An Aphoristic Treatise Regarding Organization as a Fundamental Concept to a Philosophy of Cybersecurity

By

James Palazzolo

COT 700 Introduction to the Interdisciplinary Study of Technology

Dr. Dorothy K. McAllen

December 15th, 2020

Introduction

The word treatise is somewhat esoteric. It means a systematic argument or position in writing that includes a methodical discussion of fact(s). Truthfully, this will most likely be an awful discussion of fact, not because there is no system or method applied in generating the argument. Instead, it will most likely be awful because there is no solid precedent for such a discussion. This body of work aims to take a position on a concept to a Philosophy of Cybersecurity. In truth, there is a minimal bibliological reference to the precise discussion regarding a Philosophy of Cybersecurity. We can reference literary works regarding a Philosophy of Law (Marmor, 2010) or reference to moral philosophies (Cushman & Young, 2009). However, an exact Philosophy of Cybersecurity is a rare find, if ever at all. This rarity might be attributed to a lack of philosophers who create entries into the cybersecurity body of knowledge that creates philosophical discussion about the phenomena.

Several words and their corresponding definitions were considered during the creation of this treaties. Many of which have been myopically considered to be relevant to cybersecurity. Merriam-Webster records the first use of the word "cybersecurity" in 1989, though no particular reference is given to support this date. If true, we can assume the word *cybersecurity* is now thirty years old. Definitionally, cybersecurity means activities or measures taken to protect computers from unauthorized access or attack (Definition of CYBERSECURITY, 2020). Applying the same query style for the definition of Information Security within the Merriam-Webster online portal, we find no specific definition. Lack of information security definition is odd considering the idea of information security as a set of principles (e.g., confidentiality, availability, and integrity) dates back to as early as 1976. In their work "Secure Computer System: Unified Exposition and Multics Interpretation" (Bell & La Padula, 1976), Bell and La

Padula lay the principal foundations of cybersecurity. In fact, their work is entirely concerned with the security of computing systems.

Before we proceed into understanding what philosophy is, why philosophy is important, how a philosophy is created, and how philosophies are adopted, we need to layout some fundamental definitions of the words for which will be used within the context of this discussion. We have already defined cybersecurity. So far, we have not defined the following words: technology, cyber, and security.

Though there will be other definitions presented throughout this discussion, these three words are critical to the alignment of the argument's position. Per Merriam-Webster, *technology* is defined as the capability and (or) the practical application of knowledge concerning a particular subject (Definition of CYBERSECURITY, 2020). The word *cyber*, again using Merriam-Webster (Definition of CYBER, 2020) as a credible reference, is defined as things relating to computers or computer networks. Lastly, the word *security* is defined (Definition of SECURITY, 2020) as freedom from danger, anxiety, fear, or something that is made certain. Therefore, as we seek to consider a Philosophy of Cybersecurity, we must keep in mind that we are talking about the practical application of a body of knowledge concerning computer(s) or computer network(s) in a way that keeps these computational things free from danger and that their state is made certain.

Philosophy

So, what is Philosophy? This section of the treatise will rely heavily on the work provided by Deleuze and Guattari. In their work "What is Philosophy?" (Deleuze & Guattari, 1994), they present very concisely what Philosophy is. The journey to understanding what

Philosophy is, through the author's assertion, is mind-bending. As a definition, *philosophy* is defined as the pursuit of wisdom, learning exclusive of practical arts, a most basic belief, or a set of concepts (Definition of PHILOSOPHY, 2020). "What is Philosophy?" reiterates this claim that philosophy requires concepts in order to begin to explain a thing or what it is. The idea of philosophy is also an illusion within itself. Concepts are abstractions (Definition of CONCEPT, 2020), meaning there is room for interpretation and subjectivity. Nonetheless, the concept acts as an aspectual ingredient of any philosophical recipe.

If a concept is required, what is the right number of concepts needed to suffice conceptual supply for a philosophy of something? When do philosophers know when to stop creating concepts regarding a particular philosophy? Deleuze and Guattari explain this dilemma as an unending set of back-and-forth series of conceptualizations (Deleuze & Guattari, 1994, p. viii) between the philosopher and the personae (Deleuze & Guattari, 1994, p.2).

The personae act as not a friend to the philosopher, but rather another individual to ask and receive questions about a phenomenon; an almost entirely internal discussion between the philosopher and the philosopher's self. The personae do not require the personae to exist in reality. The relationship between philosopher and personae enables an evolutionary discussion of transient states of "agreement" on what concepts help define something.

It might be easy to assume that philosophy is a method of contemplation, reflection, and communication. However, it is not (Deleuze & Guattari, 1994, p. 6). To say that philosophy is not contemplation, reflection, or communication is an important statement. As we will see later and aligning to the idea that philosophy explains *what is*, to know what something *is not* helps shape the contour and edges describing something through philosophical means.

Tentatively, let us say that a philosophy is created about something. Does that mean that the philosophy is important? Do we have to ask, as a matter of importance, how the philosophy was created; meaning, was the creation valid enough to make it relevant to importance? Moreover, as a contribution to the body of knowledge, the "So what?", if important, how is something important even adopted? It is one thing to create a masterful piece of work that has complete relevance to a body of knowledge, but if the work is never communicated, discussed, and adopted, does this mean that the work is actually of no value; of no import? These are all relevant questions to ask.

Luckily, but bitterly, we can look to previous ventures into philosophical discussion to find some solace from the past. There is no clear answer to the question: *how is a philosophy adopted?* Adoption means that the information presented within the philosophy meets some social acceptance of the information (e.g., it is agreed upon among peers). The word "peers" is significant here. It is the distinguishing word between the personae the philosopher interacts with and actual people. Personae, in imaginative form, may adopt any philosophy regarding a thing that the philosopher presents. However, the peer may not. As with any other social acceptance of a thing, there is no exact way to determine if something has been accepted by other non-personae (e.g., a body of peers). Or is there? Direct gratitude for presenting philosophical revelations might not be so apparent, but bodies of work referencing bibliographically a philosophy do mean that someone, somewhere, has accepted what the philosophy represents. For example, Cottringer has accepted particular philosophical works regarding conflict (Cottringer, 2005), Jafari et al. accepts there are reasons to adopt particular design philosophies (Jafari et al., 2018), and Mehra et al. admits there are relevant philosophies to be considered concerning orienting operations to improve performance in banking services (Mehra et al., 2011).

Like adoption, there is no clear answer as to how philosophies are created. Leaning again on the work provided by Deleuze and Guattari, we see that their opinion is that concepts are created as a result of problems (Deleuze & Guattari, 1994, p. 16). However, if no problem exists, can there still be concepts? Does one need a problem to derive something abstract if concepts are abstract statements? What if something has no problem? The connotation of "problem" implies that there is something wrong.

What if the concept is defined to describe what is abstract? As an example, a person is crossing a street. There is no problem with that. The concept is that the person simply *wants to get to the other side of the street*. Is *want* a problem? Maybe. Or *want* may simply be a condition to be set from true to false. Flipping from one to the other is not a problem. Instead, *want* is a function. Functions can be conceptualized into real concepts. Abstractedly, crossing the street can mean many things, but not entirely present a problem. Therefore, philosophies based on concept do not entirely require a problem to be valid.

Furthermore, if there is no problem or a problem that extends beyond the myopic observer, how do we know there is any import? Does import even matter? Subjectively, thinking that philosophies must include more than one person to consider the concepts important is invalid. If only one person thinks the concepts are valid, then the philosophy, built upon concepts, is important. Why does philosophy need to scale to be relevant to the body of knowledge when the body of knowledge, socially accepted, has no real connection to what is relevant because the relevance conceived by the body of knowledge is subject to social acceptance? Philosophy does not require more than one person's acceptance to make valid the philosophy itself (e.g., a personal philosophy of something). Does it help the permeation of a philosophy if disseminated to more than one person through social acceptance? Sure. Pring

argues for the importance of philosophy in educational research (Pring, 2012), and Lutz maintains that philosophy is essential with regard to Liberalism (Lutz, 1997). However, these are still subjective bodies of work. We have to ask – to what benefit is the author of such works afforded in pursuing their works as valid, relevant, factual, and requiring practical application? Again, subjectivism of authorship contributions to the body of knowledge.

What Cybersecurity Is Not

Sometimes it is helpful to understand what something is not in order to understand what something is. There is no question that cybersecurity has dominated academic, private, and public discourse. It does not take much effort to find educational programs entirely focused on delivering cybersecurity education, private entities discussions regarding the subject of cybersecurity, or public entities' concern of cybersecurity; a simple Internet query results in hundreds of search results. If we look deeper into the educational programs, conversations, and concerns, we find a few repeated themes. One is the concern of ethics and cybersecurity. *Ethics* is defined as a system or set of moral principles (Definition of ETHICS, 2020). *Morals* are defined as what is right or wrong (Definition of MORALS, 2020). We also find discussion regarding the application of cybersecurity law. As a definition, *law* is defined as binding customs, rules of conduct, formally or informally recognized by controlling authorities (Definition of LAW, 2020). The Tallinn Manual (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2020) is an excellent example of an extensive legal tract within the context of cybersecurity. Some other terminology aligned to cybersecurity includes but is not limited to Risk Management, Malware, Consequence, Invention, Innovation, Progress, Frameworks, Fear, Politics, Privacy, Enforcement, Punishment, and Intent.

The list of associated terms that connect with cybersecurity can go on-an-on. However, none of these terms are actually what cybersecurity is. Previously definitional language about cybersecurity mentioned within the course of this discussion shows that cybersecurity is the practical application of a body of knowledge concerning computer(s) or computer network(s) in a way that keeps these computational things free from danger and that their state is made certain. If we maintain this course of definitional restriction, we only reinforce that none of the connected terminologies is actually cybersecurity. Instead, they are words that label or describe doctrine, tactics, so on and so forth.

So, we can throw out most of the language used to describe cybersecurity as a thing. Cybersecurity does not require ethics, law, education, innovation, enforcement, or any other word to define it as a thing or a requirement to develop a Philosophy of Cybersecurity. We can prove the irrelevance of these words as requirements for developing a Philosophy of Cybersecurity through examples. The first example is the word ethics.

Practically speaking, ethics is not a requirement for cybersecurity exist. "How can that be?" is the predicted response from the thousands of cybersecurity practitioners. Nevertheless, it is true. Let us assume that we are a despotic dictator who is an ethically void individual and whose only goal is to remain in control over their domain at any cost. In this assumption, we will also assume that information concerning our domain is stored, altered, or transferred via cyber systems, keeping in mind that cyber systems are comprised of computers. As a despot, we have enemies. These enemies seek to exploit any weakness of our own (e.g., political, economic, social, et al.). To prevent our enemies from unauthorized access or attack of our cyber assets, we must invoke cybersecurity. To reiterate, we are despotic. We are "evil." We are antithetically

moral. However, we invoke cybersecurity? So, for cybersecurity as a phenomenon to exist, we do not need ethics to invoke it into manifestation. Purpose, yes. Ethics, no.

Another example of word irrelevance is the requirement of law for cybersecurity to exist. This example is probably easier to explain than ethics as a requirement for the existence of cybersecurity. Let us assume that we are a person who recently enrolled an account in a digital forum on the Internet. The country we reside in does not require us, by law, to secure this account with a password. However, for our personal feeling of security assurance, we create a password upon account creation. We have, at this point, invoked cybersecurity, though no law required us to do so.

But what about other aspects of cybersecurity like education and the economy? These are tangible aspects of the phenomenon. Academic institutions offer an educational curriculum that teaches students different things about cybersecurity. Economically, jobs have been created to perform cybersecurity duties. What about the emotional aspects of quality of life? These aspects, too, are tangible. Merely looking at the language used to discuss cybersecurity topics, we find words like “threat,” “vulnerability,” and “exploit.” These words may or may not instantiate emotional responses like fear from becoming insecure due to threat actions that seek to exploit cyber systems' vulnerabilities. Beliefs in improvements of one’s quality of life come through the discussion of increased assurance of security from cyber threats. However, are the educational, economic, emotional, or quality of life aspects surrounding cybersecurity make cybersecurity real? No. If a person enables a password on a digital forum, they may or may not feel more secure, as seen in the previous example. They may or may not know that a job was created to create the application's password function. They may or may not know that the job created required a particular level of education to perform. Moreover, they may or may not

know that by enabling a password, they are protecting themselves from “threats” by making themselves less “vulnerable” to “exploitation”. Nevertheless, in creating the password, they have invoked cybersecurity. It has now become manifest through a real person using a real application.

What Cybersecurity Is and Final Position

Adhering to what a philosophy is, as laid out with our previous paragraphs, we see that a philosophy is the pursuit of wisdom, exclusive of practical arts, a fundamental belief, rooted in a set of concepts. Do we need a set of concepts to begin a Philosophy of Cybersecurity, or is one concept enough? We have also thrown out the basis for law and ethics to be applied to a Philosophy of Cybersecurity as a part of the required foundational concepts. So, with these things in mind, what is cybersecurity? More importantly, out of a lexicon of words, what word can be applied sufficiently to derive a basic philosophy explaining the phenomenon via concept?

Though Deleuze and Guattari present that philosophy is not reflective, the conceptualizing and generation of a concept possibly is. Deleuze and Guattari maintain that philosophy is only embarked upon later in one’s life (Deleuze & Guattari, 1994, p. 1). The supposition is such that a person cannot sufficiently philosophize about something without enough life experience. This assertion may or may not be entirely true. However, this presents the fact that, although philosophy itself is not reflective, the development of the concepts to support the philosophy is.

If we reflect on the text presented within this treatise, we see a need for a level of abstraction in concept. Concepts that are not too precise, not too imprecise; instead, just enough to get the point across while leaving room for speculation and dialogue between the philosopher

and personae. Continuing along this line, reflecting upon some of the language used in contemporary cybersecurity discussion, we see the word *organization* contemplated and reused. But what does the word organization mean?

Definitionally, organization is defined (Definition of ORGANIZATION, 2020) as the process of organization, being organized, an association, society, and administrative or functional structure; also, the personnel of the administrative or functional structures (e.g., those who will do the work). Is this definition abstract enough to be considered worthy of concept? Possibly. There is literary reference to organization as a concept (Torgersen, 1969). The word definitely gives room for speculation and dialogue. In order to create cyber system infrastructures, IP addressing needs to be assigned and organized. To know where passwords are stored requires a level of organization of informational reference. Cataloging threats into a system taxonomy can be considered a type of organization. Legal bodies that legislate and administer cybersecurity law could be considered organizations made up of people who perform work. Moreover, still, the word organization alone remains abstract.

Therefore, the position of this treatise regarding a Philosophy of Cybersecurity is such that, in consideration of defining the phenomenon, Cybersecurity is the practical *organization* of a body of knowledge used to secure cyber things within the specific confines circumstance. In all of the literature reviewed for this discussion, there was never a quantifiable number of required concepts, simply that there needed to be concepts to create the philosophy. Here we see that cybersecurity is hinged upon the concept of *organization*.

Is this a breakthrough in the fundamental understanding of what cybersecurity is, and if so, “So what?” Firstly, and probably most *important*, by declaring the concept for a Philosophy of Cybersecurity, those who stumble upon this treatise can use it as a reference point for further

research. The reference point serves as an anchor. For example, a study on bias within cybersecurity can use the concept of organization to develop the theories for which hypothesis can be tested. Secondly, the philosophy can be challenged. A challenge to any philosophy is vital to evolving future concept creation, concept deletion, and academic discourse. Without challenge, there is concept stagnation. By creating the philosophy and concept, there is room to argue the validity of the point. Lastly, and no less profound, is the simple contribution of a Philosophy of Cybersecurity within the body of knowledge where there previously was none. In doing so, we allocate a portion within the body of knowledge that, objectively, had no other specific bibliological reference other than philosophies akin to something like a Philosophy of Cybersecurity.

References

Aleksic, A., Puskaric, H., Tadic, D., & Stefanovic, M. (2017). Project management issues: Vulnerability management assessment. *Kybernetes*, *46*(7), 1171–1188. https://doi.org/10.1108/K-08-2016-0218

Bell, D. E., & La Padula, L. J. (1976). *Secure Computer System: Unified Exposition and Multics Interpretation:* Defense Technical Information Center. https://doi.org/10.21236/ADA023588

Best Jobs in Cybersecurity for 2020 and How to Get One. (2020). Default. https://www.comptia.org/blog/the-top-9-jobs-in-cybersecurity

Burkart, P., & McCourt, T. (2017). The international political economy of the hack: A closer look at markets for cybersecurity software. *Popular Communication*, *15*(1), 37–54. https://doi.org/10.1080/15405702.2016.1269910

Clark, D. D., & Wilson, D. R. (1987). A Comparison of Commercial and Military Computer Security Policies. *1987 IEEE Symposium on Security and Privacy*, 184–184. https://doi.org/10.1109/SP.1987.10001

Cottringer, W. (2005). Adopting a philosophy on conflict. *SuperVision*, *66*(3), 3–5.

Cushman, F., & Young, L. (2009). The Psychology of Dilemmas and the Philosophy of Morality. *Ethical Theory and Moral Practice*, *12*(1), 9–24.

Cyber Security Degree Online | Earn Your Bachelor's | SNHU. (2020). https://www.snhu.edu/online-degrees/bachelors/cyber-security

Definition of AVAILABILITY. (2020). https://www.merriam-webster.com/dictionary/availability

Definition of CONCEPT. (2020). https://www.merriam-webster.com/dictionary/concept

Definition of CONFIDENTIALITY. (2020). https://www.merriam-webster.com/dictionary/confidentiality

Definition of CONSEQUENCE. (2020). https://www.merriam-webster.com/dictionary/consequence

Definition of CYBER. (2020). https://www.merriam-webster.com/dictionary/cyber

Definition of CYBERSECURITY. (2020). https://www.merriam-webster.com/dictionary/cybersecurity

Definition of DATA. (2020). https://www.merriam-webster.com/dictionary/data

Definition of DOCTRINE. (2020). https://www.merriam-webster.com/dictionary/doctrine

Definition of ETHICS. (2020). https://www.merriam-webster.com/dictionary/ethics

Definition of INNOVATION. (2020). https://www.merriam-webster.com/dictionary/innovation

Definition of INTEGRITY. (2020). https://www.merriam-webster.com/dictionary/integrity

Definition of INTENT. (2020). https://www.merriam-webster.com/dictionary/intent

Definition of LAW. (2020). https://www.merriam-webster.com/dictionary/law

Definition of MORALS. (2020). https://www.merriam-webster.com/dictionary/morals

Definition of ORGANIZATION. (2020). https://www.merriam-webster.com/dictionary/organization

Definition of PHENOMENON. (2020). https://www.merriam-webster.com/dictionary/phenomenon

Definition of PHILOSOPHY. (2020). https://www.merriam-webster.com/dictionary/philosophy

Definition of PRINCIPLE. (2020). https://www.merriam-webster.com/dictionary/principle

Definition of PROGRESS. (2020). https://www.merriam-webster.com/dictionary/progress

Definition of SECURITY. (2020). https://www.merriam-webster.com/dictionary/security

Definition of TACTICS. (2020). https://www.merriam-webster.com/dictionary/tactics

Definition of TECHNOLOGY. (2020). https://www.merriam-webster.com/dictionary/technology

Deleuze, G., & Guattari, F. (1994). *What is Philosophy?* Columbia University Press.

Dreibelbis, R. C., Martin, J., Coovert, M. D., & Dorsey, D. W. (2018). The Looming Cybersecurity Crisis and What It Means for the Practice of Industrial and Organizational Psychology. *Industrial and Organizational Psychology*, *11*(2), 346–365. https://doi.org/10.1017/iop.2018.3

Four Reasons Why Philosophy Is As Relevant As Ever. (2018, November 16). https://www.bachelorstudies.com/article/four-reasons-why-philosophy-is-as-relevant-as-ever/

Furtak, R., Ellsworth, J., & Reid, J. D. (2012). *Thoreau's Importance for Philosophy*. Fordham University Press. http://ebookcentral.proquest.com/lib/emich/detail.action?docID=3239747

Jafari, M. J., Nourai, F., Pouyakian, M., Torabi, S. A., Miandashti, M. R., & Mohammadi, H. (2018). Barriers to adopting inherently safer design philosophy in Iran. *Process Safety Progress*, *37*(2), 221–229. https://doi.org/10.1002/prs.11927

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals. *ACM Transactions on Computing Education*, *18*(3), 12.

Lackland, T. H. (1975). Toward Creating a Philosophy of Fundamental Human Rights. *Columbia Human Rights Law Review*, *6*, 33.

Lutz, M. J. (1997). Socratic Virtue in Post-Modernity: The Importance of Philosophy for Liberalism. *American Journal of Political Science*, *41*(4), 1128–1149. https://doi.org/10.2307/2960484

Marmor, A. (2010). *Philosophy of Law*. Princeton University Press.

Mehra, S., Joyal, A. D., & Rhee, M. (2011). On adopting quality orientation as an operations philosophy to improve business performance in banking services. *International Journal of Quality & Reliability Management*, *28*(9), 951–968. https://doi.org/10.1108/02656711111172531

Pring, R. (2012). Importance of Philosophy in the Conduct of Educational Research. *Journal of International and Comparative Education (JICE)*, 23–30. https://doi.org/10.14425/00.36.38

Tallinn Manual on the International Law Applicable to Cyber Warfare. (2020). http://web.a.ebscohost.com.ezproxy.emich.edu/ehost/ebookviewer/ebook/ZTAwMHhuYV9fNTI5Njc0X19BTg2?sid=299547f9-9bd8-42bd-a5e5-29d2260a8289@sdc-v-sessmgr01&vid=0&format=EB&rid=1

Torgersen, P. E. (1969). *A concept of organization*. Van Nostrand Reinhold.

Wilcox, E. W. (2015). *IF OUR SAILS ARE SET CORRECTLY, OUR PER-*. 4.