

With ChatGPT, do we have to rewrite our learning objectives - CASE study in Cybersecurity

Peter Jamieson
Department of ECE
Miami University, Ohio
Email: jamiespa@miamioh.edu

Suman Bhunia, Dhananjai M. Rao
Department of CSE
Miami University, Ohio
Email: {bhunias, raodm}@miamioh.edu

Abstract—With the emergence of Artificial Intelligent chatbot tools such as ChatGPT and code writing AI tools such as GitHub Copilot, educators need to question what and how we should teach our courses and curricula in the future. In reality, automated tools may result in certain academic fields being deeply reduced in the number of employable people. In this work, we make a case study of cybersecurity undergrad education by using the lens of “Understanding by Design” (UbD). First, we provide a broad understanding of learning objectives (LOs) in cybersecurity from a computer science perspective. Next, we dig a little deeper into a curriculum with an undergraduate emphasis on cybersecurity and examine the major courses and their LOs for our cybersecurity program at Miami University. With these details, we perform a thought experiment on how attainable the LOs are with the above-described tools, asking the key question “what needs to be enduring concepts?” learned in this process. If an LO becomes something that the existence of automation tools might be able to do, we then ask “what level is attainable for the LO that is not a simple query to the tools?”. With this exercise, we hope to establish an example of how to prompt ChatGPT to accelerate students in their achievements of LOs given the existence of these new AI tools, and our goal is to push all of us to leverage and teach these tools as powerful allies in our quest to improve human existence and knowledge.

I. INTRODUCTION

Technological advancements can have an influence on how we approach education, and the emergence of Artificially Intelligent (AI) chatbot tools such as ChatGPT will result in the next wave of debates and questions on how the existence of these tools will change our educational approaches. ChatGPT is a natural language chatbot tool (where a chatbot is an autonomous robot that will respond to user queries) that has been trained on large language models such that the tool can respond to questions and generate user-requested solutions. For example, you can ask ChatGPT to write a story in the voice of your favorite author and define a simple plot and characters. ChatGPT will create that story, and in many cases, the story will be reasonably written. Additionally, ChatGPT and other tools such as Github’s Copilot provide users with the ability to help them design and code in a variety of programming and design languages to build various user-requested functionality. For example, we have used ChatGPT to design Verilog HDL modules of a Radix-2 SRT divider with reasonable success (noting that the tool is not perfect and expertise is needed for a well-formed design).

These later capabilities have caused those of us who sit in the computing education space into debates about how the existence of these tools changes what and how we teach. In this work, we propose to approach this debate from the perspective of student learning outcomes (LOs) as defined using verbiage from Bloom’s Taxonomy [1]. With LOs for a particular curriculum (our example case will focus on cybersecurity), we can pose the simple question of how these LOs might change, and what additional LOs should be added to the curriculum. To aid in this case study, we also will guide our discussion with the help of the useful concept filter described by Wiggins and McTyghe in “Understanding by Design” to classify the importance of LOs. By approaching a curriculum and the courses it comprises with these perspectives, our goal is to demonstrate how we might approach integrating AI tools into our curricula and education.

For this work-in-progress case study, we use existing cybersecurity organizational schemes to extract the “enduring understanding” concepts. This organizational scheme will then look at some of the LOs asking if the LO can be “accelerated” given the available AI tools. Next, we will look at our existing cybersecurity curricula with courses and look at each LO mapping and where it sits in Bloom’s Taxonomy. This will allow us to see what are the LOs for cybersecurity education and ask the question, “Should they be leveled up?”

II. BACKGROUND AND DISCUSSION

Our approach in this paper is to use the lenses of Bloom’s Taxonomy [1] and Understanding by Design’s [2] filter of concepts to understand the Learning Outcomes (LOs) in a particular curriculum and its respective courses. We have used a similar approach in our previous work [3] to help educators evaluate if they should spend time creating a game to teach a concept.

A. Bloom’s Taxonomy and Learning Outcomes

We define learning in this work, using ideas from [4], [5]: “Learning is the stabilization of neural networks based on a desired response”. This definition allows us to relate the idea of learning things to the necessity of trying and doing things, since if the neurons are not firing (by thinking and doing) then your neurons are not wiring (Donald Hebb in 1949 stated, “neurons that fire together wire together”).

A *Learning Outcomes* (LO) is an educational goal for a learner such that they will be able to cognitively perform the objective once they have learned it. Typically, an LO is described by a cognitive process taken from Bloom’s Taxonomy [1] and applying the process to some content as related to the field of study. Bloom’s taxonomy provides a hierarchy of cognitive processes as defined from “lower-order thinking skills”, such as recall and classification, to “higher-order thinking skills” such as creating or planning. The “higher-order” thinking skills tend to be what society wants of our workers, but these higher-order skills are much more challenging to develop and take significantly more time than the lower-order thinking skills to teach and learn because of the profession nature of learning.

This distinction between “higher” and “lower” can, however, confuses educators to somehow evaluate the quality of an LO based on where it sits in the taxonomy. As illuminated by Lang [6] professors can fall into the trap of simply wanting to teach “higher-order thinking skills” and assume that the lower skills can simply be looked up using technology such as search engines and the like (including tools like ChatGPT). The reality is to achieve skills such as “create” and “plan” in Bloom’s taxonomy requires that a human can keep and think about ideas and concepts within a field of study that requires the “remember” and “understanding”. In this work, we are asking this question in terms of accelerating an LO to a higher Bloom’s level, but we are aware of this pitfall, and will hopefully provide insight into how the new technology modifies the space.

B. Enduring Concepts and Learning Outcomes

The LOs need to be defined in a sentence where a verb is taken from Bloom’s taxonomy [1] and the object of the sentence describes some knowledge or skill. For example, a sample LO might be, “A student should be able to *construct* a program that will then generate a desired output with a proper sequence of program statements”. This objective is *apply* in Bloom’s taxonomy cognitive process dimension [1] and is *procedural* in the knowledge dimension [7]. From the taxonomy, this learning objective would be considered a “middle-order thinking skill”.

To further determine how important the LO is, we use Wiggins and McTighe’s filter [2]: (1) worth being familiar with; (2) important to know and do; (3) enduring understanding; where the importance of a LO is more important to a student’s future as the above number increases above. This filter allows a teacher to consider their LO and qualify how important it is. The reason this is useful is that just because an objective ranks as a “low-order thinking skill” if it is an enduring concept for that student in the respective field, then it is important to emphasize and should be achieved by the student. Similarly, depending on the time in the curriculum of a field, different ideas will need to be learned to holistically progress in a field.

Table I
LIST OF COURSES AT MIAMI UNIVERSITY TO COVER THE
CYBERSECURITY ACM GUIDELINE

Course Number	Course Name
CYB 134	Introduction to Cybersecurity
CYB 234	Sysadmin & scripting
CYB 235	Computer networks
CYB 236	Data Security
CYB 331	Software Security
CYB 332	Organizational and Human Security
CYB 334	Network security
CYB 335	Defensive Security
CYB 435	Offensive Security

C. Curriculum Design and Cybersecurity Curricula

Curriculum design is not a simple process by any means, and for most educators, we can understand this by realizing that a single course is hard to design, and a curriculum is a series of courses; hence it is of greater complexity. For this reason, we will leave much of the previous research on curriculum design with the exception of noting Sheenan’s work [8] that looked at the two conceptual models of the curriculum being either a product model (resulting in a student objective ending) versus the process model (resulting in a student with capabilities). We argue that the majority of our technical curricula are mostly process models.

Harrison *et. al.* [9] have looked at Bloom’s approach to the design of an information technology curriculum as mapped to Bloom’s taxonomy. Their approach to designing the curriculum provides a nice visual representation of how we could approach asking our technological change questions about the existence of ChatGPT.

III. LEARNING OUTCOMES AND THEIR LINK TO A CYBERSECURITY EDUCATION

Using the classification of *Prevention*, *Detection*, and *Response* we will start by looking at what LOs we believe are part of a modern cybersecurity computer science curriculum. Here, we note the work on the Cybersecurity Concept Inventory (CCI) which is currently being validated in work by Poulsen *et. al.* [10] and by Herman *et. al.* [11]. Their concept approach identifies concepts that can be validated, and with the validation of this work, an important next step would be having learners progress through our curriculum (ChatGPT enhanced and unenhanced) and evaluate our learners.

Table I shows our Miami University’s cybersecurity courses [12] and the course name. The topics covered for ACM’s cybersecurity curriculum [13] is implemented in a table (not included in the paper). In this mapping, we list the Bloom level of the learning outcomes. The interesting information from this exercise is that the majority of knowledge units are with respect to Bloom’s Taxonomy. For the first three levels of “1 - Remember”, “2 - Understand”, and “3 - Apply” in our mapping, there are 22, 28, and 14 instances of these, totaling 65 of the 66 listed course LOs. The highest Bloom’s level for our curriculum includes 1 instance of “4 - Analyze”.

The main reason for the above result is the number of LOs listed for covering the cybersecurity curriculum over nine courses. The reality is there is a lot of ideas to learn about

in the space of cybersecurity as a system, and its complexities (beyond hardware and software) make technological and psychological knowledge and skills a tremendous burden on this type of education. As we've alluded to in this paper, the question is, will tools such as ChatGPT allow us to push our learners and teachers into an accelerated space?

IV. GPT EXAMPLES WHERE THE TOOL MAY ALLOW US TO RAISE AND ACCELERATE LEARNING OUTCOMES

As noted in the last section's analysis, the demands of remembering, understanding, and applying new knowledge and skills are overwhelming for the cybersecurity curriculum. This section provides a few examples of how an LO can be linked with ChatGPT to accelerate and potentially raise the skill and knowledge to a higher Bloom's taxonomy level. As stated earlier, the goal is not to simply move up in terms of Bloom's Taxonomy levels as this is not a feasible approach to learning and becoming an effective practitioner. Instead, our goal is to provide examples of how ChatGPT can be used to extend what the learner achieves in terms of the knowledge unit. In each example, we will show the knowledge unit in the title, show the prompt and response and then discuss how this allows the learner to push their knowledge further.

A. Data Security - Access Control

The original LO for this knowledge unit is "Identify and explain the importance of basic system administration tasks" in the course CYB 234 ¹.

Prompt: What is the Linux command to add execute permission to just group users

Response: The command to add execute permission to just group users in Linux is

```
chmod g+x <filename>
```

Here, "chmod" is the command used to change file permissions, "g" stands for a group, and "x" adds execute permission to the file for the group. Replace <filename> with the name of the file for which you want to add execute permission to the group.

Figure 1. Prompt and response for using Linux file permissions

Figure 1 shows an example of how to move from **Understand** to **Apply** in data security access control. Instead of just describing how the system permissions allow users to perform certain actions in Linux, we now have details of what is the exact Linux syntax for the command line and can now test it in the tool.

With ChatGPT acting as a tutorial agent, we can imagine a student being able to test out on a Linux system how the command works and observe what the system does to manage access control for a shared system.

¹<https://www.miamioh.edu/cec/academics/departments/cse/academics/course-descriptions/cyb234/index.html>

B. Software Security Analysis and Testing

The original LO for this knowledge unit is "Describe and apply static and dynamic software testing methods" in CYB 331 - Software Security.

Prompt: Does the following program have a memory leak problem?

```
void f() {
    int *ptr = (int *) malloc(sizeof(int));
    /* Do some work */
    return; /* Return without freeing ptr*/
}
```

Response: Yes, the program has a memory leak problem. The "malloc()" function allocates memory dynamically, but the "ptr" pointer is never freed, which means that the memory remains allocated even after the function returns. This can lead to memory leaks and other issues if the program continues to allocate memory without freeing it. To fix this problem, the memory allocated by malloc() should be freed before the function returns using the free() function. Here's an example of how to modify the code to fix the memory leak:

```
void f() {
    int *ptr = (int *) malloc(sizeof(int));
    /* Do some work */
    free(ptr); /* Free the memory before returning */
    return;
}
```

Figure 2. Prompt and response for analyzing some C-code

Figure 2 shows how we can use ChatGPT to accelerate a student's understanding of software security analysis from **Apply** to **Analysis**. With the ChatGPT, the user can prompt the tool to analyze their code and make it more secure.

We imagine providing code to the student that shows a number of cases such as memory leaks and buffer overflows that ChatGPT can help them analyze and understand. Next, given a larger code base, either their own or a manufactured case, could the learner use the tool to analyze the code, and then help the student create a safer version of it.

C. Component reverse engineering

The original LO for this knowledge unit is "Explain how failures in fundamental security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation" in CYB 331 - Software Security.

Figure 3 shows what ChatGPT provides when prompted to reverse engineer some assembly code. This allows students to go beyond remembering what reverse engineering is and into the space of understanding what potentially is possible with using reverse engineering.

In this space, the tool provides rudimentary capabilities in reverse engineering. The question is, can students reverse engineer other more complex pieces of code, and similarly, obfuscate their own code examples such that they can fool this simple tool?

Prompt: Reverse engineer the following code to C code:

```
fact(int):
    movl $1, %eax
    cmpl $1, %edi
    jle .L1
.L2: movl %edi, %edx
    subl $1, %edi
    imull %edx, %eax
    cmpl $1, %edi
    jne .L2
.L1: ret"
```

Response: Sure, here's the equivalent C code for the given x86 assembly code:

```
int fact(int x) {
    int result = 1;
    if (x <= 1) {
        return result;
    } else {
        do {
            result *= x;
            x--;
        } while (x > 1);
        return result;
    }
}
```

The fact function takes an integer argument x and returns the factorial of x. Here's how the x86 code translates to C code:

- `movl $1, %eax` sets the `eax` register to 1, which initializes the result variable to 1.
- `cmpl $1, %edi` compares the value of `x` with 1.
- `jle .L1` jumps to the `.L1` label if `x` is less than or equal to 1. This is the base case of the factorial function.
- `.L2:` is a label that marks the start of the loop.
- `movl %edi, %edx` moves the value of `x` into the `edx` register, which is used to calculate the next iteration of the result.
- `subl $1, %edi` decrements `x` by 1.
- `imull %edx, %eax` multiplies the current value of `result` (stored in the `eax` register) with the current value of `x` (stored in the `edx` register), and stores the result back into `eax`.
- `cmpl $1, %edi` compares the new value of `x` with 1.
- `jne .L2` jumps back to `.L2` label if `x` is not equal to 1, which means that we need to continue the loop to calculate the next iteration of the result.
- `.L1:` is the label that we jump to if `x` is less than or equal to 1. This is the base case of the factorial function.
- `ret` returns the result of the function to the caller.

Figure 3. Prompt and response for analyzing some C-code

D. Connection Security - Distributed System Architecture

The original LO for this knowledge unit is "Describe application layer security protocols" in CYB 334².

Figure 4 shows what ChatGPT can describe in terms of using a Linux system to evaluate the state of the network. Again, using ChatGPT as a personalized tutor allows the

Prompt: Write a command that will find all computers in a network running MySQL

Response: Assuming you have nmap installed on your system, you can run the following command:

```
sudo nmap -p 3306 --open -sV <network-address>
```

Replace `<network-address>` with the IP address or the network address of the network that you want to scan for devices running MySQL. For example, if the network address is 192.168.0.0/24, you would run:

```
sudo nmap -p 3306 --open -sV 192.168.0.0/24
```

This command will scan the IP addresses in the specified network range and check if port 3306 (default MySQL port) is open on each of them. It will also attempt to determine the version of MySQL running on each device.

Note that you may need to modify the IP address range according to your network configuration. Additionally, the `sudo` command is used to run `nmap` with elevated privileges, which may be necessary depending on your system configuration.

Figure 4. Prompt and response for looking at a network to find out what servers are accepting

learner to get direct feedback on how to proceed in the space.

V. CONCLUSION

In this work, we looked at our existing cybersecurity curriculum as a case study of how well AI-driven natural language processing tools such as ChatGPT change the LOs of a curriculum. To do this we used the lense of LOs and their respective Bloom's taxonomy verbiage and mapped out our cybersecurity curriculum. We noticed that there are a large number of LOs in Cybersecurity and most of those LOs sit in the "low-order" thinking skills. Based on this, we hypothesize that ChatGPT will allow us to accelerate some of our existing LOs, given the tool's capabilities. To show this we provide five examples of how an existing LO can be accelerated with ChatGPT, given the capabilities of the tool.

From this exercise, we have learned two things in particular that we believe we will need to be further examined by all educators. First, our experiences with ChatGPT suggest that the tool can provide a powerful means to allow learners to generate pieces of their work quickly. However, learners will need to be taught how to create prompts, and how to validate the responses and designs provided by the tool, and just like using the browser to find things, the learner needs to be aware of the vocabulary used to get acceptable responses. Second, we will need to consider how to teach concepts that need to be experienced from "first-principle" learning approaches and learn how to motivate students to perform some rudimentary exercises that "the tool" can easily do for me. We will argue, that some basic experiments need to be done that provide us with evidence of why certain concepts still need to be done to help us prove to our students the importance of early learning exercises.

²<https://www.miamioh.edu/cec/academics/departments/cse/academics/course-descriptions/cyb334/index.html>

REFERENCES

- [1] L. W. Anderson, D. R. Krathwohl, and B. S. Bloom, *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. Allyn & Bacon, 2001.
- [2] G. P. Wiggins, J. McTighe, L. J. Kiernan, and F. Frost, *Understanding by design*. Association for Supervision and Curriculum Development Alexandria, VA, 1998.
- [3] P. Jamieson and L. Grace, "A framework to help analyze if creating a game to teach a learning objective is worth the work," in *2016 IEEE Frontiers in Education Conference*, 2016, pp. 1–7.
- [4] J. Zull, "The Art of Changing the Brain: Enriching the Practice of Teaching by Exploring the Biology of Learning," 2002.
- [5] D. A. Kolb, *Experiential Learning*. Englewoods Cliff, NJ: Prentice Hall Inc., 1984.
- [6] J. M. Lang, *Small teaching: Everyday lessons from the science of learning*. John Wiley & Sons, 2021.
- [7] D. R. Krathwohl, "A revision of bloom's taxonomy: An overview," *Theory into practice*, vol. 41, no. 4, pp. 212–218, 2002.
- [8] J. Sheehan, "Curriculum models: product versus process," *Journal of advanced nursing*, vol. 11, no. 6, pp. 671–678, 1986.
- [9] M. A. Harris *et al.*, "Using bloom's and webb's taxonomies to integrate emerging cybersecurity topics into a computic curriculum," *Journal of Information Systems Education*, vol. 26, no. 3, pp. 219–234, 2015.
- [10] S. Poulsen, G. L. Herman, P. A. Peterson, E. Golaszewski, A. Gorti, L. Oliva, T. Scheponik, and A. T. Sherman, "Psychometric evaluation of the cybersecurity concept inventory," *ACM Transactions on Computing Education (TOCE)*, vol. 22, no. 1, pp. 1–18, 2021.
- [11] G. L. Herman, S. Huang, P. A. Peterson, L. Oliva, E. Golaszewski, and A. T. Sherman, "Psychometric evaluation of the cybersecurity curriculum assessment," in *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, 2023, pp. 228–234.
- [12] Miami University of Ohio, "Course Descriptions for Department of Computer Science and Software Engineering," <https://www.miamioh.edu/cec/academics/departments/cse/academics/course-descriptions/>, 2023.
- [13] ACM, "Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf, 31 December 2017.