The Theology of Cybersecurity

Global Threats, Local Protections, and Ethical Obligations

By Anthony J. Elia, Bridwell Library, Perkins School of Theology, Southern Methodist University

ABSTRACT Institutions of higher learning, including seminaries and theological schools around the world, are increasingly faced with not just keeping information safe, but also needing to be proactive against external cyber-threats on a global scale. Unlike the world of twenty-five years ago, unknown actors 10,000 miles away have the potential to infiltrate, infect, hold hostage with ransomware, and even destroy our valued information. In this presentation I will address the functional, relevant, and practical questions about cybersecurity in seminaries and theological schools, along with the theological and ethical questions about being proactive stewards of cyber-infrastructure. The role of cybersecurity reaches all members of a community and can affect everything from student library accounts to the reputation of an institution. In this paper, we will look at both the practical and the theological-ethical nature of cybersecurity in theological institutions, and we will ask how we can be more engaged and better protected against potential threats.

INTRODUCTION: OUTLINING THE THEOLOGY OF CYBERSECURITY

In this paper, we will discuss two key themes around cybersecurity in the context of theology, theological education, and theological institutions. These two themes are 1) the practical aspect of having an understanding of cybersecurity at ATS and other theological institutions,

where we are aware of the threats and discuss them; and 2) that technology, and especially the question of cybersecurity, is engaged with as an academic, specifically theological, and ethical topic. Too often, in the last twenty-five years of working in theological schools and educational technology and IT, the role of technology has been relegated to the backburner, as having nothing to do with theology. Yet, I recall very clearly, perhaps the most prescient of observers back in 2006, a friend and colleague, who wrote passionately about Minjung Theology, stating that technology was a force of control, post-colonialism, and oppression, something that would certainly be central to the very modes and debates of state control, corporate power, injustice, and inequality. Now, more than a decade later, I believe that this colleague had many valid points. Of course, we don't want to be puritanical about technology, but there are surely many opinions about it. In the following pages, I will discuss some of these issues, how they have manifested, and how we can work to address these topics as members of theological communities.

TECHNOLOGY, SPEED, AND WHO OWNS INFORMATION?

What is information and who owns it? Should information be free, regulated, or manipulated? Is it already? Part of our understanding about the world is how we understand our place in that world. In the last 200 years, with the advent of new transportation technologies, the world "grew smaller." Some scholars have argued that the invention of the steam engine was by far the most significant technological advancement in human history, increasing human travel speeds more than at any other point, in distinction to the period preceding that given invention, shifting our speed of travel from months to weeks. Others have said the airplane did the same, increasing speeds of travel from days or weeks to certain places to mere hours. And then there are the inventions of telecommunications and now the internet, which though different, have brought elements of information and communication to the point of instantaneity. How do these changes in our world a) make us who we are, or even change who we are; b) inform us theologically and ethically in our places of work and life; and c) make us either safer or less safe in protecting our personal information?

WHAT CONSTITUTES CYBERSECURITY?

Why should we even write a paper on "theology and cybersecurity" and what does that really mean? Part of the issue that we may be faced with in the theological and theological library world is how to engage with not only what is relevant in the present, but what will become relevant in the coming years. There has been a tendency within our disciplines to fall behind in what the tech world offers in primary, secondary, and higher education. Why? It is mostly because technological advances and innovations don't always seem immediately relevant to what has been done in theological education and libraries. For generations, the focus on texts, exegesis, and constructive theologies has often found security in the bubble of a self-sustaining hermeneutic, one which believes it can thrive on historical stability and a legacy that has existed for centuries. This seems to be true not just in the thinking about theological ideas, but also about the pedagogical practices and applications of practical studies within these fields. But as we have quickly entered the "digital age," where every other complaint about our ills is a fixation between "boomers and millennials," or the Gnostic fantasy reflected in some mysterious "paper vs. e-something," we must as librarians and educators begin to really think about cyber-presence, cyber-theology, cyber-ministry, and cyber-security. The panoply of terms to describe online ideas, identities, expressions, and interactions is countless, but we will try to contain some descriptions for the purpose of this paper.

I have utilized specifically, and importantly, the term and idea of "cybersecurity" because I believe it is far and away the most significant area of consideration and research that should be assessed by both the administrative powers of theological schools in its practical sense (asking: "How do we keep ourselves, our institutions, and our community safe in the present cyber-saturated world?") and in the theological and ethical sense: (asking: "What are the theological and ethical implications of how we do any form of theology and ethics, including ministry, exegesis, preaching, etc. in the present and future age?"). If we are not doing this now, and neglect to ask these questions, either as libraries/librarians or as theological schools and accrediting bodies in the next few years, we will be not only doing a disservice to ourselves and our communities, but we will be negligent to our commitments in cultivating real communities of vocation seekers.

We live in a world where social justice and its accompanying language plays out online in forums and discussion threads, as well as in Facebook posts, in raw, unaltered forms, and yet rarely is the format and contexts of this meta-form exegetically analyzed itself. We want to speak our minds, while having our privacy, yet we post constantly about the most revealing aspects of our personalities, habits, opinions, and political ideologies. And in those spaces, we fight against oppressions and racism, sexism, ageism, and other senses of injustice, yet reveal both our own biases, as well as the biases of technological systems, search engines, and algorithms (see Safiya U. Noble's new book *Algorithms of Opression: How Search Engines Reinforce Racism* for further details), which eventually are collected, reviewed, assessed, and commodified, whereby we become objects of monetary value, used and abused by third parties, companies, states, and other unknown actors.

FIRST CONSIDERATIONS: PRIVACY AND OWNERSHIP

Cybersecurity is one of the most pervasive, broadly misunderstood, oft feared, and completely necessary terms in the 21st century; likewise, *theology* is perhaps one of the least pervasive, broadly misunderstood, oft feared, and certainly necessary terms for a select group of individuals in the world of academics and religion. What then are the most important considerations (practical, theoretical, and theological) for us, and why is this paper necessary for us and our communities?

As we think about these ideas and how they fit together, it will be beneficial to begin with questions about "information," as mentioned earlier: what constitutes information, how we work and deal with information, and even how information has influence upon us. Primarily, though, the technology, speed, and ownership of information are vitally important. For example, we know that technology grows at certain rates, we know that technology is responsible for the speed at which information is carried and delivered, and we know that technology plays a role in both "shared" and "owned" information. In effect, we know that all of these elements are integral to how things operate in the world, but we also know how this functionality impacts some of the most vital operations in things like medicine, law, information technology, and business, among many other fields.

What is perhaps most important among these terms is "ownership." The role of who has propriety over information is key to what we might call the "new holy trinity" in global communications: technology, ownership, and privacy. Though not exclusively the same, propriety and ownership have linking roles, and both are important to how we connect both technology, broadly speaking, and the meaning of privacy—a term which is often confused with "personal." Privacy has been defined as more relational than the word personal in English. In fact, the term "privacy" has its roots in meaning "state of freedom from intrusion" dating back to the early 19th century, in contrast to simply meaning "the self."[1] Certainly, the nuances of these terms may be debated further, but for our purposes, these distinctions are helpful as we try to better understand the role of privacy, technology, and the ownership of information.

This leads us to the question: "Who owns what information?" The people, the government, third-party entities, companies, or others? As we've come into a new age, the "digital age," we have encountered new problems. The introduction of enhanced and networked technologies, for example, has led to a change in how we perceive, interact, and recognize privacy, and ultimately ourselves. The history of cybersecurity might prompt us to consider how information has been utilized, protected, or even manipulated for various reasons. Over the years, since the 1960s, the development of computers and networks has led us into a realm that has changed and about which there has been growth in areas good, risky, and even bad.[2] As some cybersecurity specialists have warned in recent years, the internet is not completely safe, because when its foundations were built, no one thought that most people would be shopping online, let alone that they would need to guard against cyberwarfare attacks. In recent years, we've heard many reports about what preparedness the U.S. government had in the late 1990s and early 2000s leading up to the 9/11 attacks. One such tale describes the utility of government computing as grossly inadequate, lagging behind nearly a decade, including a description of the situation then FBI director Robert Mueller faced in late 2001, where the technology was not adequate enough to complete basic email attachments, in order to send confidential materials across the country. Indeed, the story goes that such information had to be sent by an actual agent personally flying from one city to another.

As we address the histories of technology, we will also need to keep in mind the roles of privacy, which are part of that trio I spoke of earlier (i.e. privacy, ownership, technology). The role of privacy has been central to how libraries and other social agencies have operated for at least eighty years. In 1939, the American Library Association's Code of Ethics declared the "right to privacy" as part of its core values. In the period subsequent, especially from 1958 to 1974, multiple privacy cases were taken up within state and federal government agencies, in order to clarify where people had rights and where their rights were being infringed upon (e.g. *NAACP v Alabama*; *Griswold v Conn.*; *Katz v US*; and the *Privacy Act of 1974*). Privacy rights were even tested in the case of a Colorado county attorney, who claimed that library records were actually *public*, after a journalist sought the borrowing records and reading history of John Hinkley Jr. (Reagan's would-be assassin) from a public library. The decision was later overturned, though, for obvious constitutional reasons.[3] A later issue, prompted by U.S. Supreme Court nominee Robert Bork's hearings, led to a journalist seeking personal (and private) videos of his family in 1988. These cases overlapped with the "borrower card dilemma," which was the issue that many libraries in the 1980s had to deal with—where many end-of-book borrower cards contained personal borrower data (e.g. who borrowed what books and when). This also coincided with the development of databases, which recorded personal data that was held as secure data by institutions and libraries. As a result of some of these changes, the borrower cards were either removed or marked out by large and heavy inked black markers to ensure personal privacy. Some legal specialists have noted that both of the high-profile cases of Bork and Hinkley contributed to the question of what constitutes a public record in libraries. But the role of technology must also be considered, specifically during the early years of technological change in libraries and telecommunications. This coincided with the rise of the internet in the 1990s and ultimately the need for cybersecurity.

But these bring up at least two related stories and dilemmas that I want to share: 1) In 2008 I discovered that a book by famed scholar Irving Babbitt (ca. 1915) had a borrower's card detailing the borrowing history and had been checked out to the well-known church historian Martin Marty—back in 1954! I contacted Marty and had an excellent conversation about the book. In retrospect, I probably should not have

contacted the borrower, even if it had been more than half a century earlier, but it helped with the research I was undertaking at the time; and 2) In 2012, a professor from a major British university contacted Columbia University to ask who had consulted with a sixteenth-century volume in special collections. It was to help prove an intellectual history of a twentieth-century scholar, who made claims on certain historical themes, supposedly based on this early modern text. After consultation, the Columbia University Library's legal and copyright team did not allow for library staff to provide that information, which we weren't going to provide anyway, but said that the professor could come to the United States and view the material in person, basically giving passive permission to "see the book." Both situations were problematic on different levels, as there was a tension between what constituted historical and even "archival" research with privacy laws and protocols. I provide these encounters to help demonstrate the greater issues of privacy and the grey areas that prompt questions about the limits of this kind of historical research.

THEOLOGY, TECHNOLOGY, AND SECURITY: OR, HOW DO WE UNDERSTAND CYBERSECURITY

There are multiple terms that we might consider when looking at the current situation of cybersecurity and theology. These include privacy, education, technology, media, social media, institutional privacy, seminary IT, hacking, and safeguarding. Each of these plays a role in the way that our institutions operate, as well as how we need to look forward as proactive stewards of our communities. Cyberattacks constitute a major threat to our society, but what is less known by the general public is the percentage which is caused by us, the human actors. The general estimate is that around 95% of cyberattacks are based on careless human error, which come in the forms of poorly secured personal information or exposing one's private information in places like coffee shops or even in online forums of social media. Many of our behaviors are manifested as personal actions (things we do) versus digital actions (things our technology enables), and these can be further distinguished by types of information, all of which are important to either keeping safe or being risky and opening ourselves up to intrusion and cyberattacks. Some of the areas that we must be cognizant of include[5] 1) physical information (computers,

mobile and storage devices, printers, and white/chalk boards); 2) digital information (email, login credentials, authentication devices and portable drives, and browsing windows histories); 3) primary information (those things that cybercriminals are looking for to do optimal damage, such as bank information and Social Security numbers); and 4) enabling information (e.g., passwords). Breaking down types of primary information, we can include a) personal information (date of birth, driver's licenses), b) sensitive information (Social Security number, tax ID), and c) organizational information (intellectual property, research information). Unauthorized access to any of these can do irreparable harm.

What is important here, though, is that seminaries and theological schools need to recognize these kinds of information, as well as the safeguards that must be involved in protecting their students, faculty, and staff. There are many types of cyberattacks, as well as *cyberattackers*—not all of whom are necessarily bad.[6] More importantly, or perhaps more invasively, we have those actors in the world who are looking to and at our information for multiple reasons. Those who have been identified by McAfee Labs as "Info-Gathering" actors include 1) *The Media:* which use information to sell stories; 2) *Private Investigators:* who use information for a legal case; 3) *Debt Collectors:* who use hacking to track debtors; 4) *Insurance Companies:* which use information to adjust premiums; and 5) *Consumer Businesses:* which may sell "aspects" of information for profit.[7] Furthermore, there are multiple ways of "angling" to get people to divulge their personal and private information, and many of these are successfully employed globally but not always recognized by those who become victims of the crimes. These come in both technical and non-technical categories. (Again, these all are detailed in the Southern Methodist University data and security orientation site).

Technical

1. Phishing: using crafted emails to bait broad groups and gather sensitive data
2. Spear Phishing: using crafted emails to target employees of a specific company
3. Whaling: using emails to target high-ranking or high-profile individuals for sensitive data

4. Pharming: spoofing a website to capture personal data
5. ID Theft: impersonating someone to steal information, money, or credit
6. Privacy Invasion: acquiring and selling personal data to third parties
7. Malware: intrusive and damaging software providing data to thieves
8. Man-in-the-Middle: intercepting communications b/w parties online

Non-Technical

1. Dumpster Diving: going through trash to steal information
2. Shoulder Surfing: looking over shoulders to steal personal information
3. Pretexting: Researching and baiting a person to steal data/information
4. Mail Theft: Stealing from mail to gain information

Having reviewed some of these issues, problems, and approaches to cybersecurity and cybercrime, it is important now to understand best practices. In short, some of the examples that cybersecurity experts provide include, above all: (a) being very careful and aware of our surroundings and our stewardship of personal and private information; (b) using complex and multiple passwords, including those that might not even make sense (e.g., "place of birth?" = "Chicken Soup"), so that suspecting thieves will be way off track when attempting to make guesses; and (c) implementing and using two-factor authentication, which is in use in larger organizations and universities.[8] These practices won't guarantee our safety against attacks, intrusion, or identity theft, but they are key strategies for our basic protection.

INFORMATION ECONOMIES: HOW SOCIETY AND OUR INSTITUTIONS FACE ONE ANOTHER

When looking at cybersecurity from the standpoint of institutions, especially theological schools and seminaries, there has been a long tradition of separating the tasks of theological education from the

practical aspects of everyday work in the office space, library, classroom, and chapel, among all the places and spaces that make up such institutions. But it is necessary to think about this topic in a far more targeted, and far more serious way, where we must bring together the theological with the technological, not just as actions of training and knowledge, but as philosophical points of discussion.

Information Technology is central to the operation of almost any institution, and seminaries are no exception to this. Academic, Educational, and Information Technologies are part of the core of our operation, whether or not it is readily recognized by our colleagues and administrators. So too, then, is cybersecurity and cyber-infrastructure. Instead of being merely physical aspects of allowing us to operate, these concepts and ideas must be taken seriously as part of our challenge in understanding the world in which we live, work, worship, practice, teach, and learn. How prepared are our schools with "general plans" of digital security with in-house or outsourced IT departments, and what do we know as members of these communities? What trainings are required in terms of safeguarding our information and proper online etiquette that doesn't expose us to the risk of cyberattack? Do we ourselves or our schools assume that we won't be targets of such attacks, and if so, why is this the case? Many schools assume the mode of "we are too small" or "who wants our data or information anyway?" This, we should recognize, is the wrong, and ultimately dangerous and costly, approach.

Another area that we need to be aware of is "digital tracking" and "digital phenotyping." *Digital Tracking* involves how we leave innumerable data points on the internet, mostly through social media and mobile devices. Our phones can tell how many steps we've walked, how many times we've checked our accounts, who we've met, when we've eaten, who we've called or texted, and even the content of these interactions. We are prompted with possible "you might like…" items for purchase on Amazon or other e-commerce sites, or sent coupons from Starbucks, if you even walk by a store, because your geo-location was tagged by your phone and shared across multiple apps you may have had running on your device at a given time. *Digital Phenotyping* takes this a step further and has recently been defined by Harvard scholars and others as "a catch-all term for the trail of relevant health data people leave behind in their interactions with the internet, social

media, and technology, which has largely untapped potential for the early detection of various conditions."[9] Though there are positive aspects to what this means, there are other potential risks in how we are tracked and analyzed by external entities—as Shoshanna Zuboff calls this cleverly, "Big Other." This term is a nod to the older expression of "Big Brother," but is more amorphous, because we are even less aware of what is tracking us, or even why we are being tracked and categorized. Some potential issues of digital phenotyping (positive and negative) may include the following:

1. Predicting a health issue that goes undiagnosed (e.g., grandfather in Facebook photo whose photo was seen by a medical doctor, who saw skin cancer; child whose eyes displayed a rare disease/condition to an eye doctor);
2. Targeting individuals with social media data points, which may indicate risk factors and be identified by firms or companies dealing with medical support;
3. Potentially feeding into medical insurance firms any information that has been picked up by algorithms or social media aggregation;
4. Creating an inaccessible and unknown "phenotype" of you to be used in a variety of ways, including financial risk (e.g., credit score).

Considering all of these points, we must recognize the potential risks and threats around keeping our personal and private data and information safe. At the same time, we need to look to how we can best cultivate both an environment and a culture of cybersecurity awareness in our theological institutions.

THEOLOGY OF CYBERSECURITY

In all of what we have covered, there is really one main question that we need to consider: What is our moral and ethical responsibility in theological education surrounding cybersecurity? This is where "digital ethics" comes in. Digital ethics can be defined as "how users and participants in online environments interact with each other and the technologies and platforms used to engage with one another." But, I would also add that digital ethics includes the moral duties of those

users to be good community members in that usage. My own definition of digital ethics in 2018 is "the practice of how we live and work in the new paradigm of online environments, especially how we represent ourselves honestly and take responsibility for both our actions and our participation in communities, but also about our stewardship, and our ability to model good, safe behavior, as we are cautious and protective of our personal assets."

Our behaviors and ethics are also tied to what will constitute a theology of cybersecurity. It is necessary for us, as members of a global community of users and believers (in whatever our traditions may be), to look at the following questions, and ask ourselves how we can best work to better ourselves and communities in the world we now live in. These points are what I consider the theological principles about technology, information, and cybersecurity, and they should be used as guides to our work, ministries, and daily operations in communities, congregations, and theological institutions.

1. How do we understand social power structures in light of cybersecurity?
2. How can we as individuals and communities recognize the role of privilege present in cybersecurity and what does that actually mean?
3. How do socio-economic divisions in society play into knowledge and best practices of cybersecurity, and do certain communities suffer more/less depending on the access and awareness of certain information?
4. How can we speak both historically and prophetically about these themes?
5. What justifies best practices in the "blessed community" and the technological-informational community?
6. Where do we seek guidance and dialogue about the theological implications of an increasingly complex cyber- and tech-world?
7. Denominationally, what is the way to talk about cybersecurity and religion, and what is actually being said and done? What more can be done?
8. Can we effectively use our theological lexicons (e.g., on sin, redemption, grace, and salvation) in this realm of cybersecurity? How so?

As we near the end of this discussion, I think that it would be beneficial to offer at least an initial working definition for the "theology of cybersecurity." I provide this as a way for those in our broader community of theological educators, students, learners, administrators, staff, and others to begin to think constructively about this topic and work toward a better, safer world for ourselves and our communities.

Theology of Cybersecurity is "**the active engagement with our world's contemporary issues of technology, security, and information, through the lens of God's grace, community, and love, in order to cultivate the ethical stewardship, safety, and stability of creation.**"

And with this definition, a roadmap for our institutions then should be what we call the "SAFE" rubric: S(tandardize), A(ssess), F(oster), and E(nact). It works in the following basic way:

1. **Standardize** regular trainings about cybersecurity and safety in seminaries and other institutions;
2. **Assess** on a regular basis the tools and trainings about these topics and determine what works best;
3. **Foster** a community of open discussion and debate about both the practical issues of technology, information, and cybersecurity AND the theological language, implications, and meaning connecting these two areas of intersection;
4. **Enact** the outcomes of these discussions, debates, and conversations about both the practical trainings AND the theological discourses at your institutions—DON'T LET THEM FLOUNDER!

With these basic guidelines, I hope that you and your theological institutions may work toward a community of greater safety, growth, and hopefulness.

NOTES

1 https://www.etymonline.com/word/privacy

2 The history of important advances includes: 1969- first networked computer (ARPANET); 1971- Ray Tomlinson sends first email; 1991- first website/page; 1992- First attachment in email sent; 1993- first PDF; 1996- official release (public stan-

dard); 1997- first social media site "Six Degrees;" 1996-2000- US government establishes Y2K protocols; 2000-2001- several of the first major cyber-attacks on US government (cited: http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26_3.html); 2002- 200% increase in cyber-related security incidents; 2002- in November, President Bush signs Cybersecurity Research and Development Act—nearly $1 billion for cyberinfrastructure.

3 https://ttu-ir.tdl.org/ttu-ir/bitstream/handle/2346/1529/Privacy-AndLibrariansAnOverview.pdf?sequence=2

4 https://www.loc.gov/law/find/hearings/pdf/00183854811.pdf

5 Much of the security and cybersecurity prevention discussion is drawn from training material at the Southern Methodist University's authentication services.

6 According to the SMU site plan on cyber-safety, these are some of the types of "hacker" that are out there: (1) Script Kiddies: Unskilled Hackers Impressing Friends; (2) Hacktivists: Activists Using Hacking for Political Goals; (3) Lone Hackers: Independent Individuals Motivated by Fame or Profit; (4) Organized Crime Hackers: Gangs Attacking Governments or Corporations; (5) State Sponsored Hackers: Bureaucratic Hacking Groups (e.g., Stuxnet malware); (6) Terrorist Groups: Hackers Associated with Terrorist Groups.

7 See SMU authentication and security orientation materials.

8 See SMU authentication and security orientation materials.

9 http://www.mobihealthnews.com/43327/harvard-doctors-argue-the-digital-phenotype-will-change-healthcare