Chapter 1
Cyber + Culture:
Exploring the Relationship

Char Sample
U.S. Army Research Laboratory, USA

Jennifer Cowley
U.S. Army Research Laboratory, USA

Jonathan Z. Bakdash
U.S. Army Research Laboratory, USA

ABSTRACT

Technical advances in cyber-attack attribution continues to show incremental improvement. A growing interest in the role of the human in perception management, and decision-making suggest that other aspects of human cognition may be able to help inform attribution, and other aspects of cyber security such as defending and training. Values shape behaviors and cultural values set norms for groups of people. Therefore, they should be considered when modeling behaviors. The lack of studies in this area requires exploration and foundational work to learn the limits of this area of research. This chapter highlights some of the findings of some of the recent studies.

INTRODUCTION

The cybersecurity environment has only recently considered the role of behavioral science in explaining cybersecurity events. This addition of behavioral science disciplines will allow analysts and researchers the opportunity to gain fresh insights into these events. The addition of cultural studies to this mix provides context for these insights (Morgan, Cross & Rendell, 2015; Wang, 2016), thereby adding valuable understanding to the analysis.

Morgan et al. (2015) noted that cultural values and preferences are easily transmitted during the learning process, including copying behaviors when uncertain, rewarding conformist behaviors, and examining social learning, thereby providing an explanation of event evaluation context. Morgan et al. (2015) are

DOI: 10.4018/978-1-5225-7909-0.ch001

not alone in maintaining these views on contextual evaluation. Others (Henrich, Heine & Norenzayan, 2010; Hofstede, Hofstede & Minkov, 2010; Nisbett, 2010; Schwartz, 2012; Shewder, 1998) have voiced similar views, and, more recently, Wang (2016) has called attention to the importance of cultural context. The context that culture provides results in actions or outcomes that may seem normal for some (Minkov, 2011) but are viewed as abnormal or incomprehensible for others (Fiske & Taylor, 2013).

Wang (2016) discussed the importance of a cross-discipline approach that requires the understanding of cultural values for psychology, a view shared by Nisbett (2010), Henrich et al. (2010), Hofstede et al. (2010), Schwartz (2012), and Shewder (1998). Other disciplines such as education, business management, and marketing recognize the value of incorporating cultural understanding into the body of knowledge. In recent studies, research into information technology usage has considered the role of culture, and, more recently, cybersecurity studies are considering the importance of cultural values (Almeshekah & Spafford, 2014; Elmasry, Auter & Peuchaud, 2014; Henshel, Sample, Cains & Hoffman, 2016).

Inclusion of cultural analysis in cross-discipline research runs the risk of analysts importing their own cultural views into their analysis (Fiske & Taylor, 2013; Van de Vijer & Leung, 1997). Fiske & Taylor (2013) noted that individuals were better able to detect cultural biases outside of their own cultural group, but they were unable to do so as effectively within their own group. These observations by Fiske & Taylor (2013) along with Minkov (2011) underscore the role of cultural values in human cognition and the difficulty in preventing cultural values from informing analysis. However, this challenge should not discourage researchers, especially in cybersecurity research where the environment includes the global Internet.

Culturally aware observations have not yet been widely incorporated into cybersecurity analysis, where the emphasis relies on technical details, and behavioral science disciplines have not yet been fully integrated. The global participation of different actors implies the need for cultural analysis into cyber behaviors and events. Although the addition of psychology is welcome and needed for cybersecurity analysis, sociology provides context for this analysis.

Recently Wang (2016) called attention to the role of culture in psychological evaluation of findings. We aim to extend theories of cultural psychology to a more applied setting in order to evaluate cyber actors. We have reason to believe that cultural values can be a grouping factor for human behavior in various environments, including the virtual environment that defines cyber. Minkov's (2011) observation that culture influences individual thoughts even when the individual believes in self-determination implies that cultural values can describe and predict human behavior in various environments including the virtual environment. In the virtual environment, the human actors regularly engage in thought, and knowing that culture influences thought, a reasonable expectation that cultural values may influence cyber behaviors deserves further investigation.

Nisbett (2010) documented the East versus West differences in perception and environmental interaction. Henrich et al. (2010) observed that the majority of psychological studies were performed on students who were from Western educated, industrialized, rich and developed (WEIRD) countries, and, of these WEIRD countries, the United States provided the majority of subjects. Therefore, the findings are skewed toward the cultural values of WEIRD students from the United States.

Historically, non-cyber disciplines have assessed the capability of culture to predict or explain human behavior (Hofstede et al., 2010; Nisbett, 2010; Schwartz, 2012), but recently cybersecurity and other computing sciences have begun investigating culture as a potential grouping factor to predict or explain cyber behavior (Henshel et al., 2016; Sample, Cowley, Watson & Maple, 2016; Sample, Cowley, Hutchinson, 2017; Sample & Karamanian, 2015). Cybersecurity is a global interdisciplinary endeavor.