Chapter 17
Safe Distances:
Online and RL Hyper-Personal Relationships as Potential Attack Surfaces

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT

Online human-to-human (and human-to-robot) hyper-personal relationships have evolved over the years, and their prevalence has broadened the available cyberattack surfaces. With the deployment of malicious socialbots on social media in the virtual and AI-informed embodied socialbots in the real, human interests in socializing have become more fraught and risky. Based on the research literature, abductive reasoning from in-world experiences, and analogical analysis to project into the Fourth Industrial Revolution, this work suggests the importance of greater awareness of the risks in interrelating in the virtual and the real and suggests that there are no safe distances.

INTRODUCTION

Only amateurs attack machines; professionals target people. And any solutions will have to target the people problem, not the math problem.

Bruce Schneier (Oct. 15, 2000, in "Semantic Attacks: The Third Wave of Network Attacks" on Schneier on Security blog)

Professional intelligence services hunting for prospective candidates for espionage now have Internet-enabled spotting, developing, and recruiting tools that work just as effectively for professional handlers seeking candidates to manipulate into espionage as they do for retailers seeking to target customers susceptible to advertising.

Dr. Ursula M. Wilder, in "Why Spy Now? The Psychology of Espionage and Leaking in the Digital Age" (2017)

DOI: 10.4018/978-1-5225-7909-0.ch017

It's always about sneaking up on people. It's always about getting there first, right? It's always about blocking the other side. And so, tactics don't change all that much. It's getting the jump on your enemy. It's not letting the enemy in your own ranks, whether it's cyber-wise or having a spy in there…Everybody had to worry about what your enemy was doing and whether they're going to infiltrate you. And that is true today because I don't care how many spy planes you have, how many satellites you have in the sky, how many computers you have running, in "humint" (human intelligence), it only takes one guy with the codes to screw up $20 billion worth of equipment…If you constantly rely on the technology to protect you, and you take your eye off the individual, it's somebody behind a curtain, it's the guy next to you wearing the old-school tie that you thought was so trustworthy, those are the people you have to keep your eye on because that's the Trojan Horse.

Col. (and Dr.) Rose Mary Sheldon, in "Ancient Espionage: The Greeks and the Great Game" (Oct. 20, 2017), when asked how ambush tactics described in her presentation apply to cyberwarfare

To use a technology-based concept, humans interface with the world around them, and they interface with each other. The drive for human connection is so powerful that people are willing to put at risk their sense of self-respect and their resources and their reputations in order to engage. On social media, they "friend" and "follow" socialbots at scale, with a majority not realizing that they are not interacting with humans on the other end but simple artificial intelligence (AI) or cyborg accounts (mixing script and human interactions). This challenge of how humans interact with both each other and with social robots only intensifies with the advent of the Fourth Industrial Revolution. Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, writes:

The First Industrial Revolution used water and steam power to mechanize production. The Second used electric power to create mass production. The Third used electronics and information technology to automate production. Now a Fourth Industrial Revolution is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.

The world envisioned in this age involves humans augmented by heightened perceptions (like access to their own and others' thoughts based on electronic signals in their brains), empowered by exoskeletons to achieve speed and power not available otherwise, medical interventions that can prolong life and its enjoyment, and other seductive technologies. The melding of AI-informed human personalities into embodied socialbots is a capability that is already extant, and combined with human nature in its observed forms, the risks to humans are magnified. Before springing forward into the near-future, however, it may be helpful to explore what attempts at cyber-compromise may look like with current technologies. What follows are four non-fictional scenes of relation-based attempts to achieve cyber-compromise. In three of them, the author is the target. In one, a colleague is engaging in her own cyber-compromise and potentially that of her colleagues (including the author).

Real Scenes of Relational Risks

"Relational risks" are generally understood as those that emerge from people interacting with others, in both mediated and non-mediated ways.