Chapter 75
Death by Hacking:
The Emerging Threat of Kinetic Cyber

Penelope Wang
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

ABSTRACT

Innovation and technological advancements have seen many devices and systems being linked up on to the Internet. Such devices and systems include personal medical devices like insulin pumps and pacemakers, cars, as well as critical infrastructure like power grids and traffic light systems. However, recent research by cyber security experts has revealed that these critical devices and systems are highly vulnerable to being hacked into and manipulated. Should such an attack be carried out successfully by bad actors, like violent extremists, this could result in physical injury or even death. Hence, this chapter aims to bring awareness on the kinetic cyber threat by highlighting various forms of kinetic cyber, and the vulnerabilities that make these devices and systems susceptible. In addition, this chapter introduces the motivations and characteristics of violent extremists who might engage in kinetic cyber, and ends off by proposing some recommended directions to counter this threat.

INTRODUCTION

The rapid technological advancements in the past few decades have brought about massive improvements and breakthroughs in many sectors of society. From the enhancement of medical devices to the creation of smart homes and smart cars as well as the implementation of technology to monitor and regulate basic systems in infrastructure, technology has indeed pervaded every aspect of the world today. Nevertheless, the benefits and convenience that technological advancements bring is not without its perils. With the rise of technology, a corresponding increase in cybercrime rates can also be observed (Mendoza, 2014).

However, the face of cybercrime is changing, and cyber attacks need not necessarily be confined to non-violent acts. The possibility for cyber attacks to cause direct or indirect physical damage, injury and even death is very real. In view of this threat, former Vice President of the United States, Dick Cheney, had had the wireless function of his pacemaker turned off for fears of an assassination attempt that can be made by remotely hacking into his pacemaker (Peterson, 2013).

DOI: 10.4018/978-1-5225-8897-9.ch075

According to Applegate (2013), the classification of these kinds of cyber attacks is known as 'Kinetic Cyber'. The threat of kinetic cyber could be more imminent than commonly believed. Europol has picked up a report by U.S. security firm, IID, which predicted that the first murder via the hacking of critical devices would happen by the end of 2014 (Peachy, 2014a). To date, while there has yet to be a murder conducted via kinetic cyber, there have been cases where kinetic cyber was used to attack and damage critical infrastructure. Given the myriad of possible attacks that could be made to cause widespread damage, it is not unthinkable then, that violent extremists could use kinetic cyber as a tool to achieve their own ends. This is especially since violent extremist groups are known to keep up to date with the latest technology and to exploit them where possible, as is the case with Al-Qaeda using encrypted and secure communications methods to conceal their tracks (The Soufan Group, 2013), as well as the Islamic State in Iraq and Syria (ISIS) using social media as an effective digital strategy to recruit members online (Bonzio, 2014).

The objective of this chapter therefore is to raise awareness of the emerging threat of kinetic cyber through highlighting the types of kinetic cyber and how such cyber attacks are carried out. In addition, this chapter seeks to outline the possible offender profiles of individuals, including violent extremists, who might engage in kinetic cyber, and provide a few recommendations on how to address this emerging threat.

TYPES OF KINETIC CYBER

In general, the primary targets for kinetic cyber are cyber-physical systems (CPS), which are computer systems that are designed to monitor and control physical processes (Applegate, 2013). The use of CPS can be found in a wide spectrum of industries, ranging from personal medical devices, automotive systems, traffic control and safety systems, to critical infrastructure control systems like electric power and water resources (Lee, 2008). The fact that these systems are connected to the cyberspace implies that they could potentially be hacked into and manipulated for purposes other than what they were originally intended for (Applegate, 2013). The idea that CPS are vulnerable to attacks is not a fantastical notion commonly found in the domain of film or television shows, but instead a very real threat that has been validated by security researchers in real life.

Hacking Into Implanted Medical Devices

The primary advantage of incorporating wireless technology into implanted medical devices is to allow doctors to collect valuable patient information and modify the treatment accordingly as well as to update device software without the need to conduct surgery (Erlichman & Jack, 2012; Rubin, 2011; Wadhwa, 2012). However, when security features protecting these devices are insufficient, as is mostly the case (Higgins, 2014b), this leaves the devices vulnerable to cyber attacks. In fact, security researchers have experimented on and demonstrated how such attacks are possible.

In 2011, security analyst Jerome Radcliffe gave a presentation during the Black Hat Technical Security event on how he had hacked into his own continuous glucose monitor (CGM) and insulin pump. While he did not go so far as to manipulate the two devices he owned, he had outlined theories in which hackers could possibly manipulate the two devices. For an attack on the CGM, the goal for hackers would be to suppress legitimate sensor data from being picked up and simultaneously imitating sensor data in order