Cyber Security and Philosophy: An Intersection

By: Zaheer Charles

Introduction

Communication systems in today's world have become incredibly complex with unprecedented levels of connectivity. With the ability to communicate among individuals and organizations across vast distances (global/cyber communications systems) comes the ability to represent oneself without the need to be physically present. The reduced need to physically be in the same room with someone fosters anonymity and opens the door to cybercrime. Not everyone who communicates virtually harbors criminal intent, but the actions of enough unethical communicators have warranted the need for "officers" to police the cyber communications sector relentlessly. Historically, these cyber officers have come from Computer Science backgrounds, but with the emergence of greater dangers comes the need for Cyber Security Professionals from seemingly unrelated backgrounds such as Philosophy.

Although digital anonymity fosters the potential for unethical behavior, a greater danger may be **unethical and anonymous cyberspace hackers**. These unethical actors invade privacy and steal data from both individuals and organizations alike. Like criminals in the physical world, *cyber* criminals cause pain and suffering to innocent and unsuspecting victims for monetary gain. And like criminals in the physical world, cyber criminals have evolved in their methods and tactics for engaging in unethical hacking. Hackers are now shrewder than ever and have created the need for a cleverer cyberspace officer—a cyberspace officer who thinks outside of the box. Enter, the *Cyber Security Professional* ***from a Liberal Arts background*****!**

Purpose

Typically, *Cyber Security Professionals* emerged from a limited range of academic backgrounds. However, new methods of engaging in unethical cyberspace hacking have created the need for Cyber Security Professionals which come from backgrounds that prioritize rhetoric and critical thinking. Many students have been *discouraged* from pursuing Liberal Arts degrees and *encouraged* to pursue STEM degrees to secure stable, well-paying careers. The subsequent influx of students in more technical programs has created a higher need for students with backgrounds in the Liberal Arts, like Philosophy majors, to combat the new cyberspace threats. Thus, the purpose of this report is to encourage a paradigm shift in the way students, parents, and employers perceive the benefits of a Liberal Arts degree with respect to a career in the field of Cyber Security.

Opening Doors in the Field of Cyber Security

Recently, Philosophy majors have become hot commodities in the world of Cyber Security. According to the article "9 Career Choices for Philosophy Majors," found on the job search site indeed.com,

> "Majoring in Philosophy can grant you many interesting and unique skills. Philosophy majors learn to think deeply and complexly, they are required to consider innovative and creative solutions to society's common problems, and they have a reputation for being independent thinkers and highly intelligent" ("9 Career Choices").

The article further states that most Philosophy majors have excellent communication skills, both written and verbal, and that Philosophy majors tend to be skilled problem-solvers and great independent workers ("9 Career Choices").

The "9 Career Choices" article is not an anomaly within the Cyber Security sector; academic professionals within the field echo the same sentiment. For instance, according to the California State University, San Bernardino, Department of English Technology, students who major in the Liberal Arts "are in demand in various technical fields", with employers in the technology sector valuing Liberal Arts majors for their "ability to think synthetically, compose imaginatively, and communicate effectively" (CSUSB English Technology).
And according to the California State University, Liberal Arts majors can enjoy careers in Web Development and Cyber Threat Intelligence Analysis (CSUSB English Technology).
These careers in the field of Cyber Security would require Philosophy majors to engage in daily tasks which include:

- Identifying cyber threats to companies and organizations.
- Tracking adversarial cyber activities via social media, intelligence reports, and current events.
- Identifying purpose, context, authorship, and linguistic features of cyber activity.
- Writing reports and preparing presentations.
- Analyzing, synthesizing, and evaluating complex information.
- Collaborating effectively with team members.
- Utilizing excellent communication skills, both spoken and written.

A Philosophy major is well qualified to execute many of these tasks. Adding a few courses in computer science, and Cyber Security issues, like CS 1910 (Cyber Security for All) and CS 4940 (Ethical Hacking) respectively, the Philosophy major would have many more doors open to her/him and increase their chance in attaining a stable career in the field of Cyber Security.

Philosophical Theory Relevant to Cyber Security

Although you might initially think Plato, Aristotle, and Socrates have nothing to offer the cyber industry, that would be far from the truth. Historically, philosophers have tackled the questions in life which cannot be answered using mathematics or other hard sciences. Ethical considerations fall within the philosopher's domain. Questions concerning the

morality of choices and actions are the focus of philosophical ethical theory, with our concentration being on the choices made by the digitally anonymous. The philosophical theory most relevant to the power of digital anonymity is the theory of *Ethical Egoism*. Ethical Egoism, according to Britannica.com, is an ethical theory which claims that moral decision making should be guided entirely by self-interest ("Ethical Egoism"). Now, while ethics has an inherent dichotomy concerning the *rightness* or the *wrongness* of morality, there is also a distinction between what one *ought to do* and what one *does*. This distinction is due to the contrasting nature of morality. For there is a difference between the reasons behind what *is done* and what *should be done*. Ethical Egoism is concerned with what *should be done* for a person's actions and decisions to be considered *morally right*.

Psychological Egoism, in contrast, is a theory which describes everything which a person *does* as being in that person's best self-interest. Again, this paper will focus on what *should be done*.

Ethical Egoism and the Importance of Cyber Security

How does Ethical Egoism pertain to the importance of Cyber Security? Well, let's begin with a thought experiment provided to us by Glaucon and Socrates in the story "The Rings of Gyges," by Plato. According to Plato, Glaucon and Socrates are having one of their usual debates and their point of contention becomes whether a person, given the power to be just, has enough morality to maintain the straight and narrow path of moral rightness (Plato 4).

According to the story, Glaucon recounts a tail of a shepherd named Gyges who was in service of the King of Lydia (Plato 4). One day while tending to his flock of sheep, Gyges came across a magic bracelet which granted its wearer the **power of invisibility** (Plato 4). Once this power was realized, Gyges used the power of invisibility to gain access to the inner castle, seduce the Queen, kill the King, and assume control of the entire kingdom through unjust methods (Plato 4).

Now imagine there were 2 of these rings and only the most honest and dishonest person could possess each ring. The honest person never uses the ring and the dishonest person always uses the ring. If these 2 perfectly opposite people continued this way until the ends of their lives, what would people say compared to what they think? Glaucon believed that most people would openly praise the honest person for never using the magic ring, while secretly condemning this honest person for wasting the power of the ring (Plato 4).

Most people would agree that unused power is equal to potential power. And where there is potential, there is cause for critical analysis of possible applications of this potential. Cyber criminals have immense potential and have become increasingly kinetic with each passing generational wave of new unethical hackers. This generation also needs its heroes: The Ethical Hackers—Cyber Security professionals with the critical lens of a lawmaker or

public servant. A professional who, historically, would pursue a career in Law, is exactly the kind of professional that is necessary in the cyber neighborhood.

Skills Gained from Earning a B.A. in Philosophy

According to the UCCS Course Catalog, students choosing to pursue a Bachelor of Arts degree in Philosophy, can expect to obtain skills in critical thinking, write and orally express clear, logical, and grammatically correct philosophical arguments, and display detailed knowledge of relevant literature related to philosophical problems. Furthermore, Philosophy majors must be able to demonstrate research skills in locating and using resources and extending inquiry on philosophical questions ("Philosophy, BA"). In the domain of Cyber Security, these skills allow the Philosophy major to critically and vigilantly analyze large quantities of data while maintaining favorable ethics and using rhetoric to persuade audiences of the importance of their mission. Thus, the Philosophy major may find her/himself interacting with subject matter experts in attempts to encourage changes in thoughts and procedures, both internally and externally to their organizations.

A Career for the Philosophy Undergrad in Cyber Security

Given the range of skills Philosophy majors will gain and the flexibility of unethical and anonymous cyberspace hackers, employers have begun to seek candidates with a broader range of skills to combat the shifting threat using new and innovative approaches that resonate more with ethical hackers of Liberal Arts backgrounds.

While employers are searching for a wider range of candidates, they still want candidates to possess core skills. A Philosophy B.A., by itself, is not enough. Employers are seeking candidates who are more well-rounded, like Jack-of-all-trades, to innovate and grow with their unethical cyber-contenders. Essentially, employers are looking for candidates who are accustomed to looking at things "on the outside of the box," but capable and comfortable bringing that mindset "inside the box."

In addition to philosophy courses, Philosophy students can strengthen their preparation for careers in cybersecurity by enrolling in the following courses:

NCS 2910 – Secure Mobile Cloud Computing

- **CS 3910 – System Administration and Security**
- **CS 4910 – Introduction to Computer Security**
- **CS 4920 – Introduction to Applied Cryptography**
- **CS 4930 – Privacy and Censorship**
- **CS 4940 – Ethical Hacking**
- **CS 4950 – Homeland Security and Cyber Security**
- **CS 4980 – System Security**

This list comprises the core courses necessary to earn a Bachelor of Arts degree in Computer Science ("Computer Science, BA"). Philosophy affords the LAS student the flexibility to pursue an emphasis, a second major, or even a second degree. Philosophy majors have the freedom to explore a multitude of career paths, though they are not likely to take every course available to them due to time and financial constraints. Although an LAS student is not likely to take all these courses, any of these would supplement skills from a Philosophy BA.

Other electives include:

Information Security courses

- INFS 1100 – Productivity Apps for the Workplace
- INFS 3000 – Information Systems and Business Intelligence Impact on Business
- INFS 3070 – Business Programming Fundamentals
- INFS 3400 – Database Management
- INFS 3500 – Introduction to Cybersecurity Technologies
- INFS 3700 – Computer Networks and Telecommunications
- INFS 3750 – Organizational Cyber Security
- INFS 3800 – Programming Web-based Systems
- INFS 4050 – Information Technology Integration
- INFS 4400 – Big Data Analysis
- INFS 4700 – Advanced Networking Topics
- INFS 6000 – Information Systems

Business Law courses

- BLAW 2000 – Business Law
- BLAW 2010 – Business and Intellectual Property Law

Cyber Security Management courses

- CYSM 3500 – Introduction to Cybersecurity Technologies
- CYSM 3700 – Computer Networks and Telecommunications
- CYSM 3750 – Organizational Cyber Security
- CYSM 4100 – IT Risk Management
- CYSM 4300 – IT Security Auditing
- CYSM 4500 – Ethical Hacking
- CYSM 4700 – Cloud Computing and Security

Gaining Access to the Field of Cyber Security

The classes outlined above give a general outline of the kinds of skills a Philosophy major would bring to the world of Cyber Security if combined with the core skills inherently found in Philosophy majors. While Philosophers famously uphold the stereotype of being

freethinkers, the Philosophy major must foster a specific set of skills to maintain a competitive edge in the Cyber Security career field. Following is a list of skills requested by Cyber Security employers, according to Sonya Krakoff, the Senior Content Marketing Specialist at Champlain College Online, in her article titled "The Top Skills Required for Cybersecurity Jobs,":

1. **Problem-Solving skills**
   Explore creative ways to take on and address complex information security challenges across a variety of existing and emerging technologies and digital environments.
2. **Technical Aptitude**
   Daily activities include troubleshooting, maintaining, and updating information security systems; implementing continuous network monitoring; and providing real-time security solutions.
3. **Knowledge of Security Across Various Platforms**
   comfortable working on a variety of operating systems, computer systems, mobile devices, cloud networks, and wireless networks. while keeping up to date on advances in the field for all these technologies.
4. **Attention to Detail**
   highly vigilant and detail-oriented individuals, who can effectively detect vulnerabilities in their systems. Often responsible for continuous network monitoring to quickly identify concerns and come up with and address security solutions in real-time.
5. **Communication skills**
   Ability to effectively communicate and explain findings, concerns, and solutions to others Speak clearly and concisely on Cyber Security strategy and policy, as well as convey technical information to individuals and organizations of different levels of technical comprehension.
6. **Fundamental Computer Forensic skills**
   To effectively protect organizations' digital assets and to prevent security breaches, the Cyber Security professional needs to have a solid understanding of the ramifications of failed efforts, and the process of recovering data.
7. **A Desire to Learn**
   Commit to keeping current with the best practices and emerging industry trends and continue learning and self-educating for the entirety of the career.
8. **An Understanding of Hacking**
   understand how to perceive and exploit vulnerabilities. Essentially, the Cyber Security professional needs to learn to become an ethical hacker.

Conclusion

Unethical and anonymous cyberspace hackers continue to revise their tactics and strategies, consequently expanding the need for Cyber Security professional. Employers are

finding renewed purpose and value in graduates who hold a degree in Philosophy, especially when those degrees are supplemented by courses which give these majors the necessary technical skills. A new purpose for Philosophy majors lies in the direction of Cyber Security, where Philosophy majors can find a niche in combating cyberspace threats using their specialized skillset of critical thinking, research, analysis, and powers of persuasion. So, while the current paradigm suggests that STEM degrees are the only path into the field of Cyber Security and other technical fields, a large and growing body of evidence suggests that there is more than one avenue into this ever-evolving field.

Works Cited

"*9 Career Choices for Philosophy Majors*." Indeed.com, 23 Aug. 2021. https://www.indeed.com/career-advice/finding-a-job/jobs-for-philosophy-majors. Accessed 30 Mar. 2022.

"*Computer Science, BA*." Course Catalog. University of Colorado, Colorado Springs, 2022. http://catalog.uccs.edu/preview_program.php?catoid=17&poid=4459&returnto=1381. Accessed 30 Mar. 2022.

"*English, BA*." Course Catalog. University of Colorado, Colorado Springs, 2022. http://catalog.uccs.edu/preview_program.php?catoid=17&poid=4024&returnto=1381. Accessed 30 Mar. 2022.

"*Ethical Egoism*." Britannica.com, 10 Feb. 2022. https://www.britannica.com/topic/pessimism. Accessed 30 Mar. 2022.

Krakoff, Sonya. *The Top Skills Required for Cybersecurity Jobs*, 2022. https://online.champlain.edu/blog/top-cybersecurity-skills-in-high-demand. Accessed 30 Mar. 2022.

"*Philosophy, BA*." Course Catalog. University of Colorado, Colorado Springs, 2022. http://catalog.uccs.edu/preview_program.php?catoid=17&poid=4094&returnto=1381. Accessed 30 Mar. 2022.