The Interdisciplinary Impacts of Technology Semantics and Communicational Bypassing in the Cybersecurity Field

Brooke Nixon
Christopher Newport University

The Interdisciplinary Impacts of Technology Semantics and Communicational Bypassing in the Cybersecurity Field

By Brooke Nixon[1]

Work for this paper was supported by the Cybersecurity Undergraduate Research funded by Commonwealth Cyber Initiative (CCI). The author wishes to express her gratitude to CCI Coastal Node for the grant received.

Table of Contents

[1] Brooke Nixon is a junior at Christopher Newport University, Newport News, Virginia. This paper was supervised by Professor Iria Giuffrida, William & Mary Law School, Williamsburg, Virginia.

Introduction

In 2012, former director of the Federal Bureau of Investigation (FBI) Robert Mueller shocked many when he warned, "[t]here are only two types of companies: those that have been hacked and those that will be." As technology and information systems develop rapidly, security has become a topic of increasing interest and concern. In 2018, it was noted that the total cost to account for cybercrime on a global scale surpassed US$1 billion (Milkovich, 2020). In the United States, a hacker attack occurs every 39 seconds, and each year, 1 in 3 Americans are personally impacted by a form of hacking (Cukier, 2007). Given more than 77% of organizations do not have a cyber incident response plan in place to respond to such attacks, these statistics are perhaps unsurprising; yet, they speak to the desperate need for consistent, reliable, and thoughtful cybersecurity now more than ever.

Further than importance, cybersecurity is a unique field in its interdisciplinary nature. Recent cyberattacks have impacted every type of organization from industry leaders like Facebook, to small local businesses or online shops. As businesses, homes, and individuals continue to shift to digital and technologically advanced models and modes of accomplishing anything from playing music to storing corporate finances, security components frequently lag behind. A driving factor in this challenge is the pervasive implications it has on other disciplines. For example, U.S. legislation is inconsistent in regulatory laws and enforcement of cybercrime (Kosseff, 2018). Some attacks such as the one that was launched on Sony Pictures in 2014 insinuate acts of terrorism and silencing of free speech at the hands of foreign adversaries (Hess, 2015). Yet, not all attacks are the same. A wide spectrum can be delineated showing that cyberattack objectives can stem anywhere from achievement of personal goals, to financial gain, to activism, to a simple challenge depending on the perpetrator (Lehto, 2015). As such, there are ramifications noted in legal, sociological, and ethical views, among others.

Outside of the technical component of keeping networks secure, technology and cybersecurity is a unique field in its use and constant need in society. In recent years, there has been a notable effort for markets to push devices and applications that are usable and applicable to vast amounts of people. For example, Apple technology intentionally deploys a marketing strategy to target a variety of ages and demographics (Puslos, 2018). Whereas companies often rely on marketing strategies aimed to the specific demographics that their product is geared

towards, the technology industry makes a deliberate effort to push for all people to be digitally active. However, this presents its own obstacles.

First, technology is being used on a daily basis by people in different disciplines and with varying degrees of technical literacy. As such, the adverse consequences disproportionately affect those with less technical literacy. Technology can threaten individual's autonomy, cause harm to financial welfare, and violate privacy rights, resulting in a troubling link moral contention (Cole & Banerjee, 2013; Laczniak & Murphy 2006). Thus, clear communication with and within the technology sector is crucial; its unique pervasive and interdisciplinary nature will continue to present and grow in obstacles if not addressed. This paper will address the applications of such communication strategies through the impact and role of semantics and bypassing, practical applications to address previous issues seen from cybersecurity, and interdisciplinary case study applications of the topics.

The Peaks and Pitfalls of Communication

Communication is a pervasive and dynamic field, but also one that has been ever more complex due in part by the growth and ubiquity of technology as a means of communication. An undeniable challenge exists within the intersection of the communication and technology fields, particularly in cybersecurity. Simpson & Murphy (2016) note that the impact of technology on communication has created particular challenges with regard to law, social justice, and multi-user platforms like social media. These challenges encompass vast impacts from understanding intended meaning, to security and privacy. Indeed, even every-day forms of communication like email and text messages are capable of carrying negative implications from a semantic perspective. A study conducted by Roghanizrd & Bohns (2017) found that face-to-face communication was thirty-four times more likely to garner a positive response from both strangers and acquaintances in comparison to email communication. This was attributed to factors like non-verbal cues and physical touch that come solely from in-person meetings, as well as a greater potential for the misinterpretation of words seen on a screen (Roghanizrd & Bohns, 2017). Relatedly, Byron (2008) found that receivers of emails in an industry setting were more likely to interpret neutral syntax as negative rather than neutral or positive due to a combination framework of challenges in non-verbal communication, emotion and perception, and computer-mediated communications.

While effortful, the difficulties posed by barriers to communication can be managed. Haney (1992) outlined 4 different types of bypassing strategies applicable to technology and communication. Bypassing occurs when two or more people hear (or read) the same content, but interpret it differently (Haney, 1992). Humans have natural tendencies to assume their individual understanding and viewpoints are correct, so it is not unreasonable for one to then assume that words they use would mean the same thing to another person as they do for them (Nudds, 2009). This phenomenon also encompasses semantic misunderstandings due to word choice. Common examples of this can be seen in saying something as specific "sneakers" rather than "tennis shoes," or vice versa, or even words and phrases that may be common slang in some areas of the world, but not others, causing confusion over the contextual meaning. These natural tendencies can be frequently traced back to the use of heuristics, or the cognitive tools based on individual past experiences that help one to make quick decisions needed for everyday life interactions and judgements (Tversky & Kahneman, 1974). For example, rather than looking through an entire long menu of choices at a restaurant, one may opt for a meal previously enjoyed to save time and energy. While heuristics allow us to save cognitive effort for smaller decisions, they can also be too heavily relied on in more complex cases (Tversky & Kahneman, 1974). For example, an overreliance on one's own experience and judgements with regard to a political perspective can cause a bypass from learning or acknowledging important facts or other viewpoints. Thus, bypassing is rampant in everyday communication, and frequently unknown by those who experience it (Connor, 1991). Thus, it is worthwhile to elucidate factors that contribute to bypassing in an industry setting.

Haney (1992) notes that bypassing is commonly caused by two assumptions: first, that words have mono-usage, and second that words have meaning. The first of these accounts for the common assumption that words only hold a single meaning (i.e. chair can refer to a position of leadership, such as a committee chair, or an object, such as a chair at a desk). A multi-meaning word such as this, technically known as a homonym, is particularly prevalent in the English language with 1 in 10 of the most frequent words in the language being examples (Parent, 2012). When one uses a homonym in a chosen context, the understanding that it can mean something different still exists, but it is often not acknowledged or considered by the speaker during the conversation. This can commonly lead to confusion on the receiver's end. The second contributing factor to bypassing is that words have meaning. While humans naturally rely heavily on non-verbal cues that serve as additional carriers of a semantic message, words themselves carry their own

independent meaning. When this is disregarded or an overreliance on non-semantic cues occurs, bypassing is frequently seen. When people (typically inadvertently) make assumption on words based on, fully or in part, non-verbal cues, there is also a risk to bypassing (Haney, 1992). While these can be used to facilitate meaning, techniques like paraphrasing and sensitivity to contexts (see below) are necessary to confirm meaning on the words alone.

In addition to these unintentional factors, bypassing can also occur deliberately. When one uses language to deliberately mislead or miscommunicate, the speaker is culpable of deliberate bypassing, or double speak (Orwell, 1964). This phenomenon can take forms such as industry specific jargon or inflating language to make it seem impressive, both of which have the potential to confuse a listener (Lutz, 1989).

Haney's 4 key correctives to bypassing

While a recognition of semantic challenges such as bypassing is important, knowledge without application is futile. An undeniable challenge exists within the intersection of the communication and technology fields, particularly in cybersecurity. Haney (1992) suggests that the four strategies to combat bypassing are rooted in paraphrasing, approachability, sensitivity to contexts, and being person-minded rather than word-minded.

Paraphrasing is a form of active listening, which manifests when asking a speaker for clarification on the points made by summarizing and restating the same concepts using different words. This is an idea that has long been utilized and found effective. According to Weger, Castle Bell, Minei, & Robinson (2014), paraphrasing before speaking is one of the three key elements of active listening which has been linked to social satisfaction and increased feelings of being understood. Coupled with asking clarifying questions, this concept is an effective method to avoid bypassing because it provides frequently needed clarification and confirmation of understanding before delving deeper into a conversation.

Haney (1992) defines the next strategy to combat bypassing as approachability. In this context, approachability involves being receptive to verbal and nonverbal feedback. This can be seen as a heightened awareness of the messages one may communicate unintentionally. Morreale et al. (2007) states that these messages may be through occulesics (use of eyes), hepatics (use of touch), and vocalics (use of voice), among others. Indeed, a study conducted by Mehrabian &

Ferris (1967) found that 93% of communication effectiveness is determined by non-verbal cues: a stark reminder that one's approachability does indeed play a key role in correcting bypassing.

Sensitivity to contexts refers to the proposition that being aware of the verbal and situational context in a communication exchange prevents bypassing (Haney, 1992). For instance, using overly sophisticated language when speaking to a young child, or even someone unfamiliar in a particular industry, will frequently cause misunderstanding or lack of understanding from a verbal context. The situational context also plays a key role in this; if a communication is occurring at a busy time, like while setting-up an event, or late at night when fatigue may be present, the context would encourage a more succinct and simple communication exchange. Thus, it is crucial to be aware of the contexts in which communication is occurring to prevent bypassing.

The final corrective measure of bypassing is having a person-minded rather than a word-minded approach (Haney, 1992). Just as a word can have multi-meaning independently, different words can be interpreted differently depending on the person. For example, "down time" for some could refer to resting and watching television, whereas others could view it as cleaning or working on a creative project. When one prioritizes understanding what a concept means to an individual person rather than focusing on the word or phrase itself, bypassing is frequently avoided (Haney, 1992). Doing so often requires utilizing the other outlined strategies of corrective bypassing, such as query and paraphrase to clarify a person's idea of a word. With this delineation of correctives to bypassing, this paper now moves to explore practical applications in an industry setting.

The 2014 Sony Attack

To elucidate further the ideas discussed above, the analysis now turns to real-world applications and implications of semantics in the context of cybersecurity. To do so, it is helpful to review modern-day examples of cyberattacks to gain a fuller picture of what these issues look like. A particularly relevant case study is the 2014 high profile attack on Sony Pictures.

Founded in 1989 as a spin-off to the Coca-Cola owned company Tri-Star, Sony Pictures quickly became a leading company in filmed entertainment both in the United States and world-wide (Sony.net). In the fiscal year 2017 alone, their sales surpassed US$9 billion, and their film franchise includes acclaimed series such as *Men in Black, Spider-Man,* and *The Karate Kid* among others (Sony Corporation, 2018). The United States' headquarters of Sony Entertainment (a subsidiary of Sony Corporation in Japan) is based in Los Angeles County, California. With both a

U.S. and international presence, Sony was long regarded as a respected, influential, cutting-edge corporation. However, in 2014, much of this reputation was altered permanently.

On November 24, 2014, hackers overtook Sony's network and installed malware that wiped thousands of hard drives and servers, stole vulnerable and valuable data, and rendered the company's machines and network useless (Kosseff, 2018). What had once been considered a leading technological corporation was, in just one hour, set back to communicating through fax machines and paying its employees using paper checks. To fully understand the depth of this crash and the cyber, semantic, and legal implications that followed, it is first worth examining what happed three years prior, in April 2011.

From April 17 to the 19, 2011, Sony's PlayStation network and Qriocoty services—responsible for storing over 77 million users' data and allowing gaming consoles to access their devices—were hacked, compromising all of the data stored within them and hindering users from accessing their accounts (Richmond, 2011). Sony, having very few information security specialists out of thousands of employees, was unprepared. It was forced to shut off its systems for 23 days, and later admitted that personal data from each of the 77 million accounts stored had been compromised. Criticism over the company's response was quick to follow from consumers and government officials alike (Bonner, 2012). Sony waited until April 26 to inform the public of the data breach, citing that it had to bring in outside experts to determine the scope of the severity of data lost (Richmond, 2011). In addition, it was unable to confirm confidently what data were compromised. Sony later admitted that both personally identifiable information as well as possibly credit card and billing account information was compromised, but this was not immediately shared with consumers (Bonner, 2012). There was additional criticism regarding the lack of encryption and encryption sophistication Sony's systems had, and the lack of security protocols and measures put in place to adequately respond to cyberattacks (Kosseff, 2018). Outside of consumer concern, government officials ranging from the U.S. House of Representatives to British Information Commissioners Office, among others, expressed concern and critique over Sony's lack of information security (Bonner, 2012). The data breach cost Sony nearly US$171 million, and lawsuits in the U.S., Canada, and the United Kingdom followed (Kosseff, 2018). Despite the financial and reputational losses suffered, the 2014 hack reveals that the changes made by Sony were minimal and the security measures implemented proved insufficient.

On Monday, November 24, 2014, around 7 a.m. Pacific time, Sony faced a debilitating and permanently destructive cyberattack. Kosseff (2018) describes the attack from the employee perspective as, "employees logging on to its network were met with the sound of gunfire, scrolling threats, and the menacing image of a fiery skeleton looming over the tiny zombified heads of the studio's top two executives" (p. 990). Before Sony was able to respond to the attack, the hackers had successfully wiped half of Sony's global network – hard drives and data stored both in California and across continents – and overwrote the affected computer's startup software so they were unusable. Not only was data forever deleted, the hackers also stole highly sensitive information including salary data, inappropriate emails about celebrities, and other confidential information (Kosseff, 2018). The financial implications were tremendous: approximately US$35 million to investigate and remedy the attack itself, and another US$15 million in settlement of class action lawsuits (Kosseff, 2018). Reports followed stating that had Sony implemented common security measures available at the time of the first attack, the second hack could have been prevented (Rosenthal, Ushe, & Magaya, 2016). The media was also quick to note a 2007 comment from a Sony executive stating that he would not invest "$10 million to avoid a possible $1 million loss" (Holmes, 2007). This comment is a prime example that demonstrates a systematic lack of businesses' understanding and knowledge regarding cyber risks.

Commercially, it may appear to make more financial sense to respond reactively rather than proactively; however, the costs and losses from a cyberattack are frequently of a more significant magnitude than anticipated. Mere estimations or plans for cyberattack losses are futile for companies: there is no plausible way to effectively estimate or account for what form an attack may take of the losses that may accompany it.

Another facet of criticism for the second attack was the lack of preventative response following the 2011 PlayStation hack. Despite numerous legal proceedings and lawsuits filed, the resolution of them centered around financial compensation rather than required preventative measures (Stiegler, 2017). It would seem that Sony implemented few, if any, preventative cyber regulations. This reveals a deeper layer to bypassing: not only was there a lack of communication among Sony's executives as to how to respond to an attack, but an obvious disconnect between the legal and cyber disciplines. With relentless growth in the past decades, there has been substantial effort put forth to address the legal implications of cybercrime (McNicholas, & Angle 2020). While every state has individual laws that address the unlawful conduct linked to breaches

of cybersecurity, there is a lack of uniformity and active status within them. There have been legal efforts at the federal level put forth by the Federal Trade Commission (FTC), but most only address specific privacy and cyber concerns, and are sectoral (McNicholas, & Angle 2020). Since 2002, the FTC has brought enforcement actions to 65 companies found to have failed at putting in place necessary and reasonable security measures. However, these actions extend only to the specific sectors covered by the current patchwork legal framework. For example, the Health Insurance Portability and Accountability Act ("HIPPA") imposes, among others, cybersecurity obligations to protect the health data of patients and business associates in the healthcare industry specifically (McNicholas, & Angle 2020). Similar types of reasonable regulatory requirements for large scale companies like Sony are largely notional, which was viewed to be a contributing factor to their 2014 cyberattack.

Sony's 2014 hack also shows the dangers of cyberattacks beyond the scope of financial loss. In addition to the tangible losses and costs, the Sony attack had a direct impact on U.S. citizens and officials whether they were affiliated with the company or not. A month after the attack, the United States issued a statement stating that North Korea was responsible for the attack as a main motive was to retaliate against Sony's planned release of the movie *The Interview* (Kosseff, 2018). The fictional movie featured a plot involving an assassination attempt on North Korea's leader, Kim Jong Un (Trautman & Ormerod, 2018). In response, then President Barak Obama imposed sanctions on North Korea stating they were caused by "North Korea's ongoing provocative, destabilizing, and repressive actions and policies, particularly its destructive and coercive cyber attack on Sony Pictures Entertainment" (White House, 2014). The hackers continued to threaten physical violence at showings if the release moved forward, resulting in Sony cancelling the release in theaters (Trautman & Ormerod, 2018). Some sources, such as the Security Ledger, suggest evidence that instead points to 6 independent hackers with vendettas against Sony as the ones responsible (Roberts, 2014). The U.S. government has maintained its belief that North Korea is responsible, however, in either case of liability, the interdisciplinary impact affected political and societal viewpoints on foreign nations. Some even voiced their concerns that the actions rose to the level of allowing foreign censorship in the United States (Kosseff, 2018). Consequently, the hacking not only took a toll on Sony's finances and public perception, but stretched to have a chilling impact on free speech by giving a foreign country a symbolic victory over the United States without ever having a physical presence in the country.

A final challenge to be noted with the Sony hack is linked to the semantic and communication challenges that accompanied it internally. As an international company, Sony depends on streamlined communication that accounts for time and language barriers for senior leadership and other managers scattered around the world. With company headquarters in Tokyo, Japan, the attack taking place in the United States, and 51 other office locations across 38 countries, the bypassing barriers seen in the aftermath were calamitous (Sony.net). In an interview on the one year anniversary of the attack, one employee described, "[e]verything was so completely destroyed. It was surreal. *Everything* was down… It wasn't just one system or one part of the lot or one building. The network was *completely* chewed up by the virus." (Hess, 2015). The attack decimated the company's phone directory, voicemail systems, and company internet access (Kosseff, 2018). If communicating across the globe was challenging before, it seemed next to impossible after. When examined under the auspices of Haney's (1992) correctives to bypassing, all four outlined measures were unfeasible in the circumstances. Paraphrasing and approachability were limited by language barriers, disparate location, and pressing time constraints making the use of translators challenging. Sensitivity to context was burdened due to a constantly evolving understanding of the causes of the attack that was forced to come from an outside team Sony brought in to investigate. The people-minded approach was limited by not only the variance in language, but also in the divergent systems and structures for storing data at individual offices.

The 2014 Sony pictures hack present multitudinous applications of the disconnect between industry professionals and business leaders regarding investment in cyber protection, the impacts cyber-attacks can have across disciplines, and the rooted semantic communication obstacles often embedded in such cases.

Conclusion

As technology continues to be one of the most rapidly developing fields globally, consistent and reliable cybersecurity is indispensable. A naturally interdisciplinary field, the negative implications stretch across industries and levels of technical literacy. As such, communication is a crucial facet of successful security. Semantics have the potential to perpetuate or hinder such communication. Haney (1992) proposes aspects of bypassing that occur when different people hear the same content, but attribute different meanings to it. Noting and applying corrective measures to bypassing has the potential to be a key step in mitigating communication

challenges in the cybersecurity field. As seen in vast case studies, from small attacks to global ones such as those on Sony Pictures, one can see the holistic and interdisciplinary application of these topics and the tremendous issues that can arise from unsuccessful security, semantic understanding, and communication. This review can segue into future empirical work aimed to produce tangible applications of bypassing correctives and communicational strategies within cybersecurity across disciplines.

Bibliography

Bonner, L. (2012). Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches. *University of Washington Journal of Law & Policy, 40*, 257-277.

Byron, K. (2008). Carrying Too Heavy a Load? The communication and miscommunication of emotion by email. *The Academy of Management Review, 33*(2), 309-327.

Cole, B. M., & Banerjee, P. M. (2013). Morally contentious technology-field intersections: The case of biotechnology in the United States. *Journal of Business Ethics,115*(3), 555–574.

Connor, J. J. (1991). History and the study of technical communication. *Journal of Technical Writing and Communication. 13(*1983). 155-65.

Cukier, M. (2007). *Study: Hackers attack every 39 seconds*. University of Maryland. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

Haney, W. V. (1992). *Communication and interpersonal relations: text and cases*. Homewood, IL: Irwin.

Hess, A. (2015). *"Everything Was Completely Destroyed": What It Was Like to Work at Sony After the Hack.* http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

Holmes, A. (2007). *Your Guide To Good-Enough Compliance*. CIO. https://www.cio.com/article/2439324/your-guide-to-good-enough-compliance.html

Kosseff, J. (2018). Defining cybersecurity law. *Iowa L. Rev.*, *103,* 985-1031.

Laczniak, G. R., & Murphy, P. E. (2006). Marketing, consumers and technology. *Business Ethics Quarterly,16*(3), 313–321.

Lehto, Martti. (2015). The cyberspace threats and cyber security objectives in the cyber security strategies. *International Journal of Cyber Warfare and Terrorism. 3.* 1-18.

Lutz, W. (1989). *Beyond nineteen eighty-four: doublespeak in a post-Orwellian age*. Urbana, IL: National Council of teachers of English.

Mehrabian, A., & Ferris, S. R. (1967). Inference of attitudes from nonverbal communication in two channels. *Journal of Consulting Psychology, 31*(3), 248–252.

Milkovich, D. (2020). *15 Alarming Cyber Security Facts and Stats*. Cybint. https://www.cybintsolutions.com/cyber-security-facts-stats/.

Orwell, G. (1964). *Nineteen eighty-four*. Harmondsworth: Penguin Books.

Parent, K. (2012). The Most Frequent English Homonyms. *RELC Journal, 43*(1), 69–81.

Press Release, White House. *Statement on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea"* (2015). Obama White House Archives. https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled- imposing-additional-s.

Richmond, S. (2011). *Millions of internet users hit by massive Sony PlayStation data theft.* Telegraph. https://www.telegraph.co.uk/technology/news /8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html.

Mueller, R. S. (2012). *Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies*. FBI. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

Roberts, P. (2014). *A New Script: Clues In Sony Hack Point To Insiders*. Security Ledger. https://securityledger.com/2014/12/new-clues-in-sony-hack-point-to-insiders-away-from-dprk/.

Roghanizad, M. M., & Bohns, V. K. (2017). Ask in person: You're less persuasive than you think over email. *Journal of Experimental Social Psychology, 69*, 223–226.

McNicholas, E., & Angle, K. (2020). *USA: Cybersecurity Laws and Regulations*. ICLG. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa.

Rosenthal, R. & Ushe, N., & Magaya, I. (2016). A framework for enterprise security and forensics in Zimbabwe- A case study of the Sony Hack. 10.13140/RG.2.1.2994.2803.

Simpson, B., & Murphy, M. (2016). Technological challenges and opportunities: the future of law. *Information & Communications Technology Law, 25*(1), 1–3.

Sony Corporation. (2018). Supplemental Information for the Consolidated Financial Results for the Fourth Quarter Ended March 31, 2018" (PDF). Sony. https://www.sony.net/SonyInfo/IR/library/presen/er/pdf/18q4_supplement.pdf.

Sony History. (n.d.). Sony. https://www.sony.net/SonyInfo/CorporateInfo/History/SonyHistory/.

Stiegler, C. (2017). Sustainability in the media industries: the lack of transparency and the "Sony hack". *ReThinking Management,* 205-216.

Trautman, L. J., & Ormerod, P. (2018). Wannacry, Ransomware, and the Emerging Threat to Corporations. *SSRN Electronic Journal*.

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science, 185*(4157), 1124–1131.

Weger, H., Castle Bell, G., Minei, E. M., & Robinson, M. C. (2014). The Relative Effectiveness of Active Listening in Initial Interactions. *International Journal of Listening, 28*(1), 13–31.