Building a Theory of Socio-technical Fraud

Emergent Research Forum paper

Spyridon Samonas
California State University, Long Beach
ssamonas@gmail.com

Abstract

In the last decade, there has been an unprecedented global adoption of information and communication technologies. While developed countries are more attractive targets and suffer significantly higher losses to cyber-crime as a percentage of their Gross Domestic Product, developing and least-developed countries countries are more vulnerable. Phone-based scams such as phreaking and caller identity spoofing are instances of cyber-fraud, theft and forgery that are very widespread in these countries. Interestingly, deception is at the heart of these cyber-crimes. This paper acknowledges the extant literature on deception detection and the contribution of the related theories of deception, but proposes the development of a theory that treats cyber-deception and fraud as fundamentally socio-technical phenomena. Drawing on Humanities and the socio-anthropological concept of 'cunning intelligence', we aim to develop an explanatory lens of fraud that can be applied to different types of cyber-crime.

Keywords

Cunning intelligence, fraud, deception, cyber-crime, socio-technical security.

Introduction

Over the last decade, there has been an unprecedented global adoption of information and communication technologies (ICT). The cyber-divide has shrunk, and now, more than 40% of the world's population has access to the Internet (Intel Security, 2015). However, modern ICT have opened Pandora's Box. The interconnectedness and convenience of technologies such as the Cloud and the Internet of Things do not only assist the execution of traditional fraud schemes, but have also enabled the rise of new ones. An Intel Security-commissioned study estimated the annual cost of cyber-crime to the global economy between 375 and 575 billion US dollars (CSIS, 2014).

While developed countries are more attractive targets and suffer significantly higher losses to cyber-crime as a percentage of their Gross Domestic Product (GDP), developing and least-developed countries countries are more vulnerable. In the latter group of countries, cyber-criminals continue to focus on the extremely popular mobile telephony platforms. Besides opportunities for small and medium enterprises, voice and data communications offer better communications and greater access to information to millions of people (WTO, 2013). However, as developing and least-developed countries constantly increase their Internet access, e-commerce and social media presence, cyber-crime will be taking a much higher toll on their GDP (CSIS, 2014). Phone-based scams such as phreaking and caller identity spoofing are not the only types of cyber-crime that are prevalent in developing and least-developed countries. Phishing and spear-phishing, computer-enabled advanced fee fraud and identity fraud, are also instances of cyber-fraud, theft and forgery that are brought about by a variety of malevolent uses of ICT.

Interestingly, deception is at the heart of every recorded type of cyber-fraud, theft and forgery. This paper acknowledges the extant literature on deception detection and the contribution of the related theories of deception; however, it treats cyber-deception and fraud in the developing world as fundamentally socio-technical phenomena. Drawing on Humanities and the socio-anthropological concept of 'cunning intelligence', this research will develop a generalized theory of fraud that can be applied to different types of cyber-crime in developing and least-developed countries. The theory under development aims to provide an explanatory lens of cyber-fraud based on the *modus operandi* of known cyber-crimes. In this

effort, the research adopts a crime science perspective to postulate patterns that have led to cyber-fraud incidents, aspiring to understand how this knowledge can be used to prevent or control crime and disorder (Clarke, 2004; Hartel et al., 2011).

Following a review of the existing literature, the rest of the paper outlines the key presuppositions and methodological aspects of this ongoing research project.

Extant Literature

Cyber-crime and deception

Computer-related crime can be considered a ubiquitous variant of all crime (Dhillon et al., 2004). In this respect, the term 'cyber-crime' is commonly used as an overarching concept that encompasses so many different actions and incidents pertaining to crime. As Wall (2007, p.10), argues, the term 'cybercrime' tends to be used "metaphorically and emotionally rather than scientifically or legally." In an effort to assess the application and use of technology in crime from a criminological standpoint, Wall (2004) suggests that 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 ICT and they are only possible due to the latest advances of technology. What makes a crime *more* or *less* digital depends on the digitality and novelty of that crime (Bryant and Bryant, 2014). In fact, a variety of factors needs to be taken into account, such as the virtuality of the crime in terms of space and time, the ability of the criminal to conceal their identity and the accessibility and proximity to the victim, also need to be taken into account (Bryant and Bryant, 2014).

Similarly, drawing on Furnell (2002), Yar (2005) suggests that cyber-crime can be distinguished into 'computer-assisted' and 'computer-focused' crime. The former type of crime includes 'traditional crime' that pre-dated the Internet and is still being committed with the help of computers (Hartel et al., 2010), such as fraud, theft or money laundering (Yar, 2005). The latter type refers to the 'criminogenic' features of computers and networks (Hartel et al., 2010), and specifically to those crimes that essentially have a parasitic relationship with technology and the Internet, such as hacking or viral attacks (Yar, 2005).

Within the context of cyber-crime, the practice of deception has been widely associated with social engineering (see Mitnick and Simon, 2011) and masquerade detection (Huang and Stamp, 2011). However, it is a phenomenon relevant to various disciplines such as psychology (see Ioannou and Hammond, 2015), forensics (see Tsikerdekis and Zeadally, 2014), information systems (see Fuller et al., 2009), and computer science and engineering (see Abouelenien et al., 2014). Over the past 50 years, research in this topic has been preoccupied with the study of lying and the detection of lies (Hartwig and Granhag, 2015). 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 (2015) 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 (see Serota et al., 2010), and the capacity of people to distinguish between true and false statements (see Vrij, 2008).

Conceptual Framework

The concept of cunning intelligence can be traced back to the Ancient Greek and Chinese civilizations. 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 (1978), and more recently, Raphals (1992), Vidal-Naquet (1998) and Wanner (2009), 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. It is applied to situations that are transient, shifting, disconcerting and ambiguous, where precise measurement, exact calculation or rigorous logic are not always applicable. Cunning intelligence is a mental category that encapsulates various qualities: Human

deception, camouflage, resourcefulness, sharp-wittedness, skilful craft, speed of thought and action, self-sufficiency, and the seizing of opportunities.

Although this type of intelligence is discussed on numerous occasions in the Ancient Greek and Chinese literature – for instance, in the travels and deceits of Ulysses, the rhetorical devices used by the Sophists, or the shape shifting of various deities – the fact that there was no explicit mention of it led scholars to ignore its significance for many years. Ancient Greeks treated animals such as the fox, the cuttlefish and the octopus as primordial fraudsters. 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.

Drawing on the Ancient Greek literature, Vidal-Naquet (1998) examines cunning intelligence by highlighting the contrasting approach that Athens and Sparta followed in the military training of young men. Athenian *hoplites* were 18-20 year olds trained in a socially organized, structured program based on order that would prepare them to become citizens of a civilized world. For Spartans, on the contrary, compulsory military training was based on disorder and irrationality and started at the age of six. Around the age of eighteen, the rite of passage to adulthood included surviving the cold winters with minimal clothing and no food or water, as well as hunting animals and *helots* – Sparta's serfs, against whom the Spartan leaders would declare war every year – without fear of punishment.

Similarly, Raphals (1992) builds on the work of Detienne and Vernant (1978) to discuss cunning intelligence in classical Chinese culture and society. She examines Chinese conceptualizations of wisdom, craft and knowledge based on early theories of language, and argues that issues of language and knowledge were central to considerations about statecraft, warfare, as well as personal and social morality. Cunning intelligence underpins many aspects of the Chinese philosophical tradition, and there are, indeed, striking similarities in the way in which the Ancient Greeks and the Ancient Chinese weaved their legends, myths and stories. Further evidence of this type of intelligence is also provided by Wanner (2009) in his study of Norse myths.

Theorizing Relationships

To examine the analytical capacity of cunning intelligence as a theoretical platform for the study of cyber-crime and cyber-fraud, we juxtapose key qualities of cunning intelligence (as these were identified in the Ancient Greek literature) with cyber-crimes that involve fraud and deception. More specifically, we present an elementary comparative concept analysis between the deceit of the Trojan Horse and the activities of fishing and hunting on the one hand, and trojan horses, phishing and hacking, on the other. The three sub-sections below summarize the characteristics and skills of the predator and the prey for each set using illustrative examples: Trojan Horse and trojan horses; fishing and phishing, hunting and hacking.

Trojan Horse and trojan horses

In the Ancient Greek literature, the Greeks applied deception to sneak undetected soldiers hidden in the wooden horse and inside the walls of Troy to surprise the enemy. The people of Troy, who are in this case the prey, believed that the wooden horse was a gesture of good will and accepted the gift without suspicion.

In the world of cyber-crime, deception is also applied in the development, distribution and execution of trojan horses. Advanced malware such as ZeusVM has used steganography to conceal its configuration file within an image file. In other cases, advanced banking malware such as GameOver applied deception to remain undetectable from anti-virus software. In both cases related to trojan horses, users (as prey) were deceived into downloading and opening what they considered was legitimate and trusted material, or the malware was installed on their machine as part of a drive-by download.

Fishing and Phishing

In Ancient Greece, men were hand gathering, spearing, netting, angling and trapping fish to provide for their families. Fish were also running the risk of falling prey to other fish that were higher in the pecking

order. As a prey, fish would use a variety of counter-measures to protect themselves from predators (men and other fish). These counter-measures included camouflage (chameleonism and countershading), the projection of ink (this is very typical of cephalopods), speed to avoid the predator, poison administered through their teeth, spines or barbs, electric shock (this is typical of the electric eel), as well as special chemicals released right before the predator kills or captures the prey.

In the context of phishing, the predators prepare and send out targeted and personalized electronic messages and texts that attempt to steal identity information such as login credentials and personal identification numbers. Assuming the role of the prey, a lot of people respond to such requests because they seem credible, interesting or familiar.

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. In the role of the prey, organizations develop military-style strategies to defend their information resources and, in certain cases, fight back. 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, some organizations allow intruders to steal bogus files or "beacons" that reveal information about the hackers.

Conclusion

Cunning intelligence as a frame of mind could provide valuable insights as to how, when and where cyber-crimes that involve fraud occur. This involves thinking like a cyber-criminal and articulating the variety of considerations, decisions and actions that attackers take prior, during and after the execution of a cyber-crime. In the context of Gregor's (2006) taxonomy of theories in IS research, the theory under development is mainly explanatory. Various aspects of causality that pertain to the motives of the cyber-criminals in developing and least-developed countries are beyond the scope of the theory. Instead of adopting a criminological stance that would examine this causality, the proposed project revolves on crime science to perform a problem-oriented analysis of known cyber-crime patterns. Crime science seeks to 'design out crime' and develop intelligence-led security strategies (Clarke, 2004; Junger et al., 2012). The application of cunning intelligence to cyber-attacks could explain how different aspects of false statement, misrepresentation, or deceitful conduct come into play in cyber-crimes. These considerations can also provide insights for the development of intervention strategies that minimize the occurrence of cyber-fraud and deception in the developing and least-developed world.

REFERENCES

Abouelenien, M., Pérez-Rosas, V., Mihalcea, R. and Burzo, M. 2014. "Deception detection using a multimodal approach," in *Proceedings of the 16th International Conference on Multimodal Interaction* (ICMI '14), ACM, New York, NY, USA, pp. 58-65.

Bryant, M. S., and Bryant, R. 2014. *Policing Digital Crime*. Ashgate Publishing, Ltd.

Clarke, R.V. 2004. "Technology, criminology and crime science". *European Journal on Criminal Policy and Research*, (10:1), pp. 55-63.

CSIS - Center for Strategic and International Studies. 2014. "*Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II*", http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf, last accessed on March 1, 2016.

Detienne, M., and Vernant, J. P. 1978. *Cunning intelligence in Greek culture and society*. Hassocks: Harvester Press.

Dhillon, G., Silva, L. and Backhouse, J. 2004. "Computer crime at CEFORMA: a case study", *International Journal of Information Management*, (24:6), pp. 551-561.

Fuller, C. M., Biros, D. P., and Wilson, R. L. 2009. "Decision support for determining veracity via linguistic-based cues," *Decision Support Systems* (46:3), pp. 695-703.

Furnell, S. 2002. *Cybercrime: Vandalizing the information society,* Addison Wesley, London.

Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS Quarterly* (30:3), pp. 611-642.

Hartel, P. H., Junger, M. and Wieringa, R. J. 2011. *Cyber-crime Science = Crime Science + Information Security, Technical Report TR-CTIT-10-34*, Centre for Telematics and Information Technology University of Twente, Enschede, http://eprints.eemcs.utwente.nl/18500/03/0_19_CCS.pdf, last accessed on March 1, 2016.

Hartwig, M. and Granhag, P.A. 2015. "Exploring the Nature and Origin of Beliefs about Deception," In *Detecting Deception: Current Challenges and Cognitive Approaches*, P. A. Granhag, A. Vrij, A. and B. Verschuere, (eds.) John Wiley & Sons, pp.123-154.

Huang, L. and Stamp, M. 2011. "Masquerade detection using profile hidden Markov models". Computers & Security, (30:8), pp. 732-747.

Intel Security. 2015. *McAfee Labs Threats Report - August 2015*, http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf, last accessed on March 1, 2016.

Ioannou, M. and Hammond, L. 2015. "The Detection of Deception Within Investigative Contexts: Key Challenges and Core Issues", *Journal of Investigative Psychology and Offender Profiling* (12:2), pp. 107–118.

Junger, M., Laycock, G., Hartel, P. and Ratcliffe, J. 2012. "Crime science: editorial statement". *Crime science*, (1 :1), pp. 1 - 3.

Levine, T. R. 2015. "New and improved accuracy findings in deception detection research", *Current Opinion in Psychology*, (6), pp. 1-5.

Mitnick, K.D. and Simon, W.L. 2011. *The art of deception: Controlling the human element of security*, John Wiley & Sons.

Raphals, L. A. 1992. *Knowing words: Wisdom and cunning in the classical traditions of China and Greece*. Cornell University Press.

Serota, K. B., Levine, T. R., and Boster, F. J. 2010. "The prevalence of lying in America: Three studies of self-reported lies". *Human Communication Research*, (36:1), pp. 2–25.

Tsikerdekis, M. and Zeadally, S., 2014. "Multiple account identity deception detection in social media using nonverbal behavior", *IEEE Transactions Information Forensics and Security*, (9:8), pp. 1311-1321.

Vidal-Naquet, P. 1998. *The black hunter: Forms of thought and forms of society in the Greek world*, JHU Press.

Vrij, A. 2008. *Detecting lies and deceit: Pitfalls and opportunities (2nd ed.)*, New York, NY: John Wiley & Sons.

Wall, D. 2001. "Cybercrimes and the internet", In *Crime and the internet*, D. Wall, (ed.), Routledge, London.

Wall, D. 2007. *Cybercrime: The transformation of crime in the information age*, Polity.

Wanner, K. J. 2009. Cunning Intelligence in Norse Myth: Loki, Óðinn, and the Limits of Sovereignty. *History of Religions*, (48:3), pp. 211-246.

WTO – World Trade Organization. 2013. "*Electronic Commerce, Development and Small, Medium-sized Enterprises: Background Note by the Secretariat*", https://www.wto.org/english/tratop_e/devel_e/wkshop_apr13_e/w193_e.doc, last accessed on March 1, 2016.

Yar, M. (2005) The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory, *European Journal of Criminology,* (2:4), pp. 407-427.