If Communication is a Bridge, Cryptography is a Drawbridge: A Stage-Based Model of Communication Processes

Charles Berret
University of British Columbia

Abstract

This paper presents a model of communication based on the conditions of its success and failure. Building on Peters' metaphor of communication as both a bridge and a chasm, the model depicts cryptography as a drawbridge to selectively choose the audience of a message. The model forms a set of islands linked by a series of drawbridges, each representing a source of communication's success or failure, and each of which must be passed in sequence. The first drawbridge is *recognition*, in which the most basic source of failed communication is to be unaware that a message is even present. The next is *access*, in which some form of barrier or lack of authorization keeps one from accessing a message. Next is *legibility*, the ability to recognize individual symbols, followed by *intelligibility*, the recognition of coherent patterns, words, and syntax in those symbols. The final two stages of this model concern different stages of meaning. The *public meaning* of a message is the literal, surface sense intended to be understood without insinuation or ambiguity. The *private meaning* of a message is either selectively encoded for a specific audience, or else fully interior to our own minds. The descriptive and explanatory power of this model is illustrated through various examples in which communication is secret, secure, and otherwise selective of its audience.

Introduction

The field of communication studies needs a theory of cryptography, not only because this is a distinct form of communication that is understudied in our field, but because cryptography has become an inextricable layer of the digital world. This year, the total share of web traffic using encryption across all of Google's services stood at 95 percent, nearly doubling since they first began measuring this figure in 2013 (Google 2021). Leading tech companies like Apple and Microsoft now encrypt their devices, software, and services by default. Every online purchase, every credit card transaction, every movie you stream is encrypted for the security of users and merchants alike. And yet, despite its growing entanglement in the basic fabric of digital life, cryptography itself remains a fairly marginal subject in communication studies, playing only a supporting role in scholarship on topics such as privacy and surveillance (Lauer 2011, Tufekci 2014), hacking (Kubitschko 2015, Coleman 2019), internet policy and governance (Gillespie 2007, Owen 2015), online activism (Tufekci 2017), and journalism (Henrichsen 2019, Di Salvo 2020), but rarely treated as a subject of interest in itself. This absence is all the more pointed because digital cryptography is only its most recent incarnation, whereas the broader use of cryptography is easily as ancient and varied as communication itself (Kahn 1996).

This paper offers a new model and theory of communication that counts cryptography as a first-class citizen, asking what the means of selectively concealing messages may reveal about communication itself. Whereas cryptography is typically defined as secret, private, or secure communication, these definitions neither describe the communication process nor capture the wide range of ways cryptography works. A more useful definition of cryptography is this: any practice designed to selectively limit the audience of a message through artful manipulation of known conditions in which the communication process fails. For instance, just as a noisy transmission may cause communication failure, encryption may deliberately render a message indistinguishable from noise to guard against eavesdropping. Every historical means of information security has taken the form of communication's shadow, rendering the readable as unreadable, the visible as invisible, the clear as obscure, the open as inaccessible — but only to those who have not been granted access. The true inventiveness of cryptography lies in the assurance that a message has not actually been destroyed after being rendered unreadable, but is instead recoverable through a reversible process.

I model this reversibility by analogy to a drawbridge, building on John Durham Peters' (1999) memorable account of communication as "both bridge and chasm," a vexing duality of promise and impossibility. Peters writes that communication presents itself as a means of bridging the divide between human minds, driving us with a force of fundamental yearning that underlies the basic motivation to form friendships, relationships, families, and even societies. On the other hand, Peters notes that all communication is imperfect, minds never fully meet, and a lot of the time communication overtly fails. The case of cryptography suggests an instructive take on this duality. If communication is both a bridge and a chasm, then cryptography resembles a drawbridge with which to make inventive use of the knowledge gained from our many intimate confrontations with different chasms of communication failure. The model given in this paper suggests that any source of communication failure can be turned into a form of information security.

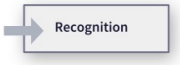
The initial motivation for this study had been to delineate how different types of cryptography and information security work in terms of communication processes, but the resulting model has broader descriptive power and unexpected implications. The drawbridge model generalizes across various forms of communication, from gestures and facial expressions to speech, text, and digital code. It covers historical practices of information security, such as acrostic puzzles and invisible ink, but also applies to a wider range of cryptic communication practices such as poetry and innuendo. The model reveals connections between historical cases and modern computational ones, as well as speculative future technologies. The structure of this model also draws from the literature on process models in computer science and data science, where researchers develop formalisms for both describing and prescribing actions taken in pursuit of specific goals (Munzner 2009, Grolemund and Wickham 2014, Ralph 2019).

Moreover, the drawbridge model should interface cleanly with many existing models and theories of communication, even those that were originally formulated as objections to transmission-based accounts. Whereas cultural approaches to communication such as reception theory (Hall 1973), the constitutive view (Barnlund 1970), and the ritual view (Carey 1992) were offered up as challenges to the transmission model of Schramm (1955) and Shannon (1948), the model presented here simply places the respective interests of these approaches at different stages of the communication process. By understanding different communication processes in terms of how they may succeed or fail, this model illustrates the many productive uses people have found when confronted with the limits of communication.

The Drawbridge Model of Communication

The drawbridge model of communication depicts a chain of islands linked by a series of drawbridges, each representing a discrete source of communication's success or failure. Starting from the initial island, communication requires successful passage over each drawbridge. Failure at any stage renders further stages inaccessible. Likewise, a successful implementation of information security at one stage will also guard the further stages. The reversibility of each stage is critical. Any viable means of cryptography must operate like the raising and lowering of a drawbridge, letting some pass through while stopping others.

Recognition



The first drawbridge to pass is *recognition*, in which the most basic source of communication failure is to be unaware that a message is even present. This can take many forms. You might wave to get my attention, but I don't notice. A shipwrecked sailor might form the word "HELP" from rocks or driftwood to be visible from the sky, but no planes pass by. We might be receiving transmissions from another galaxy at this very moment, but our antennas could be facing the wrong direction, tuned to the wrong frequency, or even incapable of detecting the signal used. In each of these cases, communication fails even if the message is perfectly viable otherwise. Communication that goes unrecognized thus stops outside the first drawbridge without encountering any further conditions of success or failure.

Information security is mediated at the recognition stage through practices known as *steganography*, or communication hidden in plain sight, relying on security through obscurity. One well-known traditional form of steganography is invisible ink, which must be heated, exposed to another chemical, or otherwise treated to be rendered visible. Other forms of steganography may be endlessly idiosyncratic, as camouflage tends to reward the unexpected. For instance, on the eve of the American Revolution, the signal "one if by land, two if by sea" made use of steganography by transmitting its message with lamps in a church tower, where nobody outside the plotters expected to see a secret signal. This is a textbook case of steganography: security rests on the difficulty of recognizing that a message is even present.

Digital watermarks are a form of computational steganography used to identify and trace copyrighted, classified, and otherwise restricted files. A digital watermark is designed to be undetectable within the encoding of the file, thus passing unnoticed at the recognition stage of this model. For example, a PDF could contain a digital watermark tied to the contents of the file when it was created. If someone alters the file, we can check the digital watermark to verify the authenticity of the contents. Because this watermark is hidden, we are not aware of this additional information layer when we simply open the PDF for conventional reading. Overall, the multiplicity of possible ways to read and display the information in any digital file leads to a corresponding multiplicity of techniques for encoding messages that escape recognition. As with traditional steganography, the point is to identify ways that communication may fail by escaping our notice.

Access

The next drawbridge is *access*, in which a barrier or lack of authorization may keep someone from reaching a message even if they are aware of its presence. For instance, even if I'm aware that a letter has been delivered to my post office box, I may not be able to access the message if the office is closed or I've lost my key. Communication fails, if only temporarily, because I am literally, physically blocked from accessing the letter. As with the case of recognition above, no further stages of this model come into play if the drawbridge is impassable. The message could be perfectly clear and legible, but I am blocked at the stage of access, thus communication fails.

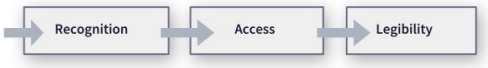
The access stage encompasses any kind of lock-and-key mechanism, but also includes a wider array of systems intended to block access to a particular message. In the case of a traditional lock, modes of circumvention include copying the key, picking the lock, or simply breaking the mechanism. A telephone wire tap is also a form of access mediation, as it facilitates a direct line for eavesdropping.

The same goes for software written with backdoors and other forms of 'tailored access,' the term used for this form of intrusion by NSA according to the Snowden documents (Greenwald 2014).

In the usual case of computer systems, file permissions and passwords are the principal means of mediation at the access stage. If I can't login, I don't get access. If my user account has not been granted "read" permission for a file, I don't get access. Likewise, if a file is protected by a password, the system only grants access if the correct answer is given. The same goes for compound access protection schemes like two-factor authorization, in which an additional token must be given.

Beyond systems designed to block dedicated efforts at intrusion, access may also be mediated in a somewhat softer manner by laws, norms, morals, and other conventions. Consider the case of the envelope, which is simple to open by design, but still provides security because it signals a desire for privacy and discourages unauthorized access on both legal and moral grounds. Likewise, if you and I wish to signal that we're having a private conversation, we may simply close the door, speak quietly, or walk to a secluded area. The point is not to sequester our conversation from a dedicated eavesdropper, but rather to signal a desire for privacy that rests on our tacit trust in the general civility of others. In the case of doctors, lawyers, and other professionals whose confidentiality is often protected by law, access is mediated by threat of punishment, even if no further means of security are in place. Neither of these systems offer airtight information security, but the efforts nevertheless operate at the level of access.

Legibility



For the sake of this model, *legibility* means the ability to recognize individual symbols. A message sent to me in letters I recognize, which is rendered so that I can reliably identify those letters, is legible for our purposes. The text may be a meaningless jumble of familiar characters, but as long as I recognize those characters, it satisfies the criteria for legibility. The same goes for a string of digits. They could be random, they could be some sort of code, they could be lottery numbers, but what matters at this stage of the model is for the individual symbols to be legible to their audience. If I have not learned the symbols, or they are scribbled in an illegible hand, communication fails at this stage.

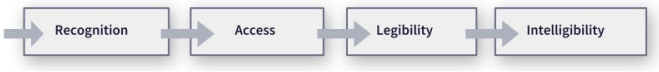
Several historical examples should help illustrate how the artful use of the legibility drawbridge has been used for information security in the past. Each one takes the form of a secret alphabet known as a monoalphabetic cipher, in which a particular symbol stands in for a single letter from another alphabet. For instance, a code known as the pigpen cipher is one of the least guarded secrets belonging to the society of Freemasons, as some members have even inscribed their gravestones with messages in this system of simple geometric lines and dots that represent each letter of the Latin alphabet (Kahn

1996). Likewise, the subculture of traveling American workers known as hobos developed a system of symbols to assist one another in surviving as they traveled through unfamiliar locales (Wanderer 2001). They might leave one symbol inscribed on a wall to indicate a good camping spot, another to warn of a vicious dog, another leading to a source of safe drinking water. In either case, you must know the symbols or else figure them out in order to pass this drawbridge.

A prominent contemporary example of information security at the legibility stage is CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHA systems are widely used today to verify that a computer user is a human being and not a bot, hence serving the basic role of a Turing Test (Turing 1950). Some CAPTCHAs present a string of mangled text, whether in visual or audible form, and ask the user to enter that text in a box. Others present a series of images and ask the user to identify which ones have stoplights, bicycles, and other objects of special interest for training computer vision algorithms. Whatever the form of the CAPTCHA, the level of security it provides will depend on the relative legibility of these symbols, images, and recordings to human beings versus automated systems designed to act like human beings.

Note that literacy is not binary, but often falls on a spectrum. Most of us can recognize two symbols in Morse Code, but only because "SOS" is a trope of popular culture. I was once able to read a few different non-Latin alphabets, such as Arabic and Tibetan, but have since forgotten most of the characters. The point is that legibility of different symbols does not necessarily come in complete groups. Before the rise of mass literacy, this was the case for most people without a formal education, who could identify a bit of written text through occasional exposure to these symbols. This point is even more pronounced at the next stage of the model, because even a full grasp of a given character set may not be enough to ensure success in communication.

Intelligibility



Closely related to legibility is *intelligibility*, whether one is able to recognize coherent patterns, words, and syntax in a set of known symbols. Successful communication of written words in any language requires not only knowing the symbolic components, but also gleaning how they fit together.

Another form of cryptography that operates at the stage of intelligibility is the acrostic puzzle, in which a sequence of letters in an otherwise innocuous text (for instance, the initial letters in a series of words, lines, paragraphs, pages, etc.) spell out a hidden message. The novelist Vladimir Nabokov was particularly fond of acrostic puzzles, using this device to implant secret messages in several stories as

rewards for his most attentive readers.[1] A similar device is the anagram, in which a message is concealed in the reconfiguration of letters. Although the writer Charles Dodson eventually settled on the pen name Lewis Carroll, he initially published as "Edgar Cuthwellis," an anagram of his given name. Literary acrostics, anagrams, and other forms of wordplay call attention to the fact that configurations of symbols can be multiply encoded, and different reading techniques may render these multiple encodings intelligible.

This drawbridge is particularly important in the realm of information security today because digital cryptography mediates exclusively at the intelligibility stage of this model. Every form of digital encryption in widespread use today relies on algorithms that scramble strings of digital characters into different strings of digital characters, reaching staggering levels of complexity.[2] The individual characters in an encrypted message remain legible, but the message itself is beyond intelligibility by design. Of course, the process may be reversed if you possess the right key or otherwise manage to attain it, whether through brute-force guessing or by simply stealing the key. Whatever the method, performing digital decryption drops the drawbridge of intelligibility and renders a message readable.

Public Meaning

The final two stages of this model concern different forms of meaning: public and private. As the ultimate stages of this model, they are also the broadest and most porous due to the sheer complexity of human communication.[3] Given that the core purpose of this paper is to model different kinds of communication failure in terms of their usefulness for information security, the distinction between public and private meaning is useful because it helps delineate distinct kinds of communication failure that can be used to conceal a message.

The *public meaning* of a message is the literal, overt, surface sense conveyed by its author, who intends for this message to be understood by anyone else who wishes to read, hear, or otherwise receive it. For the moment, I will bracket off the question of whether the speaker and listener ever truly

---

[1] The most prominent of Nabokov's literary acrostics can be found in his story "The Vane Sisters," in which the final paragraph encodes a message addressed from the dead sisters themselves. Nabokov himself later boasted that the literary use of this device could only be tried once in a thousand years of fiction, though he nevertheless used a series of subtle acrostics in the experimental novel *Pale Fire*.

[2] For a readable overview of encryption methods, both historical and digital, see Singh (1999).

[3] While some communication practices could seem unambiguously public or private, such as addressing a crowd or winking, neither of these can be neatly categorized so that we can say giving a speech is inherently public and winking is inherently private. While this caveat may also apply to earlier stages of this model, it is more pronounced in the final two stages focused on varieties of meaning.

share an identical interpretation of any given message. Instead, this stage of the model depicts a pragmatist view of successful communication in terms of mutual agreement that both parties understand one another. Moreover, it is beyond the scope of this model to assess the truth value of a statement or its propositional content, which are the central concerns for many philosophers of language when they discuss meaning.[4] Ceteris paribus, success and failure in communication are independent of truth and falsity, just as techniques of information security may succeed or fail in guarding a message whether or not that message is true.

What does it look like when communication fails at the level of public meaning? Even if each element of a sentence is intelligible, the sentence itself may still be meaningless in terms of basic semantics. Noam Chomsky's (1956) famous example of such a sentence is "colorless green ideas sleep furiously." Likewise, many works of conceptual art, poetry, and experimental literature contain grammatical messages with coherent syntax that nevertheless resist direct comprehension. These works are especially compelling because they engage with the nature and effects of communication breakdown for artistic effect rather than information security. A difficult poem invites the reader's decipherment, posing its challenge at the drawbridge of its public meaning.

Translation between two natural languages takes place at the level of public meaning, and automated machine translation offers an especially revealing case. Deep learning techniques have led to the development of translation algorithms that decode public meaning across languages with high precision, up to the point of automatic, instantaneous translation of straightforward, unambiguous messages. In terms of scientific progress in the domain of machine translation, this particular drawbridge descended only in the last decade, allowing computational efforts to be directed toward the far more difficult cases of implicit, contextual, and emotional content, which is the target of sentiment analysis (Balahur & Turchi 2014). One relatively tractable case for natural language processing (NLP) is spam detection — using patterns gleaned from past spam messages to detect new ones (Brunton 2013).

While I am not aware of any formal techniques of information security that operate on the drawbridge of public meaning, it should be possible to do so, albeit with limited practicality. For the sake of illustrating what such a technique might look like, consider Gregory Bateson's (1972) account of communication among schizophrenic patients he treated in a clinical setting. Bateson's remarkably compassionate account describes the apparently nonsensical statements of his patients as a transgressive form of resistance: their rejection of an authority figure's insistence on what kind of message counts as a message. Granted, this is a narrow and idiosyncratic case, but nevertheless relevant to this study because Bateson's patients appeared to be controlling the audience of their messages by forcing communication failure at the stage of public meaning. The sort of communication

---

[4] For a survey of work examining truth, sense, and reference in analytic philosophy, see Soames (2010).

failure that occurs at this drawbridge seems to be much less useful for information security than at any other stage of this model, yet close attention to this case reveals it to be a form of information security with a distinct, though narrow, place in interpersonal communication. In Bateson's account, active rejection of public meaning through deliberate communication failure can be seen as a form of dissent.

Private Meaning

Finally, after traversing every previous drawbridge, the private meaning of a message is either selectively or entirely accessible to others. This takes two distinct but related forms, a weak and strong version. *Weak private meaning* is the deliberate, selective assignment of a new meaning to an existing symbol. Forms of information security mediated by weak private meaning include secret codes known by one or more people. *Strong private meaning* is the inviolability of the mind itself. The principal form of information security in this domain is deception, in which the drawbridge of private meaning blocks others from access to the truth.

For the sake of information security, many statements made in public may have implicit meanings that add a layer of contextual factors requiring some level of interpretation, insight, or privileged awareness. Examples include insinuation, sarcasm, slang, innuendo, and other covert meanings that may divide an audience into those who 'get it' and those who do not. The importance of this drawbridge cannot be overstated: throughout history, the value of saying one thing and meaning another has been the bedrock of information security in everyday life, from gossip and seduction to palace intrigue and grassroots resistance networks.

On today's social media platforms, the use of weak private meaning for information security remains vital. Marwick and boyd (2014) underline this fact with their study of teenagers practicing *social steganography*, communicating covertly in the open environments where their digital lives unfold under the gaze of others, whether peers, parents, or teachers. Recalling cases discussed earlier in this model, at the stage of recognition, steganography is the practice of hiding messages in plain sight, relying on security through obscurity. While some methods of social steganography may also belong at the recognition stage, the cases described by Marwick and boyd largely operate upon the drawbridge of private meaning, where teenagers rely on coded language to control who knows what they're really talking about online. By using a code only understood by friends and confidantes, the weak drawbridge of private meaning is raised and lowered for different audiences to mediate conditions of privacy even in public speech. For this reason, deception is also a form of information security that rests on the privacy of one's own mind and the selective revelation of its contents.

In contrast to the simpler cases of NLP addressed above, the more difficult cases now being researched include the detection of sarcasm in natural language, which is often delivered in statements that overtly clash with background assumptions to indicate that they require further decoding. Other cases of implicit meaning may be vastly more complicated, perhaps impossible, to reliably detect through computational means, especially when the speaker's goal is to evade detection. Nevertheless, if and when NLP becomes sophisticated enough to reliably navigate tricky discursive stances with implicit, contextual meaning, it is reasonable to assume that human invention will lead to new tactics of evasion operating at this drawbridge of information security.

The strong version of the private meaning drawbridge represents the inviolability of the mind itself, where we may keep our thoughts to ourselves. A message may move across every previous drawbridge without reaching the private meaning that constitutes what one knows or believes to be true. This is a form of security that has not yet been broken by technological means.[5] A message may traverse the entire ladder of this model, yet still the speaker of a message may conceal their beliefs or withhold information, whether through common discretion or outright deceit. In other words, this drawbridge deserves considerable respect as a common tactic in the everyday practice of information security. We have not yet devised techniques of direct mind reading, whereas earlier stages of this model are tractable fields of inquiry.

As the strong form of private meaning, this drawbridge is not so much a redoubt of information security, but rather a gaping abyss of hypothetical failure for any act of communication. Within communication studies, this particular abyss is the primary subject of Peters' (1999) exploration of communication's ultimate impossibility and the perennial vexation this has caused for Western thinkers. Peters describes communication as a means of reaching across the gaps that separate us from one another, but also a reminder that we may never fully close these gaps. Although the animating concern in Peters' inquiry is rich enough to traverse each stage of this model, as it draws upon our general awareness of the limits and failures of communication we encounter throughout our lives, Peters' ultimate concern resides here, at the level of private meaning, where we confront a drawbridge that may never be within our power to cross.

This stage of the model, itself the final stronghold of the communication process, is also the most laden with philosophical debate, as it is the subject of Wittgenstein's famously thorny Private Language Argument (PLA). In his *Philosophical Investigations*, Wittgenstein (1953) explored counterintuitive implications of the idea that we personally ascribe meaning to the words we use. If that were true, Wittgenstein argues that language itself would be fundamentally meaningless to others, and equally meaningless to ourselves. Kripke (1980) would later take up the PLA to produce striking challenges to

---

[5] Even if a polygraph or other device should prove effective in detecting deception, this only identifies the drawbridge; it does not raise it.

the possibility of both public and private meaning. While it is beyond the scope of this paper to argue for or against private language, suffice it to say that the drawbridge model is readily adaptable to either case. As with Peters' concern, this model would depict the impossibility of private language as a permanently impassable drawbridge at the final stage, where communication has its source within us.

Unlike the weak form of private meaning, which is characterized by the familiar case of coded language, the strong form of private meaning presents difficulties for information security because its implications are so elusive. On the one hand, each of us has private thoughts that simply cannot be pulled from our minds — barring the invention of mind-reading device — because these thoughts reside in the area across Peters' chasm of communication's ultimate impossibility. If indeed this gulf cannot be bridged, it also cannot be used for information security in the sense this model implies. A drawbridge that cannot be lowered cannot be used to selectively control the audience of communication.

Conclusion

The primary purpose of the drawbridge model is to describe and categorize different forms of cryptography and information security in terms of communication processes. The model has broader efficacy as a means of illustrating how everyday confrontations with communication failure may lead to productive sources of invention. Faced with the many bridges of communication and the many chasms of its failure, the model locates means of building drawbridges with a range of social, cultural, and political uses. Inspired by process models from computer science and data science (Munzner 2009, Grolemund & Wickham 2014, Ralph 2019), this connected series of islands suggests a productive means of thinking about communication, in its broadest sense, through the unexamined theoretical lens of cryptography.

This model also presents an opportunity to rejuvenate some entrenched conversations in the realm of communication studies, where the notion of a transmission model has been treated as highly suspect for decades because human beings, unlike machines, cannot transmit an exact copy of a message from one brain to another (Barnlund 1970, Hall 1973, Carey 1992). Whereas Shannon's (1948) theory and model of the communication process was delivered alongside a compatible theory and model of cryptography (1949), the declining favor of transmission models in communication studies since the 1970s has left the field without a serviceable theory of cryptography to replace it. This model is capacious enough to contain both the workings of a transmission model (at the stages of *legibility* and *intelligibility*) as well as the cultural complexities expressed in leading critiques of transmission (at the stages of *public* and *private* meaning). Moreover, seen through the lens of this model, these opposing camps may even be treated as compatible if we separate their respective concerns into different stages of success and failure in communication. Specifically, Shannon never intended for his

model of communication to explain semantics, i.e. *public* or *private* meaning, just as Hall, Carey, and other cultural theorists of communication never intended to explain the transmission of *legible* or *intelligible* symbols. (To my knowledge, no attention has been given to *recognition* or *access* in a theory of communication.) While this distinction in subjects of interest may not resolve their ultimate differences, it may clarify the center and periphery of the work done by previous theories of the communication process.

Loops and recursion suggest additional layers of complexity to enrich the explanatory value of this model. Returning to the case of acrostic puzzles discussed above, imagine reading a text without realizing that a message is concealed in the initial letter of each word. You could still reach the stage of public meaning in the surface text, and perhaps even cross into the realm of private meaning when you notice contextual details placed by the author. But if you happen to notice the acrostic, one way to model this process is by looping back to the recognition stage and proceeding through each drawbridge once more to find the newly recognized message. Further work is needed to fully model this tricky case, which may be better understood by more complex models, such as forking paths for different messages encoded within a single source.

The drawbridge model also offers a schema for the design and assessment of information security systems and practices. Some readers may have been struck by the fact that digital cryptography, despite its growing ubiquity, only operates at the *intelligibility* stage of this model. *Access* is the other stage where most of today's digital security practices operate, while social steganography works at the level of *private meaning* in the relatively low-stakes scenarios encountered by teens, and digital watermarks perform steganography at the level of *recognition*. Delineating the different stages of this model may lead to the development of new encryption techniques that embrace a broader set of communication practices. Indeed, scholars of communication are uniquely positioned to examine how the wide range of communication practices may point to unexplored domains in which the artful use of communication failure can inspire novel means of information security.

Works Cited

Agur, C. (2013). Negotiated Order: The Fourth Amendment, Telephone Surveillance, and Social Interactions, 1878–1968. Information & Culture 48(4).

Balahur, A. and M. Turchi. 2014. "Comparative experiments using supervised learn- ing and machine translation for multilingual sentiment analysis." Computer Speech & Language 28(1): 56–75.

Bateson, G. (1972). Steps to an Ecology of Mind: Collected Essays in Anthropology, Psychiatry, Evolution, and Epistemology. Chicago: University of Chicago Press.

Brunton, F. Spam: A Shadow History of the Internet. Cambridge: MIT Press.

Carey, J. (1992). "A Cultural Approach to Communication." In Communication as Culture.

Chomsky, N. (1956), "Three Models for the Description of Language" IRE Transactions on Information Theory 2(3) (September): 113-124.

Coleman, E.G. Coding Freedom: The Ethics and Aesthetics of Hacking. Princeton, NJ: Princeton University Press, 2013.

Di Salvo, P. (2020). Digital Whistleblowing Platforms in Journalism: Encrypting Leaks. Springer International Publishing.

Gillespie, T. (2007). Wired Shut. Cambridge: MIT Press.

Google, "HTTPS Encryption on the Web," https://transparencyreport.google.com/https/overview. Accessed April 12, 2022.

Greenberg, G. (2014). No Place to Hide. New York: Metropolitan Books.

Grolemund, G., & Wickham, H. (2014). A Cognitive Interpretation of Data Analysis. International Statistical Review, 82(2), 184–204.

Hall, S. (1991 [1973]) Encoding/Decoding. In: During, S (ed.) The Cultural Studies Reader. London: Routledge, pp. 90–103.

Henrichsen, J. (2019). Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies. Digital Journalism 8(3).

Kahn, D. (1996). The Codebreakers. New York: Scribner.

Kripke, S.A. (1980). Naming and Necessity. Cambridge, Mass.: Harvard University Press.

Kubitschko, S. (2015). The Role of Hackers in Countering Surveillance and Promoting Democracy. Media and Communication 3(2).

Lauer, J. (2011). Surveillance history and the history of new media: An evidential paradigm. New Media & Society 14(4).

Marwick, A.E., and d. boyd. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), 1051–1067.

Munzner, T. (2009). A Nested Model for Visualization Design and Validation. IEEE Transactions on Visualization and Computer Graphics, 15(6), 921–928.

Peters, J.D. (1999). Speaking into the air: A history of the idea of communication. Univ. of Chicago Press.

Ralph, P. (2019). Toward Methodological Guidelines for Process Theories and Taxonomies in Software Engineering. IEEE Transactions on Software Engineering, 45(7), 712–735.

Schramm, W. (1955). Information Theory and Mass Communication. Journalism Quarterly TK(TK).

Shannon, C.E. (1948). "A Mathematical Theory of Communication." The Bell System Technical Journal.

Shannon, C.E. (1949). "Communication Theory of Secrecy Systems." The Bell System Technical Journal.

Singh, S. (1999). The code book : the science of secrecy from ancient Egypt to quantum cryptography. London: Fourth Estate.

Soames, S. (2010). Philosophy of Language. Princeton: Princeton University Press.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. First Monday 19(7).

Tufekci, Z. (2017). Twitter and Tear Gas. New Haven: Yale University Press.

Turing, A.M. (1950). Computing Machinery and Intelligence. Mind 49.

Wanderer, J.J. (2001). Hobo Signs: Embodied Metaphors and Metonymies. The American Journal of Semiotics 17(4).

Wittgenstein, L. (1953). Philosophical Investigations (3rd ed., G. E. M. Anscombe, Trans.). New York: Macmillan.