Chapter 28
US–China Relations:
Cyber Espionage and Cultural Bias

Clay Wilson
American Public University System, USA

Nicole Drumhiller
American Public University System, USA

ABSTRACT

It is assumed by most observers that China is copying or stealing vast amounts of intellectual property from US military and private industry through its cyber espionage activities, and then sharing that information with state-owned industries, giving them unfair economic advantages. The US also conducts cyber espionage against China and other nations, but chooses to not share the vast collections of intellectual property and data with its own domestic industries. By choosing not to do the same thing as China, the US may be placing itself at an economic disadvantage, and may also mistakenly be accusing China of threatening cyber warfare. What is needed is a clearer understanding of differences in national cultures that contribute to intolerance between the US and China when it comes to economics, threats of war, and the evolving new role of cyber espionage.

INTRODUCTION

In recent years relations between the United States and China have become strained over alleged instances of cyber related intellectual property theft and espionage. According to officials within the US Government, "The Chinese government has a national policy of economic espionage in cyberspace…", and, "…the Chinese are the world's most active and persistent practitioners of cyber espionage today." (McConnell, Chertoff, & Lynn, 2012). Some government officials believe that China's masses are simply hungry for economic advancement and that by stealing intellectual property (IP), China can quickly create products that are cheaper than similar items produced in the US and elsewhere. These officials warn that, over the next decade, cyber espionage could have a catastrophic impact on the US economy and global competitiveness (McConnell et al., 2012). Other U.S. military and business officials believe

DOI: 10.4018/978-1-5225-7912-0.ch028

that China has a long-term goal of "preemptive reconnaissance" intended to surpass the US economy and also affect US military planning (Thomas, 2010; Dilanian, 2011).

Former Attorney General Eric Holder reportedly stated that China has been actively hacking Westinghouse, US Steel, Alcoa and more than 60 other companies for half a decade (Hu, 2014). The McAfee security company stated in a February 2013 report that China has launched "coordinated covert and targeted cyber-attacks" against global oil, energy, and petrochemical companies since November 2009 (Barron-Lopez, 2014). U.S. officials have commented that Chinese cyber espionage is done to benefit its state owned companies. This characteristic is seen as outside the traditional bounds of espionage done for national security reasons (Michaels, 2014). Targets for cyber espionage also appear to align with China's stated economic and strategic directives. For example, in recent years the National Security Agency (NSA) and international groups watched as a group of privately employed engineers based in Guangzhou in southern China copied technology and blueprints for missile, satellite, space, and nuclear propulsion systems from businesses in the United States, Canada, Europe, Russia and Africa (Sanger & Perlroth, 2014). A clear distinction of Chinese behavior is that it blurs the lines between traditional espionage done for national security purposes, and economic theft of intellectual property directed against government and business entities. Defense consultant and author James Farwell reportedly stated in March 2013 that while espionage is not against international law, the theft and infringement of intellectual property is. Farwell even suggests that the situation is so egregious that the U.S. should initiate a case against China under the Trade Related Aspects of Intellectual Property Rights (TRIPS) agreement, stating that "… legal proceedings that found China guilty of intellectual-property theft or infringement, could render it liable for billions of dollars in compensation, expose it to multinational economic sanctions and cause it to be branded a pirate state" (McGregor, 2013).

Grievances over cyber espionage are also directed by China against the US and other countries. In particular, Beijing has accused the US of hacking its systems, claiming that Washington has long used the Internet to steal secrets. Reportedly, NSA monitored communications of top Huawei business executives looking for evidence of ties to the Chinese government and military. Huawei is based in China and is a global telecom company that ranks third to Apple and Samsung as a producer of mobile phones. The objective of the NSA surveillance program reportedly was to exploit Huawei's technology so that when the company sold equipment to other countries — including both US allies and other potentially hostile nations— the NSA could later choose to roam through their computer and telephone networks to conduct surveillance and, if ordered by the president, conduct offensive cyber operations. Recent news reports also describe cyber surveillance programs such as "PRISM" where the NSA, as part of its Signals Intelligence (SIGINT) mission, collected metadata for all telecommunications messages that transited the US involving foreign senders or receivers. In addition, the NSA reportedly has an electronic spying organization called the Tailored Access Operations, which has a mission to gather intelligence by specifically penetrating computers and telecommunications systems in China and other countries (Aid, 2013).

The United States response to the accusation from China shows how the US perceives its own behavior when conducting its own cyber espionage activities. White House spokeswoman Caitlin M. Hayden, reportedly said: "We do not give intelligence we collect to US companies to enhance their international competitiveness or increase their bottom line (Wallace, 2014; Sanger & Perlroth, 2014). The U.S. maintains this separation due to law that is in line with a general philosophy where the separation between public and private affairs means less regulation, which is viewed by many as healthy and generally good for business and innovation. Competitive intelligence is an ethical and legal business practice where information-gathering is done using open sources, such as newspaper articles, or corporate