**Analyzing the United States Naval Academy Cyber Operations Major In Relation to the National Initiative for Cybersecurity Education**

Joey Cavalli, Ryker Knight, Shane Popko, Riley Smith

United States Naval Academy

**Abstract**

Currently the United States Naval Academy has an accredited Cyber Operations Major, but has not explicitly mapped its majors objectives to industry/global needs. The goal of our capstone is to utilize the NICE framework as a foundation of cyber practice, and then correlate the knowledge, skills, and abilities needed to work in the cyber field to the classes that Cyber Operations Majors take. By comparing course objectives to this framework we can determine to what extent the Cyber Operations Major prepares students to exit the Naval Academy as competent cyber professionals.

**Introduction**

Potentially one of the most impactful advancements of humans in the late 20th century was the development and implementation of the internet, along with the increasing use of computerized devices for both personal and military use. This trend has continued to increase to today where most of the modern world is dependent upon computers and programs to carry out tasks ranging from keeping a room at seventy degrees to allowing for global trades in an instant on the New York Stock Exchange. Because so much of our modern world and infrastructure is now dependent upon these systems, it is critical that modern nations have robust ways to defend themselves from other countries, while at the same time they must develop the capabilities to go on the offensive should the need arise. At the United States Naval Academy, the Cyber Operations major’s purpose is to educate and train Midshipmen to become more knowledgeable in this new warfare domain. This major is more necessary now than ever as American military planners continue to see the cyber domain as a fundamental area of conflict in a time when peer-on-peer tensions are rising[[1]](#footnote-0). A few case studies to underscore the importance of defensive and offensive capabilities would be the recent American response to the Solarwinds attack along with the importance of Stuxnet.

In regards to the need for defensive security, the Russian Solarwinds attack proved that with timely defensive measures and communication, even sophisticated attacks from capable nation-states could be mitigated. The Russians accessed the Solarwinds server and were able to insert malicious code into an update for their Orion software. This Orion software was then sent to numerous facilities both civilian and military including targets such as Microsoft and the Pentagon. While certain American companies caught wind of this attack early, it was not until FireEye[[2]](#footnote-1) noticed and verified that the cause of the attack had been tainted SolarWinds code that efforts could be taken to combat this threat. This incident underscores the importance and necessity that quality cyber defense has in deterring and protecting nation-state interests when it comes to the cyber realm. Similarly, the Stuxnet worm demonstrates how, with offensive cyber tools, nations can project power and protect strategic goals.

The Stuxnet worm, while not “officially” claimed by any nation, was a vital tool in derailing the Iranian nuclear program much to the benefit of the US and Israel. While conventional military weapons could have taken out the facility, that would have made it obvious who the aggressor was and allowed for retaliation and possible escalation of conflict. Stuxnet was able to cause physical damage to the Iranian nuclear centrifuges and cause massive setbacks to their chances of developing nuclear weapons. The attack also allowed for plausible deniability in favor of the aggressors showing the power of cyber attacks and the damage they could cause.

In both instances, SolarWinds and Stuxnet demonstrated how important cyber knowledge is for both the protection of critical infrastructure and how its use in offensive capabilities could lead to strategic and tactical wins for the countries involved. The Cyber Operations major is currently composed of 14 “core” or mandatory classes which in total have 82 course learning objectives. The main objective of our capstone is to compare these course objectives with a series of Knowledge, Skills, and Abilities (KSAs), which have been laid out by the National Initiative for Cybersecurity Education (NICE), to determine the overlap of the Cyber major’s course objectives to these KSAs. It is our belief that the current Cyber Operations major has the necessary classes and course learning objectives, which cover the majority of these KSAs, to demonstrate the validity of the major in regards to graduating officers competent in the cyber realm.

**History of the NICE Framework**

In starting this project we decided that looking into the NICE framework would be the most ideal way to view our major’s course learning objectives (CLOs). The groundwork for NICE was started in 2008 under President George W. Bush who created 12 national standards which were called the Comprehensive National Cybersecurity Initiative (CNCI). The broad goals of the CNCI were to ensure that the United States would not fall behind in the cyber realm and retain our edge in this new domain against other countries. Under the President Obama administration, the CNCI was continued with increased support in all areas, especially in order to “begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century”[[3]](#footnote-2). This stems from the 8th initiative whose goal was to specifically expand cyber education. Finally, under the Cybersecurity Enhancement Act of 2014, the NICE Institute was established. Under Title IV of the Cybersecurity Enhancement Act of 2014, the director was tasked with broad objectives such as ensuring cybersecurity technical standards and practices were disseminated among the populace, and that these practices could be understood by average people and small businesses. The idea was to ensure that all American people would be more familiar with cybersecurity due in part to our increasing reliance on its everyday use. All children are taught how to read and write in school because the English language is something they need to use everyday, and similarly, cybersecurity education needs to become more prevalent in the education system to develop a generation of more competent cyber individuals.

We chose the NICE framework because it currently is the nexus where government and education come together to agree on what skills are critical for the cyber user. At an institution like the United States Naval Academy, we too are at a crossroads of government backing along with higher education standards, and as such, it only made sense that this should be the foundation upon which we look at our own cyber-focused major. Since the creation of the Cyber Operations major in 2013, the program has developed rapidly gaining credibility through the years, as well as serving as a foundation for other cybersecurity programs to develop around the nation.

**Similar Institutions with Cyber Programs**

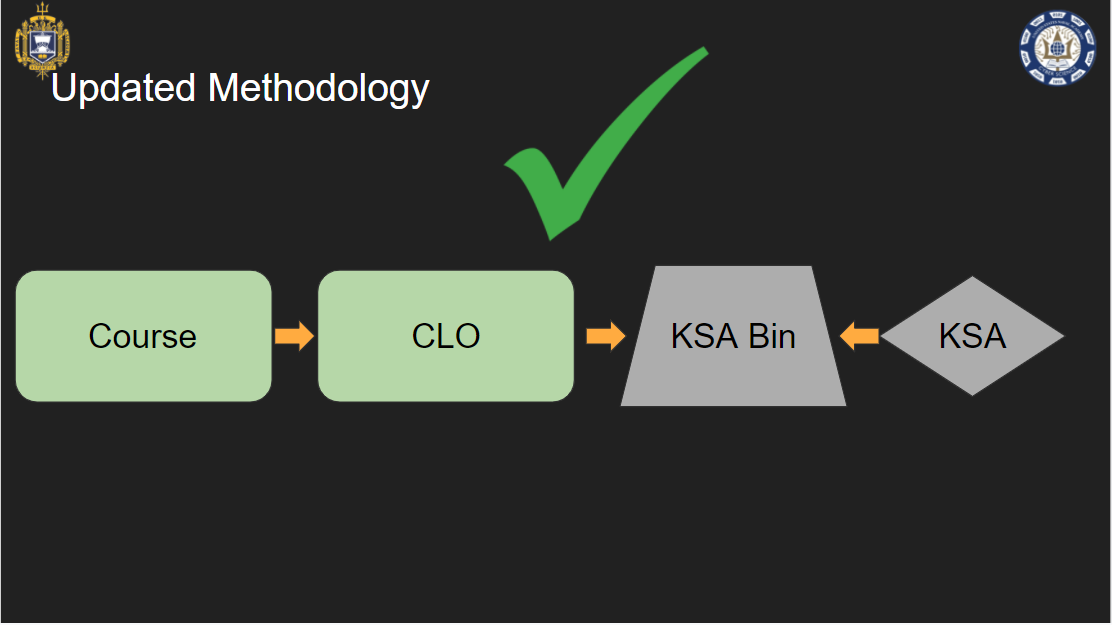
The Air Force Academy as of 2017 has been graduating officers with a Cyber Science major, however, their major is much more focused on the technical aspects of cyberspace, whereas at the Naval Academy we ensure that we supplement the technical side with policy and law.[[4]](#footnote-3) As an example of this, a Cyber Science major at the Air Force Academy will take Computer Science classes in their 2nd class year before taking their first Cyber Science class being Cyber Science 333: Cyber Warfare[[5]](#footnote-4). A student at the Naval Academy will not have the opportunity to take our comparable class, Cyber Operations I, until the first semester of their 1st class year. Similarly, Brigham Young University also has an undergraduate degree, titled Information Technology & Cybersecurity, which akin to the Air Force Academy, places a heavier emphasis on the technical side of the major. Currently, BYU’s main focuses lay in Digital Forensics, Penetration Testing, Internet of Things, and System & Network Administration[[6]](#footnote-5), but lacks the policy understanding that is present at the Naval Academy. As a leader in this field, as well as a government institution, it can only serve the greater benefit to ensure that the courses we teach and their objectives are in line with the current government and private ideals of what is critical to know in the cyber field.

We wanted to do this as our Capstone project because our group felt that through this endeavor we could further solidify our program as a “city on a hill” upon which other institutions could look as an example, or should we see that we have not met the majority of the NICE framework, then we could quickly course correct and identify where our deficiencies lie. We could then also see how to best address deficiencies in order to produce a more well-rounded cyber individual. One of the most attractive attributes of the Cyber Operations major is its holistic approach to the cyber realm where it ensures its graduates are prepared for the many aspects of cyberspace. There is no shortage of jobs for cyber professionals, however, in a survey done by PayScale, they stated that 87% of recent graduates felt that they had the technical skills to enter into the industry, however, 51% of those graduates faced unemployment[[7]](#footnote-6). The disparity between graduates feeling technically qualified for the job and lack of employment has been credited to a lack of skills such as communication, leadership, as well as a legal understanding of the problems at hand. To further add to this, there was a study done by the University of Idaho for their Agricultural Department, whose overarching thesis was the need to “produce graduates who possess the technical and professional knowledge needed by a changing society.”[[8]](#footnote-7) Though the study looked at graduates between the years 1973-1985, we believe its message of adaptability and versatility is more true in the present than people might have expected 30 years ago.

**Methods**

Our first step in this project was first finding a facility advisor who would be able to sponsor us and help advise us as to where we should begin in our project. At the onset of our Capstone, we were not aware that there was such a prevalence of government and industry backing into cyber security education. As such we initially planned to compile our own experiences from the courses and determine to what extent we had used and remembered them in our other major classes, as well as compare our course curriculum to other comparable institutions such as the Air Force Academy and BYU. However, the glaring issue with this course of action was that there was no metric by which to determine success or failure. Simply put, this would be too subjective to determine any real results or provide actionable information from which to derive anything. As such we reached out to our first capstone mentor LCDR Andrew Slack as to how we should proceed.

The advice we got from LCDR Slack was that we should look into something called the NICE Framework, and see if that aligned with our overall vision of looking into our major in a more meaningful way. During this time, LCDR Slack also mentioned that we were not the first people within the department to be looking into the relationship between the Cyber Operations major and the NICE Framework’s list of KSAs. He mentioned another professor, CDR Brien Croteau, and said we should speak with him as it was believed he was working on something very similar to what we were interested in. At this point, because our group still did not have a solid idea of how our capstone would work, we scheduled a meeting with CDR Croteau to see what his intentions were and to see if he could point us in the right direction.

Our initial meeting with CDR Croteau set the course for how we would start our project. In our first meeting, we started out by saying that our concept idea was that we would use the NICE KSAs and somehow relate them to courses to see if we could find a positive correlation between them and the Cyber Operations major’s courses. The first question he had was what metric we sought to look at classes by, to which we had no answer. He then suggested that we dive into the course learning outcomes of each class and work from there. The idea is that upon passing a class, a student would be able to leave with a full understanding of the basic objectives of that course. CDR Croteau informed us that through the past year he had been meeting with different facility members from the major to discuss their course’s learning outcomes. He desired to gain an understanding from the individual professors as to if the course learning outcomes lined up with the actual course curriculum, and their own thoughts on the subject. CDR Croteau, after hearing this pitch, informed us that he was working on something very similar and was actually looking for some help, and would be able to provide us with the groundwork he had already completed, specifically the notes recorded from his interviews. The help he specially sought was in turning the KSA list into something functional.

**Issues with NICE**

The glaring issue with looking at the KSAs that are provided by the NICE Framework is that they are not organized in a meaningful way. CDR Croteau shared with us a Microsoft Excel file titled “Reference Sheet for Workforce Framework for Cybersecurity (NICE Framework)”. This file breaks down into very nuanced tabs detailing some specific jobs such as Enterprise Architect, System Requirements Planner, Technical Support Specialist, etc. In each of these different job tabs, there might be anywhere from 10 to 30 different KSAs that NICE has determined are essential for that job. This information was not important to us because the Cyber Operations major does not graduate cyber specialists, instead, it goes for a more well-rounded approach and seeks to develop people well versed in overall cyber security. Because of this, we shifted to the master KSA list in the document where there were almost 1,200 individual KSAs that were identified as being critical to the cyber domain. An issue with this master list was that the KSAs were not ordered in any meaningful way aside from numerically going in order from the beginning to the end of the list.

CDR Croteau, while he had the same information we had in this list, needed a more practical application than simply a 1,200 item list, and as such was determining the best way to make all this data usable. His initial task for us was to determine potential solutions to accomplish this first goal so that we could seek to then compare them to the CLOs. Our goal was to sort this 1,200 list into “bins” based on their overall application, rather than their function tied to a specific occupation. Our thought process was that by creating bins of KSAs with related topics, we would be in a better position to compare these bins to the broader course learning outcomes. At this time, he mentioned that a good place to start would be to talk with Professor April Edwards, whose main field interest lies in machine learning to see if that might offer a way to sort through our list.

**Machine Learning**

Immediately following our initial meeting with CDR Croteau we then made it a priority to speak with Professor Edwards to see if machine learning really could help to sort and pair down our massive list. After speaking with her, she said that she would run our KSA list through a data parser whose purpose was to find the most commonly used words and phrases.

The issue we faced was that the KSA list is very much conceptual, and the issue with machine learning in its current form is that conceptual ideas are much more complex than matching images of apples to oranges. Machine learning can understand that if something is the color orange, then it is more likely to be an orange than an apple, but in comparing concepts such as metadata, forensics, cyber offense, and defense, it is much more difficult to differentiate. The result of running the KSAs through the algorithm was we got a list of the most common words and concepts from the overall list and how many times these words and concepts were repeated. For example, Information Technology was the most frequent result after the program was run and was found 17 times in our master list Other words such as Risk Management, Supply Chain, and Information Security were found between 4-8 times, and as such were identified as significant.

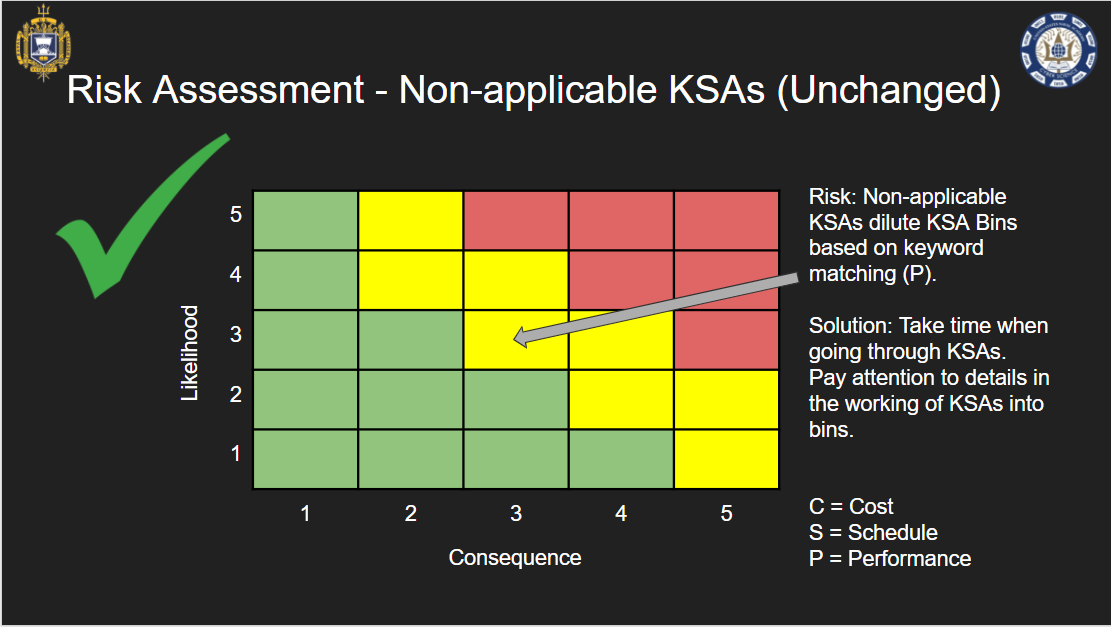
This list that we had generated, while helpful, was not the solution to our problem of how to sort the KSAs adequately. The result we ended up with was a list of around 250 “keywords”, or words that had been repeated more than once in the Master KSA list. However, out of these 250 items, only 17 were identified as appearing more than 3 times. This means that the other 93% of our data generated from the program was much less significant than we had initially anticipated. Even though Professor Edward’s program was not the final solution we had hoped it would be, it did provide a starting point to think of what the bins should be. In looking at the smaller categories, we were able to group some together into larger bins. For example, phrases such as “trigonometry linear”, “linear algebra”, and “calculus statistics”; and while these phrases were only repeated twice each, we realized that they would all fall under a larger umbrella of the bin “Cryptography”. We were able to group these together because we see that a student has to understand the underlying mathematical principles to fully understand cryptography. It was through this process of looking at similar repeated concepts that we were able to initially create our bins.

**The Bin System**

The reason we wanted a bin system was that we felt that these broad categories would be the best way to link cyber concepts to the CLOs. Many of the CLOs are very broad in their scope and act as guidelines for what a professor should be imparting to their students in that course. For example in SY110, our “Intro to Cyber” class, the first CLO is titled “Cyber Domain”, and its description is, “Explain why the Cyber Domain is important to the Navy, a Junior Officer, and an individual.” This learning objective is present because it is fundamental that a student in the Cyber Operations major understand why their major is important and how it affects all operations both in the military and civilian sectors. This CLO is also enormously broad and can have many different components under it for why the Cyber Domain is critical, it was for this reason that we wanted to create these broad bins filled with many similar KSAs. Currently, some of the bins that we associated with this CLO include Risk Management, Cyber Operations, Critical Infrastructure, and Cyber Laws, Ethics, and Regulations, to name some examples.

The bin creation process did not end with the results of the parsing program, as such, a large amount of manpower was still needed to be dedicated to going through the entire KSA list. Then, we needed to manually determine if specific results fit into our bins, or if new bins needed to be created in order to more specifically categorize certain items. It was this manual sorting process that ended up taking more time than expected to complete in our project. By the end, we had over 80 different bins that we had identified including a large miscellaneous bin for either overly specific items, or conversely, poorly worded KSAs.

**Risks with the Bin System**

To clarify, the master KSA list was not made by one person, rather it was a large collaborative effort to identify critical principles in the cyber domain. As people work together, they tend to disagree on what is most important or what needs to be included in such a broad project as describing all knowledge, skills, and abilities that are critical in cyberspace. Because of this, there tended to be a lot of unnecessary items in the overall list, as there has not been a significant effort to condense the original list since its inception. Our team in going through the master list, found KSAs that have either been redacted or more difficult for us to go through, were KSAs that were so broad or specific to one field as to be useless in our goal of creating generalized bins. For example, A0108 is “Ability to understand objectives and effects”, while A0148 was “Ability to serve as the primary liaison between the enterprise architect and the systems security engineer and coordinates with system owners, common control providers, and system security officers on the allocation of security controls as system-specific, hybrid, or common controls”. As seen A0108 is much too broad to fit into any one category, while conversely, A0148 is so specific that it is hard to identify the potential bin it would belong to. 

One of the initial risk concerns we identified early on in this project was that our miscellaneous bin would be overly large when compared to all of our other bins. This would indicate either that our group had done a poor job of identifying different bins and had failed to adequately sort through the KSAs, or that many of the KSAs in the list would not be similar enough to group well.

We initially sought to limit the scope of our miscellaneous bin to no more than 15% of the total KSAs which numbered at 1,188, meaning that we ideally wanted our miscellaneous bin to hold no more than 178 KSAs while the rest would be sorted into other bins. At the conclusion of our sorting, we are sitting at 21% of the total KSAs in the miscellaneous bin. While this is not exactly what we desired, our group feels confident in our sorting process, and thorough review of the miscellaneous bin, we believe that those discarded KSAs do not fit into any of the other 66 bins that we have created. The more critical component of our project was making sure that the bins we created would be substantial enough to provide use to professors and faculty when creating or reviewing the CLOs. We wanted to avoid having more bins of less substance for fear that it would dilute the impact of the bins as a whole. If we reduced the total number of objects in our miscellaneous bin to create more nuanced bins, we feared that the bins created would either be irrelevant to our courses or would be so small and specific as to provide no practical value to any course. Currently, there are an average of 14 different KSAs tied to each bin.

Now that the project is finished and our group has completed the full mapping of KSAs to bins, we feel satisfied with our completed work. Our initial aim in creating the bins was to make them specific enough that we could decide what KSAs were applicable to them, yet broad enough that they would help to break down the sheer volume of information. With 67 different and unique bins, we believe that we have successfully broken down the master KSA list into different cyber categories that provide a broad enough basis on which to now look at the CLOs present in our curriculum.

**Correlation of Bins to CLOs**

Our group has been able to associate the different bins successfully with the CLOs. On average we are seeing a correlation that each CLO will contain 8 different bins. On the low end, there are some CLOs such as in SY403, “Understand types and levels of cyber-power threats to national security and how U.S. uses of cyber power to achieve success in military and other operations”, that only have 4 different bins, while on the higher end SY310 has 41 bins tied to its statement, “Have a sound understanding of the technologies and methods utilized to defend systems and networks. Describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using appropriate technologies”.

Currently, through our linkage of bins to CLOs, we have managed to identify 65 of the 67 bins as correlating positively to a respective CLO. The only two bins that we have that are not linked are Supply Chain, and Enterprise Information. While there were enough independent KSAs that we felt these bins were adequately made, we failed to find a link between them and the current courses taught. Since the breaking of the SolarWinds hack, many teachers and students have discussed the concept of supply chains and how that attack occurred, however, there is no course objective or segment in any class whose sole purpose is devoted to describing the current state of the supply chain and how it relates to cyber security and operations. Similarly, Enterprise Information was also a category in which we found little association between it and the current CLOs. Still, with 97% of our bins linked to different CLOs, we feel confident that the Cyber Operations major as a whole is following the NICE guidelines and can be viewed as a model program both by the government and private sectors.

While we are pleased with our results, one thing we were not expecting was the frequency that some of our bins would be repeated when comparing them to course objectives. What this reveals is two items: one, the more a certain bin is repeated the more that class has an overarching focus on that topic, and two, the more a bin is repeated potentially it has been made too broad to be as effective as we wanted it to be.

To dive deeper into the first item, the focus of the classes, we noticed that certain elements such as Cyber Defense, Cyber Offense, and Risk Management were some of the most repeated bins in relation to our CLOs. While this was not a primary objective of our Capstone, the value gained is that our group has identified which concepts come out the most through the entirety of the major and allow at a quick glance an outside observer to see where the majors heaviest focus areas are. As the Cyber Operations major has a heavier emphasis on practical military applications, it is no wonder why these bins would see the most repeated use in connection to the CLOs because these areas in the military are more critical than Packet Analysis, or Diagnostic/Network Tools.

**Risks within our Comparison Process**

The second topic of note is the fact that we have so many of our bins relating to each CLO. A concern present in the work might be that there are too many bins (meaning there are too many correlated KSAs) for a facility or student to see how they connect back to the CLO. The CLOs must be broad because they give leeway to the teachers to develop their own styles of teaching and also allow them to change their approaches to best connect with the students. These learning outcomes are what the students should have an understanding of, the degree to which these CLOs are connected to direct testing and evaluation was beyond the scope of our project. With that being said, when we are looking to correlate these broad bins with broader CLOs, there is the possibility that we are putting too much information on the page for the viewer to easily navigate through the information. We want to provide as much information as possible that is directly relevant to the CLO, nevertheless, the broad nature allows for a higher degree of interpretation as to what actually belongs to each objective.

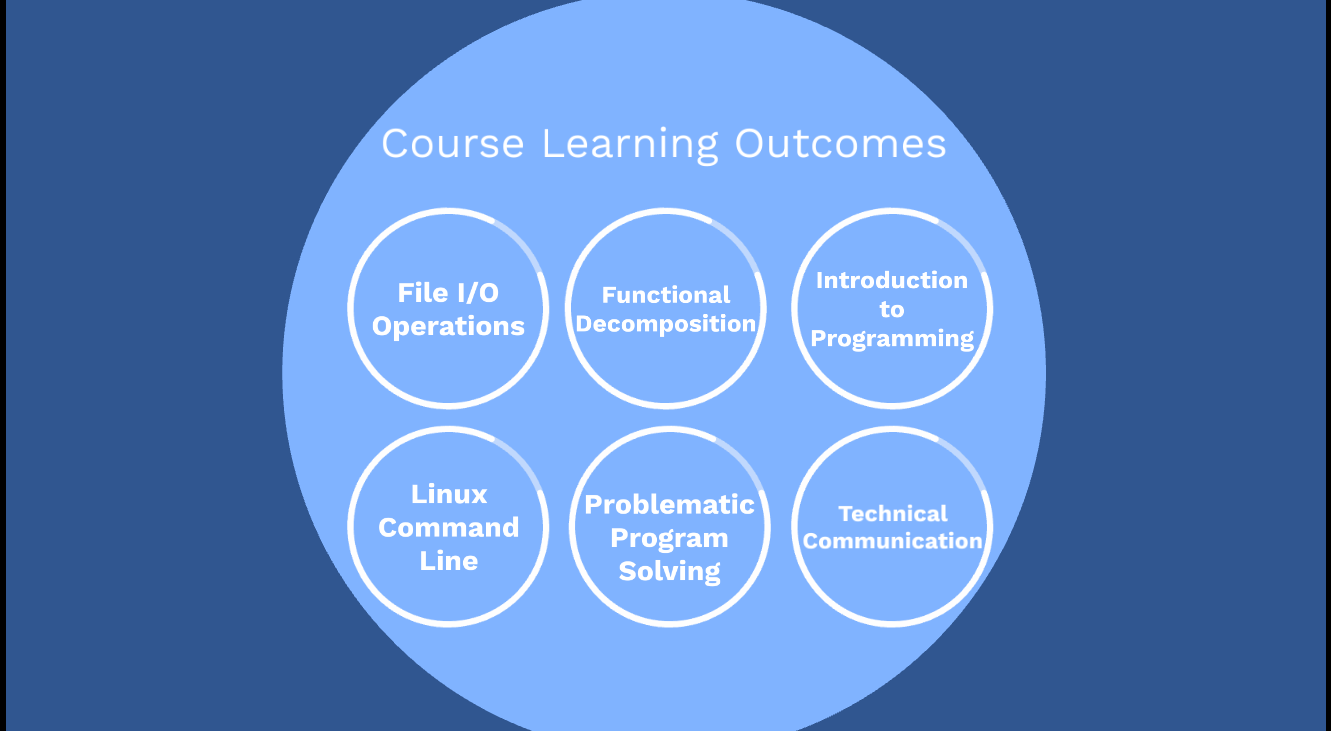
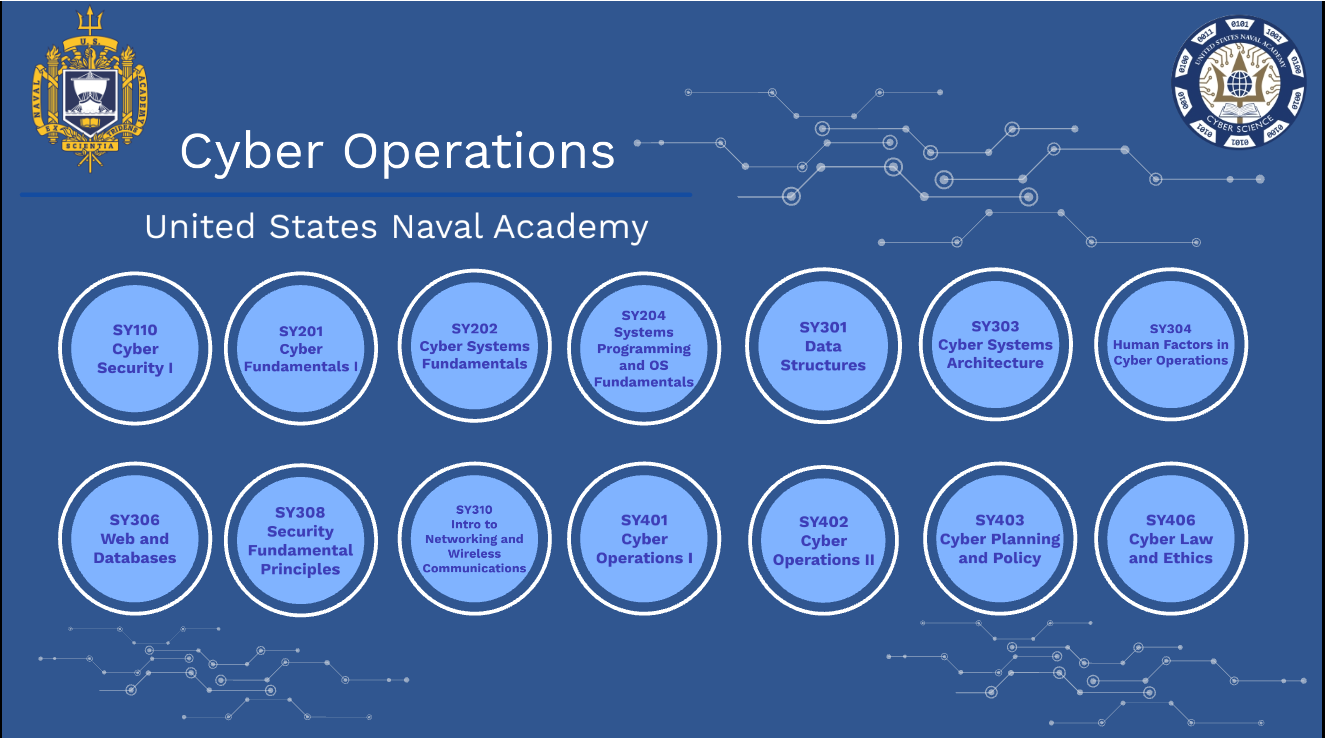
A potential solution to the above problem can be addressed by the Cyber Science Department by creating a specific list of testable items. What this means is that while a student should have an understanding of each CLO and what it entails, they should also know exactly what they are being tested and evaluated on. For example, the CLO from SY402: Cyber Operations II under Strategic Decision Making is, “Access, manipulate, and understand data to aid in effective strategic decision-making. Be able to detect possible threats, determine the risk associated with the threat, and understand what actions can be taken to mitigate the threat.” This CLO currently has 19 bins attached to it, which may make it hard to identify exactly which bins are more critical to this specific objective. If the department were to identify a few threats that would be covered in great detail for this course, then we would be able to condense our current bins to more closely align with what would be tested, rather than the broad overview. This would further narrow down the KSAs so that a user could more quickly identify exactly what the connection is between the NICE framework and what they are learning.

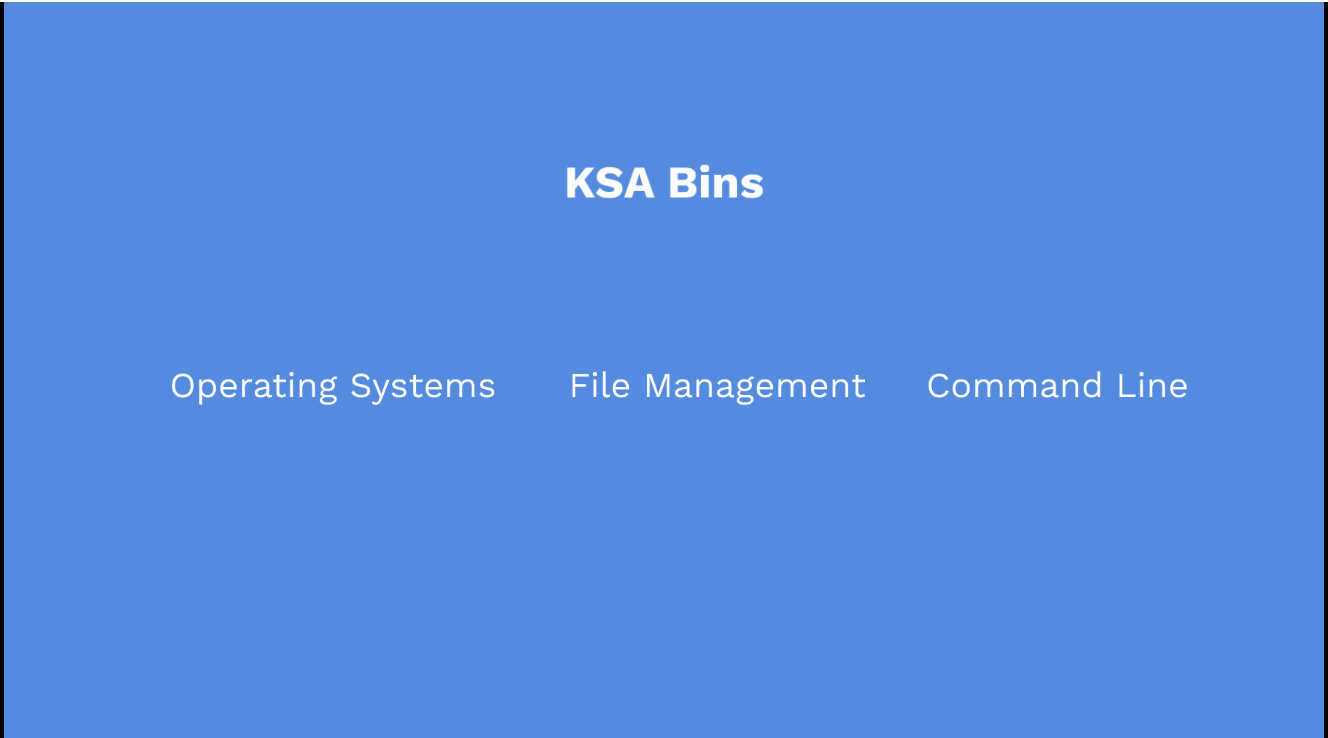
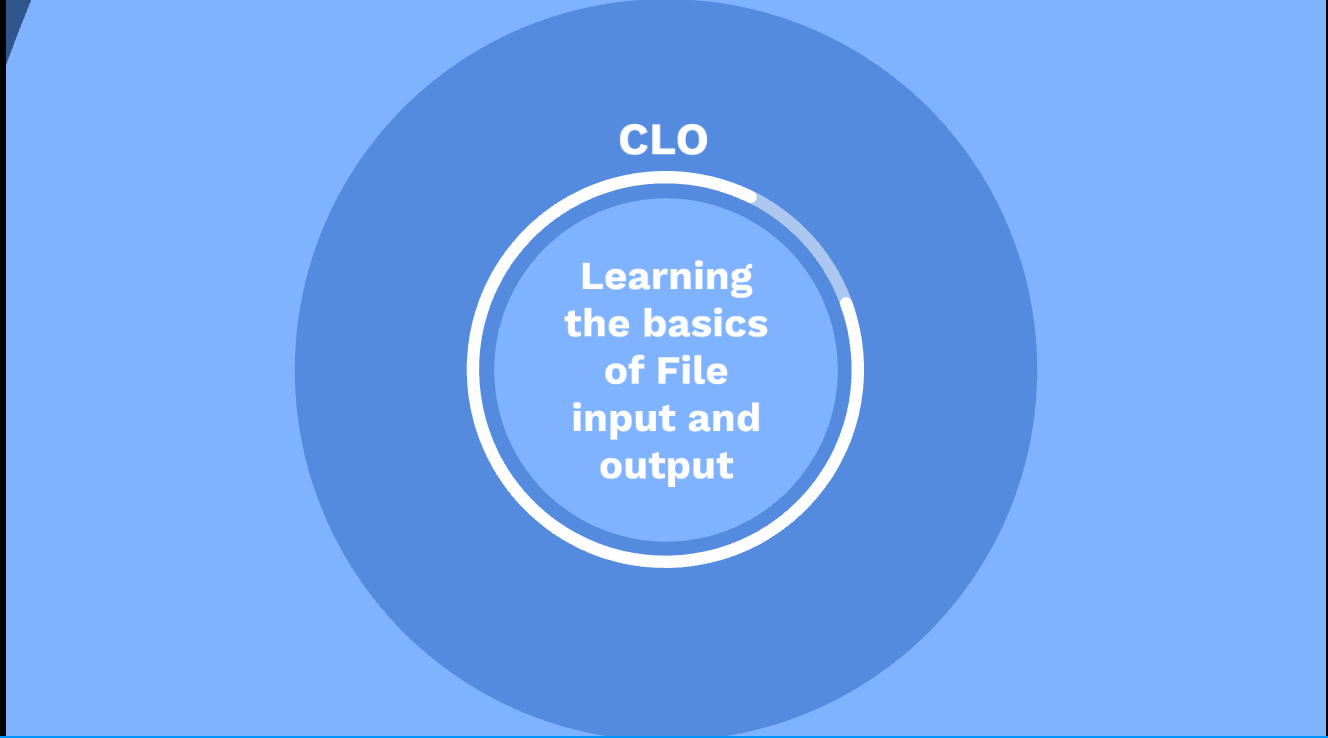
**How to Display Our Data**

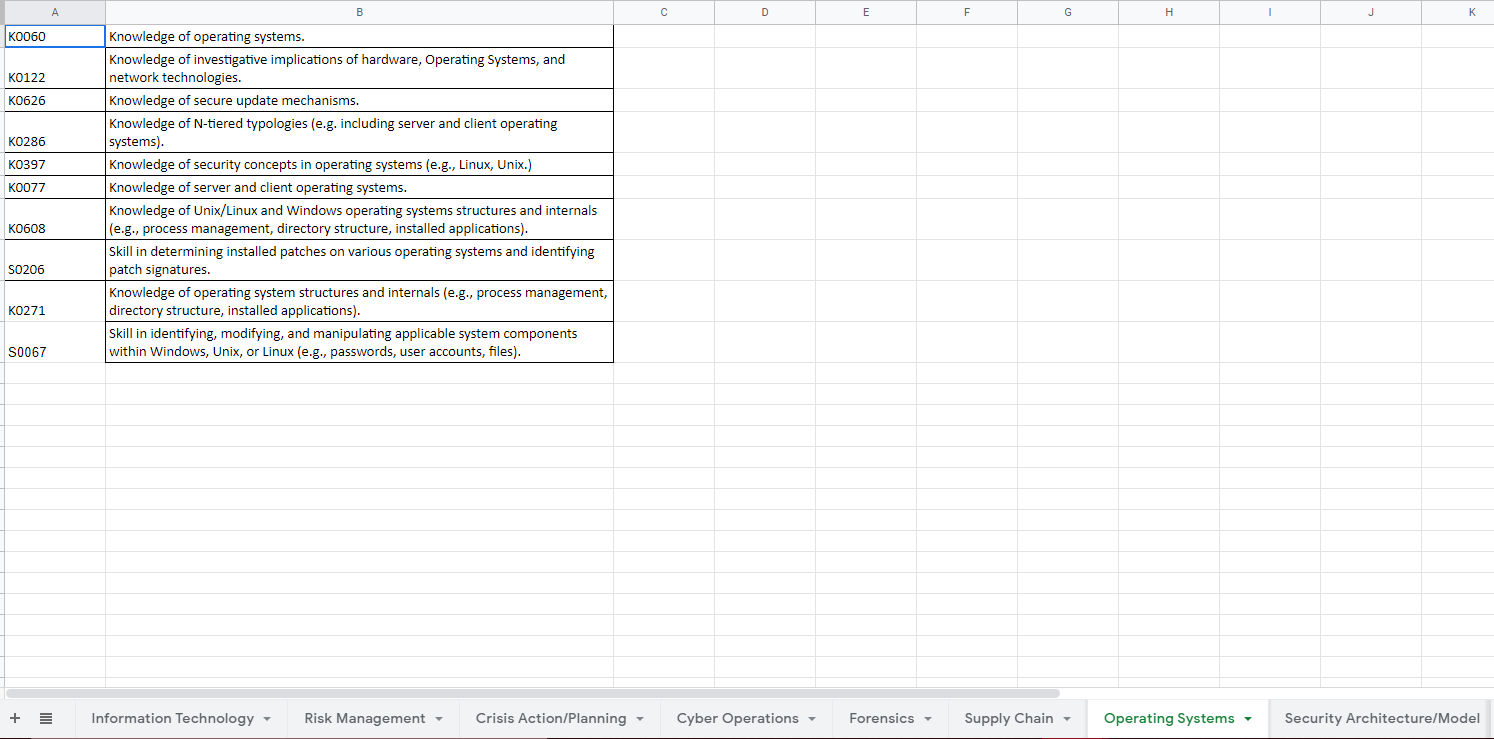
Though CDR Croteau was our initial point of contact and helped us immensely through this endeavor, our customer has been CAPT Caroland, the chair of the Cyber Science Department. In speaking with CAPT Caroland, we needed to discuss a way in which to effectively present our aggregated information. While we have done much work to find the relationships between the NICE Framework and the CLOs, it makes little difference if our end result is a poorly organized table, that much like coding, only the creators can understand. Through discussion with CAPT Caroland, we decided that the best way to present our findings would be through the use of a Prezi presentation.

A Prezi presentation was found to be the best tool to display the relationship between the CLOs to the KSAs because of its simplicity of use and ability to include large amounts of data. Prezi allows the user to see broad information and then narrow down a specific, individual item through its “add topic” feature. Each new topic can include further topics, thus creating an elegant way to display such a massive amount of KSA bins.

The Prezi begins by showing all 14 of the Cyber Operation courses that are required by majors in the curriculum. Users can then enter each individual course to see a high-level description of each CLO the course provides. Then, these high-level descriptions can be further entered to see the more specifically worded version of the CLO. After this, the user is able to see the KSA bins that are assigned to each individual CLO. In a separate Google Sheet document, all individual KSAs are listed with their assigned number and description. Each KSA bin is represented by tabs on the bottom of the spreadsheet for ease of navigation. Once the KSA bin is found on the Prezi, the user finds the KSA bin on the Google Sheet document. Then, finally, the user can see how each individual KSA relates to the overall course. The graphics below demonstrate our final product and how they would look to the end user.







**Conclusion**

In summary, the overarching objective of our project was to identify if the Cyber Operations major adequately mapped to the different Knowledge, Skills, and Abilities of Cyber Professionals, as outlined in the National Initiative for Cybersecurity Education. In order to answer this question we had to reduce the master KSA list into different categories or bins, and through the comparison of bins to the Course Learning Objectives, decide if there was a significant correlation or not. Through our work and final submission, we have reached the conclusion that the Naval Academy Cyber Operations Major covers the vast majority of what the NICE framework identifies as critical for a cyber professional, and as such we believe the current major more than adequately prepares students for both the military and professional world as a competent cyber individual.

References

“The Comprehensive National Cybersecurity Initiative | The White House.” n.d. Obama White House Archives. Accessed February 19, 2022. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

“Cyber Science • United States Air Force Academy.” n.d. Air Force Academy. Accessed March 25, 2022. https://www.usafa.edu/academic/cyber-science/.

“Cybersecurity Major - Provo.” n.d. BYU IT & Cybersecurity. Accessed March 26, 2022. https://itc.byu.edu/the-cybersecurity.

“Force Design 2030.” 2020. Headquarters Marine Corps. https://www.hqmc.marines.mil/Portals/142/Docs/CMC38%20Force%20Design%202030%20Report%20Phase%20I%20and%20II.pdf?ver=2020-03-26-121328-460.

Johanna, Jacob, Wei Wei, Kewei Sha, Sadegh Davari, and Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). 2018. “Is The Nice Cybersecurity Workforce Framework (ncwf) Effective For A Workforce Comprised Of Interdisciplinary Majors?.” ProQuest. https://www.proquest.com/conference-papers-proceedings/is-nice-cybersecurity-workforce-framework-ncwf/docview/2140023651/se-2?accountid=14748.

Riesenberg, Lou E. 1988. “Future Curriculum Emphasis For Colleges.” jstor. https://www.jstor.org/stable/43764374.

Temple-Raston, Dina. 2021. “How Russia Used SolarWinds To Hack Microsoft, Intel, Pentagon, Other Networks.” NPR. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

“USAFA COI.” n.d. Air Force Academy. Accessed March 25, 2022. https://www.usafa.edu/app/uploads/COI.pdf.

1. (“Force Design 2030” 2020) [↑](#footnote-ref-0)
2. (Temple-Raston 2021) [↑](#footnote-ref-1)
3. (“The Comprehensive National Cybersecurity Initiative | The White House”, n.d.) [↑](#footnote-ref-2)
4. (“Cyber Science • United States Air Force Academy”, n.d.) [↑](#footnote-ref-3)
5. (“USAFA COI”, n.d.) [↑](#footnote-ref-4)
6. (“Cybersecurity Major - Provo”, n.d.) [↑](#footnote-ref-5)
7. (Johanna et al. 2018) [↑](#footnote-ref-6)
8. (Riesenberg 1988) [↑](#footnote-ref-7)