CONCEPTUALIZING DIGITAL DECEPTION IN INFORMATION SECURITY MANAGEMENT

Spyridon Samonas, College of Business Administration, California State University Long Beach, 1250 Bellflower Blvd, Long Beach, CA 90840, 562-985-5672, spiro.samonas@csulb.edu

ABSTRACT

Perpetrators of digital crimes employ a range of skills to explore, identify and exploit various socio-organizational and technical vulnerabilities. Most notably, these skills include social engineering techniques and the use of anonymizing networks. Information security managers also use deceptive tactics to thwart attacks against information assets. However, while deception lies at the heart of many offensive and defensive security operations, its socio-organizational aspects are often overlooked. Drawing on Humanities and the socio-anthropological concept of 'cunning intelligence', this conceptual research paper proposes the development of a theoretical framework that underpins the socio-organizational aspects of digital deception.

Keywords: Digital deception, digital crime, theory building, information security management, cunning intelligence.

INTRODUCTION

Cyber-attacks that target personally identifiable information, payment card data, intellectual property and trade secrets, have become the new normal. As threat agents, perpetrators of digital crimes employ a range of skills to explore, identify and exploit various socio-organizational and technical vulnerabilities. Most notably, these skills include social engineering techniques such as spear-phishing, the use of anonymizing networks such as Tor, the adoption of crypto-currencies for illegal transactions, as well as the development and delivery of resilient malware that attempts to remain undetected from security safeguards. In this context, it appears that deception is integral to different aspects of digital crime that involve fraud, theft, and forgery [1].

The problem with digital crime is aggravated by the evolution of security threats, which essentially resembles an 'arms race' [2]. Threat agents devise new attacks, while the security industry is developing appropriate safeguards to address the latest known Tactics, Techniques and Procedures (TTP) that attackers employ. Gartner suggests that by 2018, ten percent of enterprises will use deception tools and tactics, and actively participate in deception operations against attackers [3]. In an effort to address this ever-changing threat landscape, frameworks such as the Cyber Kill Chain model can provide valuable input to information security managers on how to align organizational resources and capabilities to specific assets that attackers are most likely to target [4].

More specifically, Hutchins et al. [4] discuss the spectrum of activities that organizations can employ to defend themselves as part of the information operations doctrine of the U.S. Department of Defense. They identify in the form of the following types of actions: (1) detect, (2) deny, (3) disrupt, (4) degrade, (5) deceive, and (6) destroy. Interestingly, while there is currently a range of safeguards that can sufficiently detect, deny and disrupt attackers across all stages of the Kill Chain model (e.g. web analytics tools, intrusion detection and prevention systems), there is clearly a shortage of actions that relate to the degradation, deception and destruction of attacks against information assets. Deception techniques can

be deployed by organizations to effectively defend their resources by (1) misleading the attackers, and (2) impeding their decision-making with regards to a specific attack. Rowe and Rrushi [5] refer to a number of examples that illustrate the positive qualities of deception and call for a deeper understanding of the use of deception in information security. This involves 'thinking like a digital attacker' and articulating the variety of considerations, decisions and actions that attackers take prior, during and after the execution of a digital crime.

The opportunity to further enhance the Cyber Kill Chain model with deception-based countermeasures [3] opens up new avenues for the conceptualization and systematic use of deception in information security that go beyond deception detection. Drawing on Humanities and the socio-anthropological concept of 'cunning intelligence', the paper aims to develop a generalized theory of digital deception. Through the identification of a common body of attributes of digital deception, the theory under development can provide insights into the specific tactics of deception that are used in offensive and defensive security operations.

EXTANT LITERATURE

In this paper, the term 'digital deception' refers to a variety of offensive and defensive operations in information systems security that involve elements of deceit, fraud and trickery. This is evident, for example, in the deployment of honeypots, the crafting of seemingly legitimate e-mail messages, and the weaponization of undetectable malware. In all these activities, attackers and defenders use different attributes of deception, such as camouflage, chameleonism, forethought and opportunism in their use and misuse of information and communication technologies. While digital deception lies at the heart of many offensive and defensive security operations, scholarly studies across different disciplines tend to focus on the issue of deception detection, thus overlooking the relevance of the socio-organizational aspects of the concept.

Computer-related crime can be considered a variant of all crime [6]. In this respect, the term 'digital crime' is commonly used as an overarching concept that encompasses a wide range of different actions and incidents pertaining to crime. Wall [7] suggests that digital crime can be placed along a spectrum, depending on the extent to which technology is involved in the performance of criminal acts. The *less* digital crimes can be found on the one end of the spectrum, and these are crimes that simply assist criminals in the execution of 'traditional' crime schemes. On the other end of this spectrum, the *more* digital crimes are enabled by the latest advances in information and communication technologies. What makes a crime *more* or *less* digital depends on the digitality and novelty of that crime [1]. This includes a variety of considerations, such as the virtuality of the crime in terms of space and time, the ability of the criminal to conceal their identity, as well as the accessibility and proximity to the victim [1].

Within the study of digital crime, the practice of deception has been widely associated with activities such as social engineering [8], and masquerade attack detection [9]. However, it is a diverse phenomenon that is also relevant to other disciplines, such as psychology [10], forensics [11], information systems [12], and computer science and engineering [13]. Over the past 50 years, research in deception has been preoccupied with the study of lying and the detection of lies [14]. More specifically, researchers have striven to identify behavioral and physiological cues that enable the accurate distinction between truths and lies in verbal and written communication. Despite the significant contribution of this line of research in law enforcement and other applications of deception detection, Levine [15] points out that deception detection experiments can only achieve a maximum accuracy of 67%. Other research projects in this area have focused on the motivations behind lying [16], the susceptibility of users to phishing email [17], and the capacity of people to distinguish between true and false statements [18].

The literature on deception detection and the related theories of deception that are briefly examined in this section, fall short in addressing the different ways in which socio-organizational elements of digital

deception blend with, and are applied to, the technical aspects of information security management. On the one hand, social studies focus on the attributes of deception that are ubiquitously present in societies and organizations [19, 20]. Computer science and related disciplines discuss issues of deception and trust in the Semantic Web [21], and in virtual societies [22]; however, these approaches focus entirely on technical safeguards. To address this, the paper examines how deception as cunning intelligence can be considered a mental category that is applicable to offensive and defensive information security operations.

METHODOLOGY

Dubin's [23] work on theory development presents a linear eight-step model of theory building. The first four steps (Units, Laws of Interaction, Boundaries and Systems States) lead to the development of an informed conceptual framework, while the remaining steps (Propositions, Empirical Indicators of Key Terms, Hypotheses and Testing) refer to the operationalization of the theory in empirically verified ways. As Swanson [24] points out, Dubin's model has been used to develop narrower, sub-discipline theories that lack a unifying and broad theoretical perspective, which is crucial to framing a discipline. To remedy this shortcoming, Swanson and Chermack [25] propose the General Method of Theory Building (GMTB) in applied disciplines.

As depicted below, the GMTB consists of a recursive system of five distinct phases and two broad components (see Figure 1). The two components capture the dual deductive-inductive nature of a theory-building method that has been developed for applied disciplines. This duality enables scholars and practitioners to fuse their perspectives in order to achieve greater understanding of the discipline [25]. The theorizing aspects should produce an informed theoretical framework that sufficiently explains the phenomenon, issue or problem under study. The practice aspects refer to the confirmation, disconfirmation or refinement of the theory based on collected data and experiential knowledge [26].

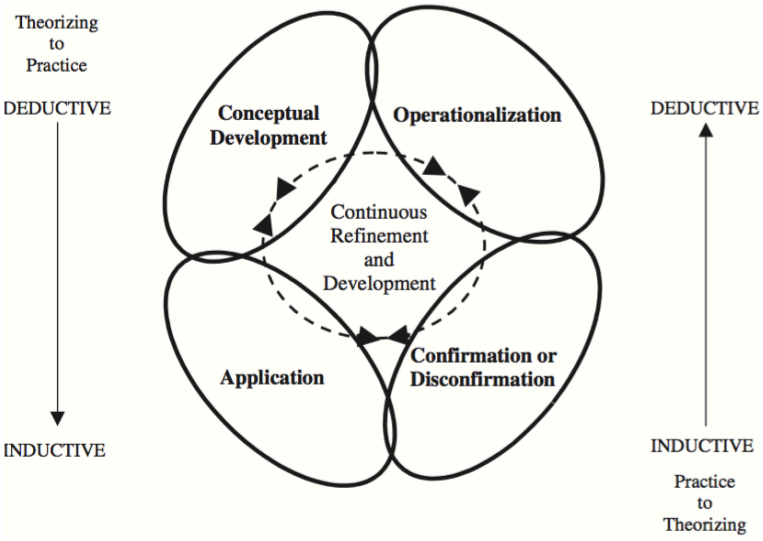

FIGURE 1: The General Method of Theory Building. Source: [25]

This paper focuses on the Conceptual Development phase of the GMTB and presents the key elements of a theory of digital deception that is pertinent to information security. In the conceptualization phase of the GMTB, the researcher-theorist aims to develop "an explicit, conceptual framework that often takes the form of a model and/or metaphor that is developed from the theorist's knowledge of and experience

with the phenomenon, issue, or problem concerned." [23, p.39]. In the Conceptual Development phase, the theorist is expected to (1) define the concepts, (2) organize the concepts, and (3) define the boundaries of the theory. Dubin [23] provides a clear set of quality indicators for each of these sub-steps, which we have sought to follow.

Finally, we adopt Weick's [27] theory construction as disciplined imagination as a suitable conceptual development method. This approach has been widely used in Management studies and is related to the work of Weick [27, 28], Weick and Daft [29] and Cornelissen [30]. Disciplined imagination is a nonlinear conceptualization process that is based on sensemaking. More specifically, it uses metaphorical images to produce theoretical representations that explain a phenomenon, issue or problem sufficiently. Digital deception as cunning intelligence was selected as the most apt and suitable to provide a set of attributes of digital deception that could be used in the context of the theory under development.

DIGITAL DECEPTION AS CUNNING INTELLIGENCE

The concept of cunning intelligence can be traced back to the Ancient Greek and Chinese civilizations, as well as to Norse myths. For many years, it was easier for Humanities scholars to understand the underlying notions that are associated with this concept, than to define it. Thanks to the seminal work of Detienne and Vernant [31], and more recently, of Vidal-Naquet [32], Raphals [33] and Wanner [34], cunning intelligence has been acknowledged as an overlooked type of intelligence that Greeks applied to a wide range of practical activities. Such activities included the making of fish nets and traps, the art of the carpenter, the skill of the navigator and the solving of riddles. Cunning intelligence is applied to situations that are transient, shifting, disconcerting and ambiguous, where precise measurement, exact calculation or rigorous logic are not always applicable. Ciborra [40, p.24] draws a well-argued connection between cunning intelligence (i.e. "the *métis* of the Greek") and improvisation, in his discussion of drift and practical intelligence in organizations:

> *"Far from what has become the conventional distinction between tacit and explicit knowledge, practical intelligence is the métis of the Greek – the intelligence of the octopus: flexible, polymorphic, ambiguous, oblique, twisted, circular. This is the opposite of the straight, direct, rigid, and univocal character of the knowledge embedded in the method. To orient oneself in the complex and changing world, dealing with forces that are too strong to be fully controlled, one needs to leverage the situation at hand by zig-zagging behaviour, which never faces such forces up-front but accomplishes the project at hand with a sudden move of improvisation."*

Indeed, according to Detienne and Vernant [31], the term 'cunning intelligence' encapsulates various qualities, such as camouflage, sharp-wittedness, resourcefulness, skilful craft, vigilance, self-sufficiency, and the seizing of opportunities. Besides Gods and mythical men, Ancient Greeks treated animals such as the fox, the cuttlefish and the octopus as 'tricksters.' They would carefully document and analyze the behavior of these creatures, particularly with regards to surviving and evading capture, to develop metaphors, stories and even precepts that would help them apply the cognitive skills of cunning intelligence to different aspects of their daily life.

Another key aspect of cunning intelligence is the temporality of time as conveyed in the distinction between *chronos* and *kairos* – the two words that Ancient Greeks used for 'time'. The concept of *chronos* is in line with Newtonian physics and expresses a standard of measurement of all motion and change that 'uniformly flows' in the cosmic system. *Kairos* refers to an 'opportune moment', the 'right time' when appropriate action is due [36]. In organization studies and IS research, Ciborra [37] examines *kairos* in the context of improvisation as situated action, while Orlikowski and Yates [38] adopt the distinction between *chronos* and *kairos* as a framework to understand temporal structuring in organizations.

The following section presents a set of theorizing relationships, building on the aptness of cunning intelligence as a metaphorical image in the development of a theory of digital deception in information security.

To better illustrate the concepts that describe cunning intelligence, some of its key aspects can be juxtaposed with manifestations of deception in current, offensive or defensive, information security practices. This takes the form of an elementary comparative concept analysis between the characteristics and skills of the predator and the prey for a set of themes that relate directly to the definition of cunning intelligence presented here: (1) Trojan Horse and Trojan horses, (2) fishing and phishing, and (3) hunting and hacking. As part of this conceptual exercise, it is also important to examine the relationship between chronic and kairic time in the context of information security management and digital deception.

However, for reasons of economy of space, we will only examine one theorizing relationship: hunting and hacking. Ancient Greeks would assume the role of a predator to hunt down and kill animals for sport or food. This activity often required excellent eyesight, force and speed. The prey would try to avoid detection by employing various techniques, such as minimizing noise production and visual cues, remaining still while hiding and changing its color (e.g. chameleonism and countershading).

In the realm of computer hacking, predators try to gain unauthorized access and exploit vulnerabilities in computer systems. They typically complete a sequence of actions that are reflected in models such as the Kill Chain and the Attack Lifecycle. For instance, the Kill Chain model consists of the following stages: (1) Reconnaissance, (2) Weaponization, (3) Delivery, (4) Exploitation, (5) Installation, (6) Command & Control, (7) Actions on Objectives [4]. In the role of the prey, organizations develop military-style strategies to defend their information resources and, in certain cases, retaliate against the attacker. Rather than expel the intruder immediately, the prey can waste the hacker's time and resources by appearing to grant access to tempting material that proves impossible to extract – this is evident in the deployment of honeypots in networks. Similarly, the use of honeytokens in some organizations allows hackers to steal bogus files or "beacons" that reveal information about the hackers.

The theorizing relationships and illustrative examples are important because demonstrate different ways in which the concepts of the theory relate to each other, as well as their analytical capacity to examine digital deception sufficiently. For instance, Trojan horses come in the form of seemingly legitimate files or software. In most cases, they are embedded in email attachments that the victim opens thinking that they come from a trusted source. Trojan horses are also capable of performing MITM attacks and can lay dormant in the victim’s computer for a long time. Hence, the analogy between the Trojan Horse and Trojan horses in computers serves as a solid conceptual platform that connects a variety of concepts such as deception, camouflage, chameleonism, resourcefulness, opportunism, ploy, and deceit.

DISCUSSION AND CONCLUSION

In light of the lack of a similar theory that encompasses a wide range of deception related behaviors, strategies and practices, it could be argued that deception as cunning intelligence attempts to explain “something that was poorly or imperfectly understood beforehand” – which is a key characteristic of a Type II theory [39]. Over the years, there has been considerable discussion (and disagreement) among information systems researchers on what constitutes theory – and more specifically, good theory [39-42]. This research aspires to develop theory that is “woven into a logical story that explains the ‘why’ behind observed connections in the proposed elements of the theory (and world)” [39, p.42]. There are several methodological challenges associated with this effort that are acknowledged and partially or fully addressed in this conceptualization paper.

The conceptualization of digital deception as cunning intelligence seems to have the analytical capacity to explain how different aspects of false statement, misrepresentation, or deceitful conduct come into play in information security and information security management. This is evident in a variety of

security-related activities that apply some form of deception, such as social engineering (e.g. pretexting, phishing, intelligence gathering), Man-In-The-Middle (MITM) attacks (e.g. ARP cache poisoning, DNS spoofing, HTTP session and SSL hijacking), SQL injection, keylogging, honeypots and honeytokens, and decoy I/O devices [5]. Digital deception as cunning intelligence can also be applied to the different ways in which malware can get installed, cause harm and attempt to remain undetected in a victim computer (e.g. polymorphic and metamorphic code, virus analysis resistance). Other key aspects of digital crime, such as the motivation of attackers or their psychological profiling, are beyond the scope of this paper. Instead, the line of research presented here is concerned with the examination of patterns that have led to digital crime incidents, in an effort to 'design out crime' and develop intelligence-led security strategies [43, 44].

Digital deception as cunning intelligence could prove to be a useful tool for the classification of information security attacks based on the type of deception that is employed each time. Along with the design of relevant deception-based countermeasures, the theory points out the attributes of deception that are being used and combined in a particular digital crime. For instance, in spear-phishing attack, there are elements of camouflage (e.g. concealing the real identity of the sender), resourcefulness (e.g. harvesting the contact details of trusted business partners and associates), and opportunism (e.g. sending out e-mail communication during business hours or asking for a follow-up to a specific event), among others.

Such identification and matching of attributes raises key questions regarding the overall contribution of the theory. First, how can we improve the design of spear-phishing counter-measures, knowing that these attributes of deception are at play? Second, could there be other attributes of deception that attackers could potentially use in future spear-phishing attempts? And, if that is the case, how can we better protect against them? Third, does the degree of digitality and novelty of a particular digital crime [45] have an effect on the attributes of deception that attackers are employing to commit said crime? Naturally, these questions cannot be answered in the Conceptualization phase of the GMTB, which is covered in this paper. But they will need to be addressed in the Operationalization and Application phases of the theory development process.

Going forward, this paper will be used as initial input towards the completion of the remaining phases of the GMTB. As discussed earlier in the current section, the refinement of the conceptualization of digital deception as cunning intelligence (particularly in the Operationalization and Application phases of the GMTB), may benefit greatly from the input of industry practitioners such as IT security managers, system administrators and ethical hackers. Such dialogical relationship with practitioners is an integral part of theory building in applied disciplines, but also of any effort to develop current and relevant theory in a field such as information systems [46]. As part of the Operationalization phase, a Delphi study that comprises seasoned security practitioners and former hackers will seek to refine the list of attributes of digital deception, and their importance for offensive and defensive security operations. If the completion of this phase produces any testable propositions of the theory, these propositions will need to be empirically tested during the Confirmation or Disconfirmation phase as per the generalizability requirements of Lee and Baskerville [42].

REFERENCES

References available upon request from the author(s).