconsistency of lecturers.

These cons reduce the effectiveness of the prototype course in delivering cybersecurity education to military officers and should be addressed for future courses. Next we will evaluate how effective the course was in achieving the stated course objectives.

C. DID THE COURSE MEET THE OBJECTIVES?

To answer this question, we will go through each course objective listed in the syllabus and analyze whether or not the pilot course achieved the desired objective. Then we will look at the course from a macro view and provide a few conclusions.

(1) Objective One: Demonstrate your understanding of cyber operations by making judgments regarding malicious intent and true accidental incidents in a before and after wargame.

The pilot course did not meet this objective because we ended up playing Cyberstrike only once. The course design was to have us play Cyberstrike during the first and last weeks of the course so that we can demonstrate our understanding of cyber operations during a wargame. We played Cyberstrike during the first week when we knew very little about cyber operations, but the schedule changed for the labs and we did not get the opportunity to play a second time at the end of the course. We were not given

a second opportunity to demonstrate how much we learned and our new understanding of cyber operations, so almost by default, this objective was not achieved. Had we stuck to the original schedule and played the Cyberstrike game again, we believe that we would have seen how far our cyber knowledge had come in just ten weeks, but we were never given that opportunity.

(2) Objective Two: Compare the differences and relationships between cyber operations and military operations.

The course achieved this objective. Our professors emphasized the legal issues involved with our nation conducting cyber operations, and how the decisions are made on who actually conducts the attack due to the different title responsibilities of our various government agencies. We also contrasted traditional military operations and the use of force or kinetic attacks with cyber operations, although when cyber-attacks result in a kinetic attack that can be considered a military operation. A key takeaway from our lecture on military operations was the paradox of when to use cyber operations. If you have an attack vector that can take advantage of a known vulnerability in your adversary, then you may only have this one chance to use the attack before your adversary identifies the weakness and patches it. If you conduct the attack, then your adversary will almost certainly patch their vulnerability. Our leaders must carefully weigh the risks of attacking or not attacking against the stakes involved, which will almost certainly be a very complex decision where the consequences are not fully understood.

(3) Objective Three: Identify internal and external threats and countermeasures as well as opportunities for risk management.

The course achieved this objective. We discussed the internal threats to a networked system, and the trade-off between security and productivity. The more secure your system is, the less capability your workers have to produce. As you reduce security and production increases, this can lead to internal mistakes like clicking on an email attachment that lets malware into the system. We covered a variety of external threats and attack vectors, including several examples of real life case studies of cyber-attacks. We spent an entire lecture covering risk management, which stated that the cyber-threat

cannot be eliminated and thus cybersecurity risk needs to be managed. The lecture gave us specific models of risk management and examples of government and civilian corporations adopting policies to address cyber threats.

(4) Objective Four: Assess how DON can improve resiliency from normal accidents, malicious attacks, and provide high reliability by using your understanding of various theories such as network theories, information systems theories, or electrical and engineering theories.

We do not believe that the course achieved this objective. During the lectures, we discussed concepts like defense in depth and active defense that would theoretically improve the Navy's resiliency to malicious attacks, but there was very little assessment conducted on what specific steps the DON should take to improve reliability and resiliency. The course exposed us to concepts of how networks and information systems work, but we do not recall any specific network theories, information systems theories, or electrical and engineering theories that we can apply to the DON to improve resiliency and reliability. We do not feel like we have gained sufficient understanding of any theories that we can directly apply to the DON to improve resiliency and provide a higher reliability of information systems.

(5) Objective Five: Predict potential future capabilities, tools, trends, and possible shocks or disruptions resulting from cyber evolution.

We do not believe that the course achieved this objective, and would argue that this objective should not be included in the "All hands" cyber course. No student will be able to make accurate predictions of future capabilities and trends after taking a ten-week course on cybersecurity. Students should focus their effort on improving their knowledge of current cybersecurity concepts and on understanding the complex cyber operations in a political environment, not on becoming subject matter experts capable of making sound predictions. The class did discuss possible shocks or disruptions, such as an attack on our financial markets or critical infrastructure. Yet we recommend that this objective be removed or re-written since making predictions based on concepts that you are just learning is not a reasonable objective.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS ON THE COURSE OBJECTIVES

Overall, the pilot course did not achieve the stated objectives. Of the five stated objectives, the course achieved two of the five, clearly did not meet two of the five, and partially achieved the remaining objective. While the pilot course did get us familiar with applicable terminology and concepts, we did not gain a deep understanding of any one topic. No one will be a cybersecurity expert after taking a 10-week course, especially one that is mostly abstract and theoretical and that contains very little practical instruction. We did gain a broad understanding of cybersecurity concepts and terminology, and the course was worthwhile. If the Cyber Working Group alters the objectives and adapts the lectures to address these concerns, then this course could easily be re-formatted to achieve the desired objectives. The course needs some improvements to effectively teach the material which will enable military officers to mitigate the rising cyber threats. While our opinions on the level of achievement of the course objectives are subjective, we think they are valid and would represent at least a portion of the student population. We believe our recommendations for future courses will address the cons of the prototype course and will more effectively deliver cyber education to military officers.

B. RECOMMENDATIONS FOR FUTURE COURSES

We will now discuss our recommendations for the next version of the “All hands” cybersecurity course at NPS.

1. Four-Unit Structure

Based on the amount of value-added time this class should be no more than a four-unit course. The labs typically lasted less than the two hours allotted, and most of the labs were not very valuable in reinforcing the lecture material, so we believe that the labs could be eliminated. Future courses can accomplish the few valuable things that we did during the labs in their normal lecture hours. We spent a lot of time on discussions that took away from the pertinent points of the lectures. Reducing this class down to four-

units may lead to a “less is more” situation where the instructors need to get to the pertinent information and main concepts to get the objectives complete, without the long conversations that go off topic. A four-unit structure can still provide all the value of the pilot program. Our lab time was used no differently than our class time, so combining the labs into the class time would not be very difficult. Most of the labs were of limited value, and it would be possible to incorporate the material that we covered during the labs into the lectures. For the labs that were exceptionally valuable, such as Cyberstrike and the ITACS lab, we recommend these be scheduled and conducted during the normal class lecture time.

The four-unit maximum is justified by the already packed schedules for the typical NPS student. We have personally had 18–20 units per quarter for each of the last four quarters. With the Naval War College (NWC) Joint Professional Military Education (JPME) courses already a very time-consuming commitment outside of our core MBA classes, there is not a lot of room in the schedule to reasonably expect people to add a six-unit course and complete their thesis on time. Adding one extra class and completing a thesis on time is feasible, but it seems like that would be a lot to ask given the already crammed schedule for students who are on shore duty. If departments are hesitant to force another course into their students’ schedules, then one alternative that could be explored is an online delivery for military officers. An online delivery, or video lectures, would enable students of all programs to fit the course into their schedules whenever it works best for them, and could potentially save on the amount of faculty time that would need to be devoted toward in-person delivery. An online delivery would alleviate scalability concerns discussed previously.

One alternative that the NPS Cyber Working Group may consider is a two-part course offering similar to the USNA sequence. The first part could serve to educate those with a non-technical background and fulfill the requirement for an “All hands” cybersecurity course. The first part would be a two-unit course and include the following topics: cyber concepts, IOT, and cyber-attacks crimes. The second part would be an optional two-unit course to cover the most relevant cyber areas in more technical detail. The objective of part two would be to allow students of technical and non-technical

backgrounds to gain and apply cyber skills in a real life setting that could be utilized in future assignments. All students at NPS would be required to take part one, although students with a cyber related degree (or those in the computer science program) can validate the course. This application would be more efficient because non-technical users would not be subjected to material beyond the scope of an "All hands" course, and technical users would not be subjected to redundant information.

One additional specific recommendation for the structure of the course would be to move the lecture on cyber-crimes, weapons, and attacks from week five to week one or two. This lecture was a basic lecture that defined cyberspace and attacks, and is something that we felt we needed very early on in the course, and were surprised it took five weeks to get to this lecture. Other than this one lecture, we felt the order of the remaining lectures was acceptable and needed no major changes. Finally, if this course is extended to "All hands," then consideration should be given for students with extensive computer science background, such as a computer science degree, to validate this course, as they are unlikely to get enough out of this course to justify their time.

2. Make Discussions More Worthwhile

A consistent critique in our course journals was the discussions that we had in class, as discussed in the cons sections. To make the discussions more worthwhile for everyone attending the class, they need to be at an "All hands" level. The instructors should not allow a computer science student to dominate the discussions and steer the conversations toward more complex material that is outside the scope of the course. We recommend assigning a short article on a relevant topic and spending 10 to 15 minutes discussing the article. Centering the discussion on an article will give everyone the opportunity to read the article and formulate opinions or questions, and should ensure the discussion stays on relevant topics that effectively reinforce the lecture material. We also recommend holding off on discussions until after all the introductory material is taught, perhaps waiting four weeks until assigning articles and opening up class for discussions. This would allow people who do not have any computer science background to gain an

understanding of basic concepts and to focus on learning the introductory lecture material before discussing cyber issues.

3. Scheduling the Course for MBA Students

With students typically spending significant time in their fifth and sixth quarters writing their thesis or MBA project, we would not recommend adding a class during those quarters, especially since students often enroll in NWC JPME courses during this time. The first quarter has a lighter load as students transition back into an academic environment. Quarters two through five have 18 or more units and students are working on their thesis during quarter six. Quarter one only has 13 units, so this is the only viable option that we see based on the current course matrix for MBA students. If the course is required and remains at four or six-units, then we recommend either 1) enroll students in the "All hands" cybersecurity course during quarter one, or 2) have students complete a JPME course through NWC (for example, Strategy and War) during quarter one and replace that block in their future quarters with the "All hands" cybersecurity course.

The ideal situation for MBA students is if GSBPP can create and deliver a Business School tailored version of the cybersecurity course that fulfills the requirement of taking an "All hands" Cybersecurity course. A Business School tailored version of this course would allow MBA students to learn cybersecurity concepts that are applicable to future tours and could remove the excessively in depth discussions that are only relevant to computer science students. A "One size fits all" course may not be the most effective way to deliver the course content, given the obvious disparity between MBA students and computer science students. If the Business School course is condensed down to a two-unit class and still meet the requirement, then the best place to schedule this course for MBA students would be in the first quarter. During the first quarter, we took a one-unit ethics class that met once a week on Tuesdays for five weeks, or the first half of the quarter. A GSBPP two-unit "All MBA students" Cybersecurity course could be offered during quarter one at the same time as the ethics course but on Thursdays. This would give 10 class sessions of two hours each during the first quarter. If GSBPP can create their own course that will fulfill MBA student's requirement of taking an "All hands"

cyber course, then this would be the ideal place to put it. Quarter one is very light, and after the fifth week the Ethics class no longer meets, so by assigning the bulk of the work in the second half of the course it will have the least impact on students' workload and schedule. If this is not an option, then we recommend the previous two options we discussed for MBA students to take the "All hands" cybersecurity course.

C. RECOMMENDATIONS FOR FURTHER RESEARCH QUESTIONS

These are possible follow on thesis topics that could provide value to NPS as they budget for future cybersecurity courses.

1. Cost-Benefit Analysis of Different Teaching Methods

Is an "All hands" NPS cybersecurity course the most cost-effective method of delivering content? Requiring all NPS students to take a cybersecurity course will demand a team of professors and support staff to provide the necessary number of offerings in order to get thousands of students through this course. Online versions of the class could be a viable alternative to in-person meetings. JPME courses are offered in person at NPS and NWC but also through distance learning courses to officers in the fleet. We recommend a cost-benefit analysis be conducted on the different possible versions of the course. Historical JPME course data would likely be analogous to future offerings of cybersecurity courses.

2. Analysis of Civilian Universities' and Corporations' Cybersecurity Training

How do civilian universities, businesses, and other organizations conduct cybersecurity training? We discussed some basic findings of what a handful of civilian universities are doing with cyber courses, with several universities offering degree programs in cybersecurity but none offering "All hands" courses. More in-depth research into the material and content of civilian universities' courses would be beneficial. Researching how civilian companies (especially tech companies in nearby Silicon Valley) conduct cybersecurity training could be an even better insight into what content we should include in future iterations of this course.

D. CONCLUSION

There is a definite need for cybersecurity education, both in civilian and government organizations. Our military seems particularly vulnerable and ought to lead the charge on cybersecurity education. The “All hands” cybersecurity course at NPS is attempting to deliver effective cyber education to military officers. We believe the course would be more effective with a four-unit structure to ease the burden on students with full schedules. Minor changes in the delivery of the course, such as eliminating the labs and tailoring discussions to students without a computer science background, will help achieve the course objectives. The structure of the course and number of sections needed to get “All hands” through this course needs further evaluation. The ideal situation for MBA students is if the Graduate School of Business and Public Policy can create and deliver a Business School tailored version of the cybersecurity course that fulfills the requirements of taking an “All hands” cybersecurity course. Delivering cybersecurity education in the most effective way will raise our officer’s awareness of cyber issues and help mitigate the rising cyber threats.

APPENDIX A. BARDWELL COURSE JOURNALS

A. JOURNAL ONE: JULY 11, 2017

The “Five W’s” of cyber offer a good reason as to why we should all care about cyber and how it is used, whether for good or nefarious reasons. First, why is there cyber? Communications were standardized. This allowed for things to be reverse engineered. Modern computers all became comprised of the exact same thing, a processor that runs instructions from rewritable memory. This made it easy for anyone to run almost any kind of program they wanted. Whether they were the owner of the system or not. Mass production off identical systems started becoming possible. When did standardization occur? It happened in the 1990s due to the fall of the Soviet Union and commercial off the shelf (COTS) parts becoming significantly cheaper than custom ones. What could be in cyberspace? Anything with computer power and an input/output interface. Many of the items we use in our everyday life fit this description. Phones, laptops, cars, and some refrigerators. Where is cyber? Anywhere a processor capable of sending and receiving information exists. For the humans, this means cyber stretches way out into space where we have sent out satellites like Voyagers 1 & 2 or Pioneers 10 & 11. It also means cyber stretches all over the globe. Who must worry? The answer is simple, everyone. A great example was given in class with the MRI scanner. Although there wasn’t any data that needed to be protected on the machine itself, it was connected to a network with other computers that did have important data on them. The MRI served as an access point for those wishing to cause harm to the system.

For the content presented in class, the introduction was a bit advanced for a class that claims “This course does not assume a technical background in cyber or computer systems.” Specifically, the discussion about mal-ware, ransom-ware, and Wanna-cry without explaining their definitions or the scenario. Followed by a discussion of Wanna-cry that only a few (2-3) students even knew enough to comment on. Seemed too advanced a discussion for the class. After that specific topic was wrapped up then the rest seemed more at the level the course was described to be. It would have been more helpful for us if the Wanna-cry was explained to us like the Morris Worm was. Good use of

metaphors such as guerrilla warfare, electronic frontier, and wilderness to explain the cyber environment. This made information much easier to absorb.

B. JOURNAL TWO: JULY 18, 2017

Cyberspace: "Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networking systems and associated physical infrastructures." Cyberspace is hard to define though because other domains also use electromagnetic spectrum and can affect cyberspace. Like jamming for example. Jamming uses the electromagnetic spectrum and can affect cyberspace but still would not be considered part of cyberspace. Using whiffle balls we demonstrated how data travels through cyberspace. Data doesn't travel how a person thinks it would. It doesn't always use the shortest route getting from one destination to another and doesn't always use the same route. I enjoyed the professor describing the Internet as not streamlined like a German car but more like a shanty held together with lots of duct tape.

From there we went on to the five-layer (TCP/IP) model. This Internet Protocol is a set of rules for how a process should be carried out. After covering TCP/IP, we then went on to encapsulation. This concept was demonstrated to the class through the use of envelopes. As data moves through the layers it is given a header. The header is like an address written on an envelope. As the data moves through the layers more and more headers are attached to it. In class we put envelopes into bigger envelopes. This was a pretty easy concept to grasp, especially with the envelope reference.

Next we dove into physical equipment and network infrastructure. I thought it would have made more sense to talk about this topic right after defining cyberspace but before we learned TCP/IP and encapsulation. More people are familiar with the hardware involved but not the protocols.

On July 11th, second half of class we stopped the PowerPoint presentation and went to open discussion for any questions the class may have. Good in theory, but the questions weren't related to what was talked about in class. They were about quantum computing and unbreakable encryptions. A question related to infrastructure eventually

came up. It was good, understandable, and related to the lesson topic. Felt like 2–3 students controlled the whole discussion and left the rest of the class in the dark. Instructors need to be aware the level of the discussion is elevating beyond comprehension of the majority of the class. Didn't have the same problem on the 13th. Questions stayed on topic and all the class was able to benefit from it.

C. JOURNAL THREE: JULY 25, 2017

This week in class we discussed IOT. To my understanding, IOT is a bunch of network capable devices all connected around the world. We were given the official definition of "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies." Networking evolved in three waves. The first, taking place in the early 90's was when we were still perfecting how to connect PCs to other PCs. All the users at the time were pretty tech savvy since it was all text based data sharing. Still, there were 100's of millions of devices connected. The second wave came about in the 200's with user level sharing. Users were no longer just the tech savvy but also consumers with little technological knowledge. The number of devices connected had jumped to around 6–7 billion. During the third wave in the 2010's, large volume data sharing had come about. Devices were autonomous and not needing a user to operate them anymore. This was the dawn of the IOT. Over a 50 Billion devices connected and rapidly growing.

On the subject of IOT, we also discussed cloud computing. Cloud computing is using someone else's equipment for your own computing needs. Companies like Google lease out equipment for data processing and storage. This allows users to access larger computing capabilities without spending the money for the equipment themselves.

The pros of this are more capability, more storage, and cheaper. The cons are that the servers are public, a connection is needed, and there is an inherent risk of data being stolen or shared without authorization. Along with cloud computing the idea of using cellphones as servers was also brought up. The perk of this would be that we could be our own server instead of trusting other companies to store our data. Like posting pics on

Facebook. The pics would be pulled from your cellphone instead of the Facebook servers.

Finally, we discussed different computing systems like cyber physical systems, pervasive computing, ubiquitous computing, ambient intelligence, and automatic computing. Cyber physical systems are controlled by their own IOT. Ships can have multiple CPS like the electrical system or water system. Pervasive computing is an intelligent environment like an automatic light switch and is not mobile and is highly embedded. Ubiquitous computing is like pervasive but is very mobile. An example of this would be GPS.

The lab this week was very lacking. I do not think any value was added by showing us the Raspberry Pi parts or the tour of the Robo Dojo. All of this could have been accomplished during normal classroom hours I think.

D. JOURNAL FOUR: AUGUST 1, 2017

Without looking at the slides and regurgitating what they say, I think I can only give a rough definition of Big Data. Which to me is large amounts of information that are almost inconceivable to store and process. This includes things that one would not initially consider data like sites visited, items bought, movie preferences, etc…

In my notes:

Taxonomy of Surveillance (high too low):

1. Open source Data: websites, social media, and public records (example: police response to 911 call).

2. Ecosystem Tracking (bread crumbs that point back to where you've been)

    a. websites

        i. Cookies/Flash Cookies

            * Unique identifier

            * Transmitted to websites to remember preferences

* (Flash) save adobe Flash preferences

ii. Beacons

* Alerts owner (tracks amount of users)

* Identify active email accounts

* Can be used in webpage or email

iii. Browser fingerprint

* User agent string: browser type/version, OS, language

* Time zone

* Fonts used

* Browser plugins

* Screen size and color depth

* Cookies enabled

iv. Canvas fingerprinting: browser is identified uniquely

v. OS fingerprinting

b. Countermeasures

i. Incognito mode (weak)

ii. Tor

* Proxy service

* The Onion Router(TOR): Hops between multiple routers

* Virtual Private Networks(VPN)

* Portable apps

iii. Opt-In's

3. Real time monitoring

a. Rogue base stations

b. Unsecured control plane data

c. MAC address randomization

i. Example of a cell phone constantly beaconing while looking for a gateway.

d. De-anonymization attacks

e. Content based attack vectors

i. Camera: taking and sending constant photos without user knowing

ii. Screen refresh: using screen refresh to transmit a fm signal and send data off a device.

iii. Microphone

iv. Eyeball reflection

v. Accelerometer

Four V's of Big Data:

1. Volume: loads, click stream, active/passive sensor, speech, social media…

2. Variety: Structured, Unstructured, Semi-structured

3. Velocity: Speed of generation and rate of analysis

4. Veracity: how much do I trust the source of the data

Lesson seemed to be taught very rapidly and seemed a bit advanced for me. I was unable to retain much or take notes effectively. I need a slower and more rudimentary class to explain this topic of Big Data and Cloud Computing. After class had concluded, I could define Big Data and that's about it. Also, discovered there is a 'Weekly Topics Area' tab on Sakai. Possibly all other students as well since no one knew there was an article to read or video to watch.

E. JOURNAL FIVE: AUGUST 8, 2017

Material Comprehension:

Digital Dark Age: The perception of a possible future situation where obsolete file formats will make it impossible to read historic electronic documents. I do not really see this as a problem if everything is being stored in the cloud. Seems like it applies more to obsolete media forms like old floppy disks.

OODA Loop: Observe, Orient, Decide, Act, Feedback

Data flow:

1. Collect

2. Process

3. Preparation/Clean: id missing data or anomalies (incorrect data), detect redundant data, rescale and normalize.

4. Understand data: Use of 'Features' (representation of data in another space) like a histograph to understand the data.

5. Build Model

Attack Vectors:

1. Spear Phishing: Lures unsuspecting people to act or provide information via seemingly trustworthy electronic communications.

2. Watering Hole: Malicious actors infect a legitimate website with malware for the purpose of targeting visitors of that site.

3. Point of Sale: Compromises POS terminals where customers swipe a payment card at a checkout counter.

4. Web Applications: Exploit a Web application vulnerability in order to access resources or make changes to data.

5. Distributed Denial of Services (DDoS): Flood a target server with thousands of communication requests originating from multiple compromised machines to deny access or service. Used either to use up bandwith or overload a service or database.

Observations:

Lesson on 01AUG was taught very rapidly again. Professor Stefanou needs to slow down. Once again, the discussions are beyond my comprehension. The same 2–3 students asking/answering all the questions. The rest of the class is completely quiet due to the level of material being taught and discussed. I think the more advanced students, who you were hoping would help enrich the learning experience, are actually hindering it. Where was the Data Analysis ppt located? All my time was devoted to note taking and not towards comprehending the material. The articles and videos posted are not preparing me for class.

The lesson on 03AUG "Actors and Attack Vectors" was a good lesson. This was taught at a level I could understand. Recapping general concepts like, what is cyberspace, can be helpful instead of bombarding the students with new information constantly. The lesson also tied in well with other lessons we've learned along the way like the IOT and general networking concepts.

I think the class has lost sight of the difference between a Lab and a Lecture. If there is not productive activities to fill the lab time then I would suggest not having it.

F. JOURNAL SIX: AUGUST 15, 2017

Material Comprehension:

WWII: Colossus was the first programmable electronic digital computer… Code making and code breaking led to programmable digital computers.

Ciphertext vs Plaintext: Plaintext is encrypted with a key, changing it to ciphertext. Cipertext is transferred to its destination where it is decrypted with the key and turned back into plaintext

Types of encryption:

1. Symmetric [secret key]: both keys are the same

    * Secret key must be conveyed to recipient

    * Short keys, very fast encryptions

2. Asymmetric [public key]: two different keys

    * +private key never travels

    * –long keys, slower encryption

3. Combo:

    * +Use public-key system to send a secret key

    * Secure key distribution

    * +Use that secret key for symmetric encryption

    * Fast encryption/decryption of main message

Styles of encryption:

    * Block ciphers: fixed number of bits, encrypted as a unit.

    * Stream ciphers: encrypted bit by bit, usually Extendable Output Function (XOR) with keystream.

Brute-force attacks try guessing every possible key. Requiring long passwords with numbers, special characters, and capital letters make it harder if not impossible for these attacks to work.

Block cipher modes:

1. ECB, electronic codebook: block by block. Not recommended because easy to break.

2. CBC, cipher block chain: randomize plaintext first. Better, cannot encrypt blocks in parallel but can decrypt in parallel.

3. CTR, Counter: encrypt counter to get keystream: stream cipher. Good if used correctly, can encrypt and decrypt in parallel. Need to change values constantly to maintain security.

Observations:

Good discussion about trusting DOD certs for DOD websites. We are so used to just continuing to/trusting websites our browser tells us use an untrusted cert because it seems like all DOD websites pop up as untrusted certs. This poses a vulnerability to the DOD because if someone were to spoof a .mil website, we would most likely just tell our computer to trust the cert and continue to the website. Hash function was a bit confusing.

History wrap up at the end was a good way to end the class. Examples of code breaking changing the course of history like during WWII. Information advantage can allow victory even when there is a material deficiency. Although we have used this to our advantage in the past, it could be used against us in the future.

I'm still confused on the concept of public and private keys. The key demonstration didn't really help solidify how the keys work. I think the diagrams used in class were more useful than just watching text go across the screen and taking his word that these keys are doing their thing.

Footprinting Lab: This portion of the lab has potential. Once again, the lab turned into just another lesson it seemed. Recommend not running through all the steps of the lab and then having the students do the exact same thing. If you want to show us how the steps are done, then use different websites, servers, and IP addresses.

G. JOURNAL SEVEN: AUGUST 22, 2017

Material Comprehension:

Security vs Usability: There is a balancing act between the two. High security can hinder usability and High usability can create vulnerabilities in security. What we aim for is "usable security" or "secure usability." Good examples of this was demonstrated with the security pop-up prompts. Although the system caught something, the user would be

unable to understand what is meant by it and could choose the wrong option presented to them and compromise the system.

Basic Design Principles:

1. Visibility: User is aware of system status.

2. Math the system to the real world: Use of effective metaphors and real world language wherever possible.

3. User Control: Try to give the user the initiative.

4. Consistency: Always use words, imagery, and symbols the same way.

5. Error Prevention: Try to put the user in a position where errors cannot occur.

6. Recognition not recall: Do not force the user to remember commands and actions.

7. Flexibility and Efficiency: Should be usable by a novice and efficient for an expert.

8. Aesthetics and minimalism: keep clutter to a minimum

9. Meet user's security expectations: Meet expectations and assure the user would have tto explicitly act to violate.

10. Secure all interfaces, not just the main one: Its one system to the user, so be consistent.

11. Place files in location that meet the minimum security expectation: If files are encrypted, keep files encrypted.

User Principles:

1. User is usually a weak link in any security system.

* Users can be fooled.

* Users behave in predictable ways

* Users may act under stress

* Users are careless

2. User interface security is far more than just having an effective password and encryption policy.

* Make it easy for users to make secure choices and actions.

* Design security into the interface.

* Make security visible and obvious.

Observations:

Lab this week was more on par with what I expect from a lab. Very hands on and not just another lecture. The game was very engaging and will be even better once software is developed and the human factor for calculating points/outcomes is removed.

H. JOURNAL EIGHT: AUGUST 29, 2017

Material Comprehension:

22AUG: Acquisition of Cyber Capability; COL (R) Ray Jones

There is a major dependence on software in acquisitions today. 85% of the F-22 functionality is software driven. Lines of code needed to operate these new high-tech project is exponentially growing. Definitions: Global Information Grid (GIG), Joint Capabilities Integration & Development System (JCIDS).

Cybersecurity sustainment components:

* Software maintenance

* Software patching

* Disposal of hardware and software

* Impacts to the LCSP (LCSP?)

24AUG: Cybersecurity for Supply Chain Management (Dr. Doug Brinkley)

Even the simplest of supply chains have many entities within them. Now compare that to the military supply chain where 4.9 million repair parts move through. The most

important element of a supply chain is information flow. Complex systems are used to control these operations. This presents a problem because many of these entities in our supply chain are not held at the same security standards that we are.

Cyber strategies should be developed with the assumption that your system will be hacked.

GAO found out the DOD supply chain is vulnerable to counterfeit parts and when we find them we aren't taking appropriate action to correct the problem (inspect systems/ recall parts).

25AUG: Lab; Cybersecurity Incidents

Surface Web: Wikipedia, google, bing, etc.. Publically indexed and accessible by anyone.

Deep Web: Accessible through your normal browser but not indexed so it does not show up. Example: Our student profile at NPS. PYTHON is part of the deep web.

Dark Web: Special software needed to find or view contents.

TOR & I2P used for Dark Web

Cyber-attack types:

1.Theft of Data (criminal)

2.Exploitation of data (espionage)

3.Denial of service (protest)

4.Destructive action (damage)

Observations:

22AUG: A little too in depth on the whole acquisitions process. Felt we were just in an acquisitions class for the first hour. Did not relate to cybersecurity at all except for the stats on the increases in the use of software in programs. By the last half hour, cybersecurity was getting tied into the acquisitions process finally. Lots of acronyms make the information hard to absorb. Made even harder by the fact that not all acronyms

are explained or spelled out. I would recommend simplifying the acquisition process and relating it to cyber more. If this class cannot be taught by a cyber-professor than it is too advanced for the cyber course. I thought the software stats given at the beginning were a good example of this or the software code example given on Thursday at the end of class.

24AUG: Even though we discussed supply chains, it was very cyber oriented. PCS to Guam story was very interesting in expressing the point that IT only needs to be disrupted a little to cause huge problems. This was a very good supply lesson from a cyber viewpoint. Stories were engaging and interesting.

25AUG (Lab): Not a lab, just another lecture. "To my understanding" seemed to be the phrase of the day. Otherwise, it was a good class with lots of good information related to cyber-attacks to give us a better understanding of what hackers are capable of.

I. JOURNAL NINE: SEPTEMBER 5, 2017

Material Comprehension:

31AUG: Defense in Depth

Layers of Defense were covered, including: Perimeter Security, Network Security, Endpoint Security, Application Security, and Data Security.

Protect Confidentiality, Integrity, and Availability (PCIA)

Security Objectives: Each dictates the security controls prescribed to safeguard the objective: confidentiality, integrity, availability.

Layer Security Controls that are preventative and detective: physical layer, network layer, host layer, application layer, data layer. Definition: Web Application Firewall (WAF).

Definitions: HUMINT (human intelligence) and SIGINT (signal intelligence).

Actionable Intelligence: To effectively defend against cyber-attacks an organization needs access to threat intelligence and the ability to act on that intelligence.

Mapping and military deception…

Observations:

A breakdown of the risk management process is not needed because USN personnel are required to do annual General Military Training on the subject. The process is engrained into us. “The cyber threat cannot be eliminated; rather, cyber risk must be managed.” This applies to all aspects risk in the military and is not cyber specific. Simple conversation on the generalization of this quote spiraled out of control into a conversation with so many unknown acronyms that I could not follow it.

Risk cannot be eliminated, only reduced to an acceptable level. It is everybody’s responsibility to reduce risk. We are all taught and retaught this concept every year.

Risk Analysis, risk response, risk tolerance, and risk transfer are all part of our annual GMT’s. Most of the first half of class could have been skipped without affecting the learning we received from the class. The discussion on moving certain services at NPS to cloud services run by a public company was a good example of risk vs reward in the cyber arena.

Defense in Depth lesson went by way too fast for me to really retain anything but the basic concept that several layers of protection are needed. Also, it seems almost impossible to make a system that is “user proof” when it comes to security.

During the Lab, we saw a lot of really interesting graphs displaying active attacks, email filtering numbers, etc… These would be nice to use in the classroom.

J. JOURNALS TEN AND ELEVEN: SEPTEMBER 12, 2017

Material Comprehension:

05SEP: Ethics of Cyberwar

Pacifism vs Real Politic: Two extremes of the spectrum on the justification of war.

Jus ad Bellum: Justifications for going to war: just cause, just intent, last resort, proportionality (strategic), hope of success, legitimate authority, public declaration.

Jus in Bello: Justification of tactics used during war: proportionality (tactical), distinction, necessity.

A nation could be justified in their reasoning for going to war but not use justifiable means and vice versa.

Attribution Problem: Cannot attribute an attack to an actor due to the inability to identify the aggressor. Common problem in cyberspace. Can you be morally justified to go to war without 100% knowing who the aggressor of an attack is?

Norms for the cyber realm and the physical realm are very different. The door analogy was a good example. It would never be ok for someone to just walk around a neighborhood checking front doors to see if they are unlocked but it is ok in cyberspace for people check for open ports on someone else's computer.

07SEP: Military Cyber Operations (John McEachen)

Timing of Cyber Conflict Model: Value of a weapon is a function of: Stakes, Stealth, and Persistence.

08SEP: Lab, Russo-Georgia War

Cyberwarfare offers an offensive and defensive capability.

1. Targeted government websites
    a. Overloaded sites
    b. Defaced with "win+love+in+Rusia"
    c. Spoofing websites
2. News Agency and Radio were hacked
3. Internet traffic was rerouted through Russian servers
4. Denial of service attacks

To win against cyber militias we need to be able to detect, track, and disrupt financial flows to these groups.

Observations:

‘War’ was not defined at the beginning of class. Hard to have an ethics discussion without defining the item being discussed. Good comparison of cyberwarfare to the submarines sinking ships in the Mediterranean. Do not assume the class knows what Stuxnet is or is familiar enough to talk about it. A little 5–10 second summary is all me really need to get up to speed.

Not labeling the y and x axis on the graph at the beginning of class render it pretty useless. I couldn’t tell what the graph was supposed to be telling me. Most all graphics used today seemed too busy and not very useful. Less is more when it comes to text on a ppt.

Not a lab once again, but another lecture. This was a great lesson connecting cyber and military tactics/strategy but it seems like we skimmed it a bit too fast. I would like to see more emphasis on the actual war. Maybe in the form of a case study for the class that goes through the full timeline so we can see the events unfold for both cyber and physical attacks. Some good points were brought up during discussion but I feel it would have been more productive if we had gone through the war in more detail. This could be one of the strongest lessons for the class if presented correctly.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. BUGGY COURSE JOURNALS

A. JOURNAL ONE: JULY 11, 2017

This week was the beginning of our quarter, and after our first two sessions I feel like I am becoming aware of how much I do not know about cybersecurity. I am a Surface Warfare Officer in the MBA program, and I have very little experience with cybersecurity. As a junior officer at sea I was not given any training on this topic outside of annual NKO courses. I was a math major for my undergraduate degree, so I have no computer science knowledge and do not consider myself very tech savvy. I feel that I am a perfect candidate for this pilot program, because if this course is going to be taught to all hands at NPS, then many people like myself who have no cyber experience will need to go through this course.

The first session we had really opened my eyes about cybersecurity. It made things seem very doom and gloom, as if there is not a very high probability of success when it comes to cybersecurity. With the computerization of everything from health care to financial markets, it seems like our technology has advanced far ahead of our cyber defenses and regulations. I left our first session with the feeling that we are extremely vulnerable to a crippling cyber-attack, and that even our military is unprepared to handle this issue. I certainly appreciate the need to create a "cyber turn of mind" in our military forces, as the next conflict will undoubtedly involve direct cyber-attacks on military assets.

I got a lot out of listening to the 5 W's of cyber. WHY there is cyber: the standardization of computer systems that enable reverse engineering. HOW computers behave differently: the processors have changeable memory that will easily receive different instructions. WHEN cyber began: as the price-point for standardized, commercial off-the-shelf communication gear fell to a level that became widely available. WHAT cyber can be used on: anything with computing power and input/output interfaces. Finally, WHERE cyber is: anywhere are everywhere that a processor capable of receiving input or sending output operates, which as pointed out during the lecture is

literally beyond our galaxy since we have spacecraft operating far away. As a non-computer science savvy person, I found our discussion on the standardization of computers very interesting. Very few people are capable of making a computer from scratch, and it would be incredibly costly to do so since you would have to create your own chips and hardware and software. It is very cheap to buy a chip and existing commercial off-the-shelf computer parts to build a computer, which is what led to standardization in the first place and why cybersecurity is now such an important topic.

I enjoyed playing our cyber-attack game; playing the game really hit home how difficult cybersecurity is with just six actors, even though in real life there are millions of actors. I would have liked to play the game a second time during the same lab; my team spent most of the game just figuring out how it works and what it is all about. If we had played again, we would have been able to focus more on a strategy and forming alliances.

B. JOURNAL TWO: JULY 18, 2017

This week we focused on networks and systems technology. I really got a lot out of the lectures and feel that I have a much better understanding of how the Internet works and what the ramifications of the Internet are for cybersecurity. The slides used were very instructive and did an excellent job of using visuals to portray the underlying themes. For example, it was easy to visualize how the Trojan horse viruses work from the graphics on the slides. There was a lot of terminology and acronyms introduced, but the professor did a good job of explaining in detail how the components interacted and communicated. The envelope analogy was helpful to understanding the concept of TCP/IP protocol, with the 5 layers: physical (1), data link (2), network IP (3), transport TCP (4), and application (5) (J. Roth, class notes, July 11, 2017). We discussed the connections that form the Internet from a network of networks, including: backbones, provider networks, and customer networks. I learned the difference between a MAC address and IP address, and how the MAC address is permanently attached to a device while the IP address is given by the network. I found it interesting that a router can accomplish essentially the same tasks as a firewall, and that neither is immune to Trojan horse viruses. The CyberCIEGE game was very beneficial as a student with no networking experience. I felt that playing the

CyberCIEGE game really re-enforced the material that we learned in the lectures on how a network works, and how to configure networks so that they are reasonably protected. Getting to play around with the game will be very helpful and appropriate for "All hands" as they learn this information. The CyberCIEGE game also illustrated the concept of a balance between security and capability or production. We saw the effect of limiting the flow of information, and how people couldn't get things done. On the flip side, we also saw that not having any restrictions on a network and not training new employees can be disastrous and easily let in hackers and viruses. I also realized the importance of isolating computers that have vital information so that they are not vulnerable to attack.

On Tuesday instead of continuing with the lectures we opened up a class discussion for the second half of class. I got very little out of this particular class discussion. The same three or four students who have an advanced understanding of networks were the only students asking questions, and most of what was discussed went well over my head, for example when we started talking about quantum computing. The discussion was not structured and got very complex, and did not re-inforce the lecture material very well. This is an "All hands" cyber course, and that level of discussion is not beneficial to the majority of people that will be taking this course. What I recommend is to structure our class discussions around an article so that each student can read it and have a chance to contribute to the discussion.

C. JOURNAL THREE: JULY 25, 2017

This week we covered IOT: having more devices that are connected to the Internet than people. Billions of dollars are spent online, which illustrates the accelerating technology and the speed at which IOT is becoming a reality. With more than eight devices per person, there will be significantly less human interaction with the Internet, with most devices automatically interacting with one another through nodes (G. Singh, class notes, July 18, 2017). We saw in our show and tell day how far the technology has come and how cheap the pieces are, with the raspberry pies as an example of a commodity that is incredibly functional for its size and cost. The video we watched on robotic animals was very interesting and eye opening. The technology that we have today

makes it seem like we are not that far away from “Star Wars” types of droid or robot armies. For IOT, the professor emphasized that the most precious resource is power, so an important part of IOT is to have nodes operate in low power mode, and then “wake up” only when needed, and have nodes wake up other nodes to conserve power (G. Singh, class notes, July 18, 2017). We discussed the implications of IOT on the military, and how it can save on manpower and create far more technologically advanced and interacting weapons, as illustrated by the mine warfare example that the professor talked about. We also discussed the implications of having non-state actors being able to tinker with IOT and devise innovative means of attacks to further terrorist’s goals.

Feedback: On Thursday, once again the second hour of class was discussion based and the same four or five students who have an advanced understanding of computer science were the only students asking questions and participating. I did not get a whole lot out of this discussion, and I think that the level of complexity of these discussions should be geared toward “All hands” and not just the computer science students. I understand that there are a lot of computer science students in this pilot program, but it is an “All hands” course and in the future will be offered to a lot of people who have very little understanding of computer science, so I recommend that the discussions be tailored more toward them so that everyone is getting something out of the discussions. You might also consider in the next course moving the discussions back a few weeks until we have gone through all the introductory material. It may be beneficial to non-computer science students to get a basic understanding of cyber in the first month or so of class by focusing on the material, then launching into discussions in the second month of the course.

D. JOURNAL FOUR: AUGUST 1, 2017

In my opinion this was the best week of the class so far. I really enjoyed the material of cyber surveillance and big data, and I appreciated that we stayed on topic and did not have many discussions. Both professors did an outstanding job in explaining the material, and I came away from this week feeling that I got a lot out of both sessions. It is very helpful for me to absorb this basic, introductory information because I do not have a

lot of experience in computer science. I feel that after this week I have a better understanding of the material and am set up well moving forward.

For the cyber surveillance lecture, I learned a basic understanding of our individual online presence. I have had many experiences online that left me wondering "How did they know that?" When I visit a website and then later visit a different website, I would see advertisements for the previous website that I visited. Now I understand that the reason for this is the cookies, flash cookies, and beacons that store information on my hard drive and transmit personal preferences and activities to other websites (J. Roth, class notes, July 25, 2017). It was interesting to see that our browser fingerprint can be traced to me and just how much information can be mined from my browser fingerprint. We discussed a few ways around this lack of privacy, like TOR and proxy servers, but each solution presents new challenges and issues for privacy. Another cyber experience that I had is when I signed up for the Thrift Savings Plan (TSP), the military 401k plan. I had retirement accounts in Vanguard, and when I signed up for TSP, before TSP even mailed me my welcome packet and everything, I received a letter from Vanguard and it was apparent from the letter that Vanguard knew that I had signed up for a different retirement account, and they were explaining to me what options they have for me and asking if they could help me set up a retirement account. It is shocking how quickly information, no matter how private, can be sent over the Internet and how much these companies track what we do every day.

This story leads me perfectly into our lecture on big data, which we defined as large, complex data that push the limits of our technology due to the difficulty to store, process, and analyze with our traditional methods (M. Stefanou, class notes, July 27, 2017). Big data, and the gold mine that it represents for corporations, has led to innovative means of storage and processing such as NOSQL and cloud computing. We discussed the four V's of big data: volume (clicks, events, logs), variety (structure), velocity (speed of generation and analysis), and veracity (untrusted) (M. Stefanou, class notes, July 27, 2017). We went in detail on how cloud computing works, and the infrastructure and platforms associated with it. The key advantage with cloud computing is the ability to ramp up storage and capacity when needed, such as peak online shopping

days like Black Friday. I am excited to continue learning these basics and get into the relationship to cybersecurity, both offense and defense.

E. JOURNAL FIVE: AUGUST 8, 2017

This week we discussed data analytics and once again the discussion went very deep and detailed and was asked by the same four or five students who have computer science background. I understand that these students are very advanced and that most of this is below them, but this is an "All hands" Cyber course, and in order for everyone to get the most out of it I think the discussion should be tailored to people of all different backgrounds. The professor laid out a plan and we did not follow the plan at all because of these discussions. We did not even get to discuss the videos or articles that we watched/read before class, and he skipped the exercise that was planned for the end of class. During the lecture the professor did discuss how people can use data modeling or algorithmic modeling to analyze and make sense of the data. One example was how search engines like Google can use the number of searches for flu like symptoms to predict the patterns of seasonal flus.

In contrast to Tuesday, I thought that Thursday was the best lecture of this class so far. I have actually been waiting for a lecture like Thursday's, to get to the basics and definitions of what exactly cyber space, cybersecurity, and cyber-attack entail. I was very engaged in this lecture, and I felt that it was geared way more toward me and other people who do not have a computer science background, which was what I was expecting from an "All hands" Cyber course. We classified the different types of cyber-attacks, from data theft to destructive action. The phrase "armed attack" came up, meaning a cyber-attack that reaches the level of a kinetic attack, which I believe is a key definition in our world today because the next war will most likely involve "armed" cyber-attacks (S. Jasper, class notes, August 3, 2017). We discussed different attack vectors and ways to deliver malware or ransomware, as well as how companies find these vulnerabilities and then release patches to fix them, but the patch is only effective after an administrator applies it (S. Jasper, class notes, August 3, 2017). On day 1, Wannacry came up several times and I had no idea what that was, and after today I feel like I have a basic

understanding of that and other cyber-attacks, like spear phishing. Of all our lecture so far, I feel like I got the most out of this one. I recommend moving this class up in the schedule! I would have liked this lecture, or at least some elements of this lecture (the definitions, basics of cyber-attacks…) in week one or two.

During our discussion on Netflix and HBO's shows being hacked and released, I thought about how cyber could drastically change businesses. If these company's shows are stolen and released online for free, that might change the whole business model similar to the record labels when all of a sudden Napster was releasing their songs for free. Netflix can sue and take this to court, but the courts will never catch up to the hackers especially if it takes so long to figure out who did it. This could fundamentally change the business – if information (like videos of TV shows) is suddenly free, no one will want to pay for it and the value of it may go down – Netflix might have to make all its money on advertising and give away its TV shows for free.

F. JOURNAL SIX: AUGUST 15, 2017

This week we discussed encryption, authentication, anonymity, and attribution. I thought the lectures were very good and I was able to follow along without any issues. This lecture really reinforced concepts that we discussed earlier in the course, such as security built into the layers of the Internet and TOR. The professor did a really good job of explaining symmetric and asymmetric encryption, and the examples he gave in class really reinforced those ideas. I especially liked the example that he ran in class, where we actually got to see him code a message, encrypt it, and decrypt it. I believe we need more of these practical examples to see what it really looks like when cyber operations are conducted. Asymmetric cryptograph was counter intuitive at first, because it does not seem very secure to release a public key to everyone so that they can decrypt messages, but when combined with secret keys there are ways to get your message securely to someone else, with them using their private key and your public key. The public keys are effective and secure because the math behind the encryption is nearly unsolvable, but as computers advance quickly it seems like the encryption keys and math will need to be constantly updated to stay ahead of hackers with their new computer technology for code

breaking (D. Canright, class notes, August 8, 2017). Authentication comes down to our public key infrastructure and certificate authorities. The certificate authority issues public key certificates that enable authentication, although this method leaves a few vectors open for attack (D. Canright, class notes, August 8, 2017). We discussed anonymity that is achieved through the use of TOR, and allows people access to the dark Internet. Even though our adversaries might use anonymity to hide, there are still circumstantial ways to identify people online, especially when analyzing the coding of cyber-attacks and malware that was sent. Our brief discussion on attribution illustrated that attribution is an incredibly difficult challenge. There is not a lot of information about attribution since we do not want to publicize our secrets on how we do attribution. Our lab this week was worthwhile, and I feel like I learned a few resources to go to for information on websites. Actually getting on the computer and running some of those tests was a good exercise, especially for me because I am not very computer savvy, but I feel like this could have been done during lecture time and not during a lab.

Our discussion on the 1password and lastpass apps was very beneficial on a personal level. I believe the lecture stated over two thirds of attacks involve personal passwords being compromised, and this discussion actually prompted me to go home and change the passwords to my critical accounts: email, bank accounts, and investment accounts in particular. I used the guidance that was discussed in class to change my passwords, making them all 18 characters long since length is the most important factor for password strength. I have not yet downloaded lastpass but I plan to look into using a password app to further increase my security. This course has certainly opened my eyes to cybersecurity and I have made some changes around my house and on my accounts and passwords to shore up my own personal cybersecurity.

G. JOURNAL SEVEN: AUGUST 22, 2017

This week we discussed System and Network Monitoring on Tuesday, then human factors and designing secure user interfaces on Thursday. The lecture on network monitoring was very interesting and gave me a good idea about the capabilities we have to detect and prevent cyber-attacks. The professor discussed how cyber is all about

automation, and that our adversaries are using automation to attack us, therefore we need to use automation to defend our systems because there is no hope if the attackers are working in microseconds and we are working at "human speed." We discussed ways to monitor for events of security relevance, with those ways including statistical data, full packet data, session level data, and alert data (J. Fulp, class notes, August 15, 2017). Advanced persistent threat (APT) was defined as an attack that penetrates a system then sits dormant for a long time to collect data before blowing up (J. Fulp, class notes, August 15, 2017). To counter this, they have developed intrusion prevention systems to examine network traffic and detect and prevent attacks automatically. The Security Information and Event Management (SIEM) is the latest tool to perform this task. The SIEM collects logs from all systems on a network and normalizes them for comparison (J. Fulp, class notes, August 15, 2017). This allows for better detection and even automatic responses to perceived threats. We also discussed CANES, which is the IT system that the Navy is installing on ships, and I personally shared my experience with our Sailor's lack of willingness to adjust to new changes in technology, with everyone claiming they do not like the new system and things like that instead of embracing the change that is making us more secure. We really do need a cyber turn of mind…

The lecture on human factors and designing secure user interfaces was also very interesting, and something that we have all dealt with while using computers and phones. The key concept here was usability vs. security, and analyzing how we can make it easier for users to make secure choices. Several examples were given that show a prompt that is very confusing and that do not lead humans to choose the correct option. A better design would be to have software that automatically flags sketchy emails and alerts the user what the correct course of action (COA) is to avoid compromising security.

The lab this week was changed; the schedule promulgated had us doing Cyberstrike Wargame Part 2, with Freeman as the instructor but we did something entirely different. Are we not going to play Cyberstrike again in this course?

H. JOURNAL EIGHT: AUGUST 29, 2017

This week we discussed cybersecurity in acquisition and for supply chain management. The acquisitions lecture began with an overview of the acquisition system, with the basic question of how do we get the equipment that we have? In Business School we have taken courses on acquisition, so this first part was redundant for us. Professor Jones gave several examples and tied in cybersecurity into the acquisition process. One of the examples that stood out was the fact that Program Managers are responsible for creating KPPs, or key performance parameters, that keep the system secure from cyber-attacks (R. Jones, class notes, August 22, 2017). This does not seem very feasible, because first of all it is incredibly difficult to keep any system completely secure from cyber threats, and especially because the Program Manager is not a subject matter expert at the system they are responsible for or for cybersecurity in general. Professor Jones' point about the requirements creating growth in costs is valid; program managers need to be very careful about what they ask industry for, otherwise we will still be working on R&D for a project 10 years later with nothing to show for it.

Professor Brinkley discussed supply chain management and how information flow is critical to support supply chain management and thus cybersecurity becomes a big risk. One good point was in order to generate operational resilience, you should assume you will be hacked and have a plan in place to carry out the mission. Professor Brinkley shared his personal experiences in Guam and how even though the parts that ship's needed in order to get underway were sitting in their warehouse, they were unable to deliver them due to systematic issues with their software. When he tried to adjust their coding to run a different function, he did not realize that a few lines of code could have such a dramatic effect. They did not understand the coding in the system, and inadvertently ordered countless parts that they did not want at a cost of millions of dollars.

Friday's lecture was interesting as we went over a number of case studies that hacked into systems to accomplish theft of data, exploitation of data, denial of service, or destructive actions. Target and Home Depot were eye-opening examples because hackers can fairly easily steal valuable data on millions of people. These attacks are all very

complicated, but usually followed similar methods. Thieves will penetrate the system, maneuver around and chose their attack vectors, then release the malicious code to accomplish their objectives (S. Jasper, class notes, August 25, 2017). We also discussed the surface web and the deep web vs. the dark web. The iceberg image was very helpful, and it was amazing that only four percent of content is on the surface web, even though most people surf on the surface web and it should have most of the Internet traffic.

I. JOURNAL NINE: SEPTEMBER 5, 2017

This week we discussed Risk Management and Defense in Depth. For the risk management lecture, we defined risk as based on a function of how adverse the impact would be of a threat and the probability of the threat actually occurring (S. Jasper, class notes, August 29, 2017). Cybersecurity risk in particular is the specific threat to an information system, such as unauthorized access, disclosure, modification etc (S. Jasper, class notes, August 29, 2017). The model shown was a triangle with "frame" in the middle of assess (identify threats, vulnerabilities), respond (develop and determine COAs), and monitor (monitoring effectiveness and threat changes). We discussed how the cyber threat really cannot be eliminated, thus you need to manage the cybersecurity risk. I also thought it was interesting how executive orders have been passed to protect critical infrastructure (most of which is owned by private industry), and they required government agencies to follow the best practices while private companies are strongly encouraged to follow the guidance provided (S. Jasper, class notes, August 29, 2017).

For Defense in Depth, we discussed how this is the way that both private industry and the government go about defending their systems from cyber-attacks. Defense in Depth is split into layers: perimeter security, network security, endpoint security, application security, data security, all the way down to mission critical assets (S. Jasper, class notes, August 31, 2017). You also have the prevention and policy management aspect, as well as the operations, monitoring, and response side of defense. Defense in depth is basically a layered system that has multiple levels of defense, all of which will have to be infiltrated to get to the mission critical assets and this theoretically improves our defenses and makes it more difficult for adversaries to penetrate (S. Jasper, class

notes, August 31, 2017). It encompasses people, processes, and technology, and works to protect our confidentiality, integrity, and availability (S. Jasper, class notes, August 31, 2017). We also discussed the distinction between preventative and detective controls. We briefly touched on cyber threat intelligence and trying to identify the actors and threats using the intelligence cycle.

The lab on Friday was interesting to see how we actually handle cyber incidents and attacks, but it did drag on a little long at the end.

One critique on a common thread of the course: on Tuesday we had a lot of discussion time, and the professors keep saying that these discussions are great, however I personally am getting very little out of these discussions. We had a long conversation about decentralized vs. centralized cyber decision making that ended up way off track from the pertinent information in the lecture. I understand that four or five students in the class have a deep knowledge of these topics, but their deep discussions are going way over my head and I do not think that these types of discussions are helpful for "All hands." I recommend that if we deviate from the lecture on these discussions then we should keep them at the "All hands" level, or center the discussions around an article that we can read so that we can all contribute to the discussion instead of the same four or five students.

J. JOURNAL TEN: SEPTEMBER 12, 2017

This week we discussed International Law and Military Cyber Operations. We went over the differences between the cyber domain with the traditional domain, and how cyber is man-made while the traditional domains are natural. We have talked a lot during this course about how cyber is a game changer, and how we need to shift our thinking on how to use cyber. Some key takeaways from this week were the paradox of when to use cyber operations. We discussed the stakes, stealth, and persistence, and the risks of using or not using a cyber capability. For example, if you have an attack vector that you know will take advantage of a known vulnerability in your adversary, if you use it then it is likely the only time you can use it because they will then move to defend against it. If you do not use it, then it is possible that your adversary will identify their vulnerability

and patch it, then your attack will no longer work and you may have wasted an opportunity for a guaranteed attack. The stakes need to be at an appropriate level in the international realm, otherwise there is no need for an attack. The decision to use offensive cyber operations, taking all of these factors into account, is incredibly complex. This echoes what we have discussed for so much of this course; the cyber realm is a very complicated, complex world, which completely redefines our world order and social norms. The international laws of armed conflicts are perhaps outdated, and not so easy to apply to cyber operations. Another theme for our course is the use of non-state actors in the cyber realm, which makes attribution such a nightmare.

In conclusion for the entire course, I feel like I have learned a lot about cybersecurity, and am much more aware and enlightened on what cyber operations entail. I certainly appreciate how complex it is, and feel humbled on what I do not know about cybersecurity and cyber capabilities. Seeing how vulnerable we are, both in our societies and in the DOD, I realize the importance of cybersecurity moving forward and the need for us to get ahead on this. I certainly have a lot of criticism and critiques about this course, but completely endorse the need for more cybersecurity education in our military. I have personally ramped up my own cybersecurity by changing my passwords and setting up text-codes and alerts for logging into my crucial accounts like my bank account. The “turn of mind” that I have gotten from this course could potentially have a huge impact in my career.

K. JOURNAL ELEVEN: SEPTEMBER 13, 2017

We were asked to do one more cyber journal for the last day of class on Tuesday, in which we discussed strategic cyber deterrence options and active cyber defense. The lecture on deterrence went over the need for capability or ability to act and respond, credibility and being willing to actually deploy your force, and communication or sending the right message in order to have effective deterrence (S. Jasper, class notes, September 12, 2017). Deterrence is very complicated and challenging in cyber space due to the many non-state actors involved, difficulty and timeliness of attribution, and the entanglement of states that may or may not encourage responsible behavior due to other

competing interests (S. Jasper, class notes, September 12, 2017). The argument was made that basically deterrence is not going to work in cyber space and has not worked in the past. This leads us to active cyber defense. Key elements of active cyber defense are real-time detection, analysis, and mitigation using automated artificial intelligence to act at the speed of cyber (S. Jasper, class notes, September 12, 2017). The idea is to limit damage inside your network by blocking, killing, or quarantining the malware, and also to go outside your network and employ countermeasures, which are basically counter attacks (S. Jasper, class notes, September 12, 2017). When legal, these countermeasures can be very effective, but the legalities are in question. Also we would not want artificial intelligence conducting counter attacks; there needs to be a human in the loop in order to prevent terrible decisions that may have massive undesirable political ramifications.

This course certainly raised my level of mindset on cyber and cybersecurity. I recognize the vulnerabilities we have in cyber space, both civilian and military, and was glad to be a part of this cyber pilot course. I expect this cyber mindset to serve me well on my future tours onboard a ship.

APPENDIX C. WALLS COURSE JOURNALS

A. JOURNAL ONE: JULY 11, 2017

To perform a proper reflection on the lecture and associated PowerPoint presentation presented by Dr. John McEachen, I have to admit that my knowledge about the background of cyber and its related issues are negligible. My primary curriculum within GSBPP pertains strictly to financial management; however, I am intrigued by how much cyber and energy (my other academic focus) share similarities. Both of these fields have become increasingly vital to national security as more state, and non-state actors strive to manipulate each of them as a resource to further their agendas on the local and international stage. As discussed during Dr. McEachen's lecture, cyber has not long been considered a strategically vital interest. However, continuing technological integration with legacy systems can be a vulnerability or threat that will require an increased cyber institutionalization throughout society as a whole and especially DOD.

To understand cyber and associated suffixes, the five W's laid the groundwork that got me to thinking about where we are today. Before the 1980s, the factors behind the rise in cyber operations came from the lack of standardization, which had been anything but consistent. This situation was possibly perpetuated within DOD due to antiquated systems and the slow acquisition process, which is plagued, by congressional red-tape and COTS requirements. Additionally, many commercial industries did not see themselves as targets. By understanding the simple mechanics behind a processor that functions as a computer, a network and even the equipment or systems connected to it can be instructed to perform unauthorized actions.

As a result of the Internet, today's commercial market can bring products and services to everyday consumers that were initially unobtainable. Many systems are built from commercially available hardware and software that is accessible around the world. This avenue creates a more significant opportunity for cyber to disrupt and sabotage anything that has the computing power and an interface. When Dr. McEachen disagreed with the saying, "security through obscurity," basically he was validating the fact that we

can no longer successfully combat today's cyber issue by avoiding to bring widespread attention to it. Cyber is in almost everything that makes life simpler or allows us to connect and share information with one another.

Based on reactive initiatives used in the past, which were ineffective, we need to change how we combat the challenges faced in the cyber domain. By understanding, the limitations and authority provided in U.S. Codes such as Title 6, 10, 18, and 50 we can adequately pursue threats without violating laws established to maintain individual rights. Despite the numerous cyber events, which have led to continued disruption, we are on a promising path to eliminating future attacks on national security with the campaign like JTF-ARES, which proves we are on a strategic offensive.

B. JOURNAL TWO: JULY 18, 2017

In the following, I will reflect on the lecture and lab coordinated by Assoc. Professor. John Roth. In summary, the objectives of the lecture provided a thorough breakdown for those not familiar with Internet protocols and cyber networking. Looking back, I was completely unaware of just how fragile and spontaneous the Internet happens to be. The CyberCIEGE wargame session provided a somewhat navigable exposure to network mechanics and support. However, I feel as if I gained only a small amount of personal knowledge based the amount of time exhausted. Obviously, we will spend more time on CyberCIEGE during future lab sessions where I hope to grasp the bigger picture since my initial opinion reflects a non-technical support perspective.

Before discussing the formal definitions of cyberspace, my explanation would have been partly wrong. My interpretation would have centered on just the events occurring over the Internet and not included the aspects of the electromagnetic spectrum. Understandably, it would be hard to draw a map of cyberspace. Much of the intricate details of cyberspace are yet to be discovered and share more than a couple of similarities with other resources in the world. For instance, the oceans of the world and cyberspace are far from being wholly mapped and continue to grow in size and complexity. As demands on cyberspace increase across its physical, logical and cyber persona layers, so will its vulnerability to future threats unless appropriate measures are taken. The physical

layer is what we operate through and controlled by various protocols, which direct how things will operate over the Internet.

The Internet architecture is complicated and developed on a fragile initial design however, it continues to grow. Increases in technological advances are restricted to protocols, which have led to things like Wi-Fi and the ability to transfer more data over the air. Consequently, these protocols are not confidential and are vulnerable to disruption and manipulation.

Additionally, functional layers however, I think it would have been easier to follow by building and discussing the layers separately illustrate the Internet architecture. The layers are distinctly different but have coordinated actions. The application layer initiates the request by which a function will be completed. Then the transport layer dictates the logical connection or path for the packet. The network or Internet layer determines the most optimal route to use to get to the ultimate goal. The data-link layer, which is referred to as a single-hop handoff, coordinates how the data gets to the next point in the delivery.

Unfortunately, there was not much detail on the objective of cloud computing and how the provisioning of virtualized resources forms the basis of cloud computing. I feel that it would have been worthwhile to spend more time on cloud computing since more data is being stored in a virtual cloud.

C. JOURNAL THREE: JULY 25, 2017

My paper will reflect on the lecture provided by Professor. Gurminder Singh. The videos and real-life stories used to meet the objectives of the lecture provided the most comprehensive and enlightening material presented as of yet. Following the lecture, I felt that I could speak intelligently about IOT as well as some of the negative aspects surrounding it. IOT is more than a single technology but a collection of independently developed but technologically advanced devices that share a common link such as the Internet. The examples used by Dr. Singh illustrating the IOT applications such as the digital lock was clear and provided the clarity. In my opinion, this lecture is essential for any introductory cyber course.

Based on the information from the lecture, current predictions indicate that by the year 2020, there will be five Internet connections for every person in the world. In my opinion, this increases the opportunity for a cyber-event where enforcement will require special authority and endless resources.

Multiple tradeoffs take place over the Internet because of the associated data collection and dissemination of it to decision-makers and consumers. In some cases, technology has removed human decision making from the equation. As additional (IOT) gateways become active, more capacity will be required to store this data, which is inevitable. There is a reduction in controlling risk. In most cases, the risk tradeoff can be consumer privacy and protection of that information as it becomes the responsibility of the Amazon and Google companies of the world who manage the data clouds. The concept behind cloud computing is ingenious because convenience for things such as security and dedicated storage/ server offers flexibility.

Positive Takeaways:

a) Historical Analysis of Gartner Hype Cycle for Emerging Technologies – provided a platform for what is possible based on market hype to mainstream adoption.

b) Dimensions of Computing

i. Pervasive/Ubiquitous/Ambient Intelligence/ Automatic

a. This will grow in importance as more regulation is passed. (e.g., forms of computing might be allowed in one area but not in others.)

c) LAB: After spending the last year at NPS, I misunderstood the premise behind the RoboDojo emails and now regret that I did not look into them more. It was an eye-opening experience to learn about how the IOT has enhanced this hobbyist trade into the realm of possibilities it offers today. Through the simple integration of creativity and just a few commercially available components, a single item can perform multiple functions while simultaneously being operated from a few feet or several miles away. Following the tour, the IOT prediction of having over 50 billion items providing a gateway to the world via the Internet as a whole is more evident than some imagine. Notably, I also

understand that many of these future products will serve multiple roles that today I have no way of knowing or preventing.

D. JOURNAL FOUR: JULY 27, 2017

My paper will reflect on the lectures provided by Assistant Professors John Roth and Marcus Stefanou. Based on the objectives identified in the cyber surveillance lecture, the format was easy to follow and allowed me to grasp the objective/takeaways. The topic of cyber surveillance appears to be vague for a few reasons. One reason stems from the right of privacy. Any respective cyber oversight from the government seems to threaten privacy because the public does not benefit from it. Over the last several years, the Internet has closed the connection gap between people and businesses however simultaneously the unintentional connection between personal and public information has increased. The general interaction over the Internet has manifested into an ever-growing number of open data exchanges which is driven and collected by external parties such as Amazon who wish to manipulate for future sales. Law enforcement uses cyber resources in order to grow its portfolio for investigation, which can be easily seen as a violation without proper authorization. Naturally, malicious examples of surveillance are varying.

The big data lecture appeared to be very broad based on the class inputs identified as objectives. Honestly, the lecture became too broad for my practical understanding as well as how it relates to cyber. If this lecture could have been limited in scope, then there might have been more to gain from big data. I would have like to know how to determine what data is worth keeping and purging from the storage banks. Additionally, I would have been interested to see if there are any studies on “big data” storage, which addresses the risks and opportunities of the single user since the security of the data is in the hands of a third party as opposed to the confines of the user’s hard-drive.

Positive Takeaways:

a) Unique identifiers are embedded in cookies and things like social media, which makes the general public more vulnerable to being surveyed in unauthorized manners. Additionally, it was interesting to learn how much information is collected from various websites.

b) It is concerning how much regulation for domestic surveillance is shut down despite the massive compilation of data that is commercially collected from unknowing consumers.

c) NO Lab was offered; however, I think that the timing worked well to allow an opportunity to prepare for upcoming midterms and recalibrate priorities after completing first 4-weeks of the quarter.

Possible Changes:

d) Cyber surveillance class - Legislation was covered in a Dr. McEachen lecture. However, it might be good to consolidate these regulations to possibly one single or half class session.

e) Big data lecture part 1 – It was insightful to ask participants about what they wanted to get out of the class; however, I think it ate a lot of the time which could have been used to define the concept of "big data" better. More operational research centered than on applicable cyber manipulation or vulnerability of big data.

E. JOURNAL FIVE: AUGUST 4, 2017

My paper will reflect on the lectures provided by Professors Marcus Stefanou and Scott Jarvis. Based on the objectives identified in the machine learning and data analytics lecture, the opening analogy was relevant in today's operating environment. Instead of the strategic requirements of metal or oil that secure prosperity for growing nations, we now face the additional challenge of mining for information in a data-driven society. This lecture had quite a bit of significant information, however, came across as a bit rushed. Unfortunately, I believe the need to expose the class to as much information as possible became overload for those who lacked the fundamental understanding of data science. Therefore, I was not able to grasp many of the objective/takeaways. What I wanted to take away from the data science lecture was how it could help me to make better or quickly informed cyber decisions and the available resources for getting the right information. The thing that I have noticed from military data collection is that it works

for establishing predictive trends, but most of our data is not real time, which makes it usually too slow to achieve a prescriptive outcome.

My knowledge in cyber was recalibrated during the Professor Jasper's lecture on cyber-attacks. It provided a midpoint to bring the class back into perspective. The lecture addressed topics that applied to a broad audience of different levels of knowledge. The availability of resources to commit cyber-attacks was surprising based on the potential to cause market failures within the global market. Based on this lecture, there is a dual hat of leadership across Cyber Command/ NSA/CSS who serves as the executive bodies on cybercrimes. There is vagueness worth exploring. How are cyber resources employed and whose instruction supersedes various cyber policy efforts if crimes or attacks affect both civilian and military operations? Both rely heavily on the commercial market.

Takeaways: Data Analytics

a) Application of data analytics used across law enforcement termed "predictive policing" was impressive. This technique of data mining led me to evaluate the predictability of human nature, which should be rational. Additionally, I imagined how this extrapolation of data could be used to forecast events that are more sensitive topics. The most important part of the data analytics process is the confidence of the data. Reliable, real-time data is mission essential.

b) I would have liked to participate in the planned class exercise; however, we ran out of time. This possibly could have served as an alternative lab for the following Friday session.

c) Appreciated the opportunity to reflect on previous class questions to tie things up.

Possible Changes:

a) Lab on port scanning was hard to follow. The lab served more as a refresher to reinforce previous learning. A better use of the time could have gone to linking the lectures from earlier in the week where applicable.

F. JOURNAL SIX: AUGUST 11, 2017

My paper reflects on the lecture provided by Assistant Professors David Canright and Kristen Tsolis. Based on the objectives identified in the cyber lecture on attribution, anonymity, authentication, and encryption, the format provided details on how the flow of information is controlled. The lecture applied to the course and I wanted to learn about how cryptologic tools are used in the cyber realm. The background analysis used to discuss the topic allowed me to grasp the objective/takeaways. The various types of securing data are complex because as we have increased computing power things have become harder to crack.

Positive Takeaways:

1) Hash functionality as a cryptologic tool provides secure access to some systems while others simply store the user's password which creates vulnerabilities. Basically serves as a fingerprint for user identification. Honestly, the common user would not be knowledgeable to know how each site stores their password. This information is not publicized to my knowledge which is possibly due to the implications on sales and the costs it would create for companies that do not.

2) Password Managers to alleviate the burdensome process of resetting accounts. Many of the stolen passwords originate from the physical weakness of passwords or method of storage employed by the user where allowed. Consequently, the platforms that would be used to store this information should be federally regulated to ensure compliance of updated security and software patches. I am not sure how, if any, of these checks are conducted on a federally level.

3) Encryption came about in the 9th century. The idea that the use of the German Enigma machine cipher was thought to be unbreakable was broken. Many do not imagine that an application on a computer as a threat and is actually running continuously to capture their password.

4) Anonymity or privacy mode removes Internet history from device however the Internet keeps a log of the activity. This is not removable. The use of third-party anonymizer services or TOR software.

5) LAB: Encryption lesson illustrated the complexity of the public and private key process however, I did not feel that it was necessary to understand the math. I was particularly satisfied with the fact that it is merely math running in the background. This proved to me that based on the level of complexity in password or encryption that computers can be programmed to crack some of the most basic encryptions.

Possible Changes:

1) Foot-printing lab did not allow much time to execute the actual lesson. Unfortunately, the instructor only stuck around for a short period. I left with the impression that it was not important.

G. JOURNAL SEVEN: AUGUST 18, 2017

My paper reflects on the lecture provided by Professors J Fulp and Rudy Darken. The cyber lecture on system and network monitoring provided some fundamental details on cyber = automation. This topic was relevant and lectured with a general audience in mind. Additionally, I found the objective not to be too complicated or too broad. The various types of monitoring information along with models of detection were fascinating.

Objectives/ Positive Takeaways:

The three main components of cyber monitoring were identified as being storage, transmission, and processing. Consequently, storage was identified as the one of least interest. Through previous lectures, I believe that stored data will play a much greater role in the future. Future decision-making will depend on readily available data that will come from some stored mechanisms. Interestingly, the U.S. Navy has started to move in the direction of a smart grid, which also stores data. Using tools like tripwire to monitor/ review the hash of data used to manage these smart grids do not offer any offensive capability to prevent or eradicate the idea of long-term or dormant threats before causing damage. I believe information at rest should be of greater interest in specifically larger

applications. Arguably, I understand that we cannot monitor ALL information (PUFNTAL-R), but there is still a lot of risk in cyber. My basic understanding of cyber monitoring has been improved by this lecture and personally appreciated the wrap-up Q&A + blanks that required fill-in!

The lecture on human factors based on the concepts of security and usability met its objectives however, I wished that we could have spent more time on OBJ 6. This objective focused on identifying social engineering and interface design countermeasures that decrease security risks (i.e., phishing). This topic would serve as an opportunity to train and cross-train fellow service members. I learned that there is a tradeoff because rational humans like many things in nature will travel the path of least resistance. To change the current trend new things will have to offer an incentive compared to over previous efforts. Today's environment is inherently more vulnerable than in the past; therefore, we must make it convenient yet secure.

Possible Changes:

1) Many members have experienced some form of a socially engineered scheme personally or through a close acquaintance. Is it possible to share some of these real-life scenarios to learn from a classmate's experience collectively?

2) Fewer human factor slides consisting of basic design – aesthetics and minimization.

H. JOURNAL EIGHT: AUGUST 25, 2017

My paper reflects on the lecture provided by Professors Ray Jones and Doug Brinkley. The cyber lectures on acquisition of security products/services offered some basic details on products procured for military use. This topic was relevant and lectured with a business focus audience in mind. Additionally, I found the objective not to be too complicated or too broad. The various types and efforts of acquisitions discussed warranted further identification based on some growing vulnerabilities.

The objective expressed in the acquisition lecture (Jones) to educate the class on complexity of the Defense Acquisition decision support system only skimmed the

surface. The details used to describe the acquisition process of security products and services did not appear to pull out some of the significant cyber implications that currently exist. One possible alternative to the lecture would include discussing how or what cyber requirements are integrated into acquisition programs. Despite the idea of the net ready key performance parameters (KPPs), there doesn't appear to be a metric to track the status of meeting cyber KPPs. In my opinion, the concept of cyber KPPs is good however the bottom line is to become more cyber-ready. The security parameters have not been established for many items whether militarily sourced or commercially available. Is there an entity that tests military equipment for cyber vulnerabilities? Moreover, if so, how is this process handled? These are some questions that strike a bit of interest.

In my opinion, the significance of cybersecurity within the contracting field is an after-thought based on procurement criteria. In the midst of updating legacy systems, I am sure that DOD is more vulnerable than ever before due to antiquated systems, which are used to support day-to-day operations. The discussion of risk analysis and contingency planning for readiness provided by Dr. Brinkley applied to the current DOD environment. Interestingly, this lectured provided a link between the human factor lecture surrounding the aspects of security and usability. The legacy supply systems used today are being combined with modern technology that creates legitimate issues.

The Friday lab centered around cybersecurity incidents along with a detailed breakdown on the dimensions of the web. The amount of data accessed from the surface vs. the other dimensions of the Internet provided a valuable aspect of the lecture. This lecture/lab complemented previous lectures and solidified the real-life impacts. As addressed, the big one [strategic cyber-attack] has yet to happen however we have a lot of work to do in the supply chain. It is what I would consider as the weakest link.

Exploitation of data can be executed in various ways, Dr. Aquino brought up a great topic on mapping. Our adversaries get to map our defenses and operating framework without ever being seen as a threat.

The military relevancy hit the mark, but I think that the acquisition lecture could be applied better to cyber topic.

I. JOURNAL NINE: SEPTEMBER 1, 2017

My paper reflects on the lectures provided by Professor Scott Jasper and Mr. Bob Goodwin. The cyber lectures addressed the topics of risk management, defense in depth, and cyber threat intelligence. In my opinion, these lectures took an administrative approach to how leaders and management build strategies to reduce and eliminate cyber threats but not necessarily the risk. This topic was relevant and lectured with general audience in mind. Notably, I believe the lack of clearly defined objectives resulted in my confusion at times since we as military officers are trained to eliminate risk, first. Next, I will discuss some of the takeaways that had the greatest impact in shaping my current perspective.

The objective that I took away from the risk management lecture centered on the aspects of risk management. Risk management and the associated frameworks share a common link between mission impacts, which take place in and outside of conflict situations. This supports the claim that cyber is multi-domain. For military units to complete their overall mission, then risk has to be managed at each level for a successful "ends." Cyber is a part of the "means" by which we may be the victor. To quote Professor Brinkley, "we can only expect what we inspect," which is why I feel that we have not fully embraced the concept of risk management in cyber. Possibly, some of the problem stems from the less than basic knowledge about cyber that many users demonstrate. Other factors include the potential of reducing the number of technological advances or capabilities due to cyber implications. Arguably, we - DOD, continue to accept cyber risk because new capabilities funneled through the acquisition system sharpen our offensive interests. Meanwhile, our adversary may use this predictable behavior to their advantage by putting weight on defensive measures like cyber defense.

The lecture on defense in depth cleared some ambiguity surrounding the topic. The idea that more than one defense layer is eye opening. The industry sector is investing

in projects to protect vital information. During the briefing, I was surprised to learn about how many companies felt confident in their systems yet continue to be hacked.

The Friday lab provided a tour of the ITACS Data Center along with the Security Operations Center to gain exposure to the number of processes and technology in place to detect, prevent and respond to network intrusions at NPS. Despite the overview, I could not talk in detail about the threats and challenges that members of the SOC team face, however, I realize that trends are used as a measure of cyber-risk analysis. I would have liked to learn more about the barracuda and other local applications that help to keep the email system safe. Overall, this experience supported the topics covered in during the week and served as a visual aid to other lectures covered earlier in the course.

J. JOURNAL TEN: SEPTEMBER 8, 2017

My paper will reflect on the lectures provided by Associate Professor Bradley Strawser and Dr. McEachen. Based on the objectives identified in the International law, ethics, standards lecture, the opening examples to discuss the Just War theory were relevant in today's operating environment. Notably, the lecture stepped away from the technical side of the course and applied a very critical yet ethical thinking aspect to cyber that military leaders will face. The justification for going to war and tactics used in war pose a challenging dilemma in cyberspace. In my opinion, my comprehension of international law and ethics in the domain of cyber were enhanced as it relates to those efforts that serve to create social operating norms within cyberspace as well as cyber being used a form of warfare.

The lecture provided by Dr. McEachen on military cyber operations was hard to follow. The offensive aspect of cyber was discussed but appeared to state the obvious questions, which are conclusive with the topic. Unfortunately, I did not find the lecture informative or able to meet the objective of understanding of how military applications of cyber effects (MACE) can be used in supported and supporting roles to achieve mission objectives. Not sure if the coauthor of the slide deck should have been a co-presenter since Dr. McEachen appeared not to be familiar with some of the material on the slides.

Notably, there was a distinction between this cyber lesson and others observed at the current stage of the class.

Cyberspace could benefit from more internal controls on an international basis due to the evolving frameworks being employed by independent and state-sponsored economic disruptions and criminal operations.

Takeaways: International Law and Ethics lecture and Russo- Georgian Analysis

a) Benefited from open dialogue with Dr. Strawser's topic of interest. Lecture style was one of the better due to its framework. "Single briefing document that collected and focused the group's interest in the topic of Jus ad bellum and Jus in Bellum."

b) Lab on the RUSSO-GEORGIAN WAR served as unique story, which promoted some interesting dialogue. Great lesson on the history of how the virtual aspect of cyber has physical consequences at the nation-state level. (DDOS, etc.)

c) My concern lies in the ability of our modern defenses to operate in a protracted cyber campaign.

Possible Changes:

a) Honestly, I believe that lecture provided by Dr. Strawser could have been a two-part session to dive further into the implications of a practically lawless cyber domain. We have witnessed multiple scenarios where criminals go unpunished due to the gray "deniability" area or limitation of regulating the international cyber-domain. When compared to the sea there are some similarities between cyber however, criminals are likely to get away with malice in cyber than escaping the law of the sea where international justice is upheld.

K. JOURNAL ELEVEN: SEPTEMBER 12, 2017

My paper will reflect on the final lectures provided by Scott Jasper. The objectives identified in the strategic cyber deterrence options lecture shared some of the concepts learned in the Theater Security Decision Making course offered through the NWC. Despite the lecture's emphasis on cyber, the relationship between politics, policy,

and strategy have military significance. As described in the lecture, the basis of deterrence involves the three C's (credibility/ capability/ communication) however, creditability in cyberspace has a paradoxical meaning unless the actors are willing to take accountability for their action(s) by identifying themselves. Also, the sovereign territory of some malicious actors protects them from international indictment and prosecution. International politics complicate cyber oversight by entangling the latest form of deterrence against attacks. The mutual interest of the majority creates decreased optimality in cyber deterrence because the goal(s) of the malicious actor will target/ exploit these arrangements.

The second lecture on active cyber defense discussed the aspect of breach detection, which illustrated the fact that many companies have not entirely closed the gap between detection and what has been comprised because of cyber threats. Within the private business realm, retaliation does not have an offensive limitation like the DOD where aggressive response requires permissions to employ countermeasures. Following the Equifax breach, the malicious actors, whether foreign or domestic, have been able to demonstrate that our defensive cyberinfrastructure is weak.

Takeaways:

a) Based on the lack of measurement or effectiveness of cyber deterrence, I would not be able to ascertain if our cyber deterrence strategy is winning. It appears that our adversaries are much more advanced from a defensive/ offensive standpoint because of the legal framework that has restricted the avenues on deterrence.

b) Hackers and the malicious intrusion tools used are breaching systems faster and faster; however, the intended outcome is not necessarily immediate.

c) How do we get away from data at rest if cybersecurity is not fully obtainable?

Possible Changes:

a) The lecture of cyber deterrence sets the stage as to "why" we need this type of strategic option. The timing of this lecture appeared to be out of sync based on previously covered topics.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Brown, C., Crabbe, F., Doerr, R., Greenlaw, R., Hoffmeister, C., Monroe, J... Standard, S. (2012). Anatomy, dissection, and mechanics of an introductory cyber-security course's curriculum at the United States naval academy. *Proceedings of the 17th ACM Annual Conference on Innovation and Technology in Computer Science Education.* ACM. 2325, 296–367. doi: 10.1145

Bumiller, E., & Shanker, T. (2012, October 11). Panetta warns of dire threat of cyberattack on U.S. *The New York Times.* Retrieved from http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Clapper, J., Lettre, M., & Rogers, M. S. (2017). Foreign cyber threats to the United States. *Hampton Roads International Security Quarterly, 1.* Retrieved from http://libproxy.nps.edu/login?url=https://search.proquest.com/docview/1865125438?accountid=12702

Commission on Enhancing National Cybersecurity. (2016, December 1). *Report on securing and growing the digital economy.* Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf

Department of Defense. (2012). *Sustaining U.S. global leadership: Priorities for 21st century defense*. Washington, DC: Author. Retrieved from http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf

Department of Homeland Security. (2017a). *About NICCS.* Washington, DC: Author. Retrieved from https://niccs.us-cert.gov/about-niccs

Department of Homeland Security. (2017b). *National centers of academic excellence (CAE).* Washington, DC: Author. Retrieved from https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae

Department of the Navy. (2016). *Vice chief of naval operations.* Washington, DC: Author. Retrieved from http://www.navy.mil/navydata/bios/navybio.asp?bioID=483

Harvard Extension School. (2017a). Cybersecurity certificate courses. Retrieved from https://www.extension.harvard.edu/academics/courses/courses-by-certificate/Cybersecurity%20Certificate

Harvard Extension School. (2017b). Cybersecurity: managing risk in the information age. Retrieved from https://gs.harvardx.harvard.edu/harvard-cybersecurity-online-short-course-hm/?utm_source=PPC&utm_medium=adwords_ppc&utm_campaign=HAR_CYB_aw_usa_br&AdID=217859486637&CID=909428304&AgID=53840386068&KW=%2Bharvard%20%2Bcyber%20%2Bsecurity&gclid=CNf3td6jxtYCFcNlfgodLqAE3Q

Jones, D. (2017, January 23). Cybersecurity training is worth repeating. *The University News*. Retrieved from https://www.ucdavis.edu/news/cybersecurity-training-worth-repeating/

Morgan, S. (2016, May 9). Top 2016 cybersecurity reports out from AT&T, Cisco, Dell, Google, IBM, McAfee, Symantec and Verizon. *Forbes.* Retrieved from https://www.forbes.com/sites/stevemorgan/2016/05/09/top-2016-cybersecurity-reports-out-from-att-cisco-dell-google-ibm-mcafee-symantec-and-verizon/#1ce01a1d1caf

Newsweek Educational Insight. (n.d.). The cybersecurity threat – fighting back. Retrieved November 2, 2017 from http://www.newsweek.com/insights/leading-cybersecurity-programs-2017

Obama, B. (2016, December 2). *Statement by the President on the report of the commission on enhancing national cybersecurity.* Washington, DC: The White House, Office of the Press Secretary. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity

Ponemon Institute. (2017). *2017 Cost of data breach study*. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Reveron, D., & Mahoney-Norris, K. (2011). *Human security in a borderless world*. Boulder, CO: Westview Press.

Sciutto, J. (2015, July 10). OPM government data breach impacted 21.5 million. Retrieved from http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html

Williams, B. (2014, March 13). Cyberspace: what is it, where is it and who cares? Retrieved from http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/

Zepf, A. L. (2013). *Cyber-security curricula for basic users* (Master's thesis). Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/37750/13Sep_Zepf_Art.pdf?sequence=1

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California