Chapter 11

The Electronic Hive Mind and Cybersecurity:

Mass-Scale Human Cognitive Limits to Explain the "Weakest Link" in Cybersecurity

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT

If people are the "weakest link" in cybersecurity because of their psychological make-up and hardwiring—their socialized desire to trust and cooperate with others, their cognitive biases and misperceptions, their preferences for convenience, their general going with System 1 inattention instead of System 2 attention and thinking—this begs the question of whether the same micro-scale cognitive limits found in individual users are also present on a mass scale. After all, there have been discovered problematic unthinking leanings in group decision making: obedience to authority, bystander effects, groupthink, and the Abilene paradox, among others. Using a range of often mass-scale data sources and data analytics tools, research questions were asked around three areas: (1) the level of sophistication of the cybersecurity electronic hive mind towards cybersecurity issues, (2) the gap between the non-expert members and the expert members in the hive mind, and (3) whether the extant hive mind was more reflective of mob unthinkingness or deliberation and wisdom.

INTRODUCTION

In every chain of reasoning, the evidence of the last conclusion can be no greater than that of the weakest link of the chain, whatever may be the strength of the rest. – Thomas Reid in Essays on the Intellectual Powers of Man – (1786)

A chain is only as strong as its weakest link. – a common saying

DOI: 10.4018/978-1-5225-5927-6.ch011

Intelligence is highly improbable, and collective intelligence is even more so. It runs into misinformation, misjudgment, and misunderstanding. This is unavoidable because thinking is a site for conflict, tactics, and strategies. Insight jumps out of the clash of argument as well as linear discovery of truths. – Geoff Mulgan (2018), in Big Mind: How Collective Intelligence Can Change Our World (p. 126)

Online is where a large portion of the world's population live and breathe and have their being. As the cyber footprint is broadened—through mobile devices, locational apps, games, smart cars, medical devices, and the Internet of Things (IoT)—there are that many more potential attack surfaces through which people may be affected negatively through hacks and cyberattacks. Adam Segal (2016) writes: "An estimated 75 percent of the world's population now has access to a mobile phone, and the Internet connects 40 percent of the planet's population, roughly 2.7 billion people. Information and communications networks are embedded in our political, economic, and social lives." (p. 1). He predicts an intensification of the battle over cyberspace, with Year Zero of this battle starting June, 2012 or June, 2013, given a number of high profile uses of cyberattacks by nation states. In 2016, there were four billion cyberattacks, a major jump from the 600 million in 2015 (IBM, as cited in Balaish, Aug. 21, 2017). By 2021, cyber crime is estimated to cost US$2 trillion (Cybersecurity Ventures, as cited in Balaish, 2017). Cybersecurity efforts focus on preventing the illegal exploitation of technology systems and the protection of data integrity, among other things.

In cybersecurity studies and practices, humans are known as "the weakest link" (Belbey, 2015); their decisions and actions put their information at risk and also those of others. Humans will use and re-use weak passwords or leave passwords unchanged from factory defaults; they over-share with friends, family, and strangers; they click unthinkingly on risky links and download files (with malware) from others; they will receive emails from strangers or apparent colleagues and click on links or download files without thinking; they'll receive USB drives at conferences and use these in their laptops and desktops; they'll download apps from unknown websites; they will visit the Web's dark spaces to buy illicit goods; they're prone to being social engineered; and they do not begin to understand the "cyber" threats arrayed against them.

One way to begin to understand why people are so vulnerable to cyber-exploitation is to not only explore people and their individual cognitive limits and biases but also to explore the "electronic hive mind" around cybersecurity to understand mass-scale human cognitive limits and biases. A "mind" refers to consciousness, thinking, intellect, and will. A "hive mind" refers "group intelligence" (Jones, 2011, p. 2). A hive mind refers to the consciousness, thinking, intellect, and will of a collective of people. Such collectives occur organically, with people coming together around shared interests. A core purpose of a hive mind is to learn from the environment, from others outside the hive, and from each other. Bloom's taxonomy of learning domains types (1956) can apply to group intelligence: the steps include remembering, understanding, applying, analyzing, evaluating, and creating. (Conceptualize teams collaborating around shared research and design and development work.) As in learning communities, consensus and dissensus are both important. Certainly, if hive minds can function like individual ones, they can also be misled, misinformed, irrational, and deluded.

A hive mind does not have centralized control; rather, control is distributed and devolved, with each member and small groups within the collective making decisions, sharing ideas, and taking actions. How these hive minds coalesce and evolve is determined in part by the group impetuses and interests, and evolved social norms. Hive minds can be informed by co-created culture. In the same that that the