

Chinese Espionage Threats to U.S. Security and Economic Interests

by

Jillian Spampinato

Honors Thesis

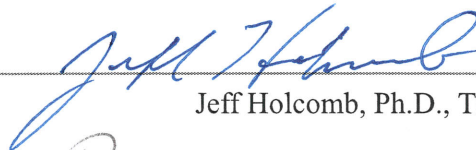
Appalachian State University

Submitted to the Department of Government and Justice Studies
in partial fulfillment of the requirements for the degree of

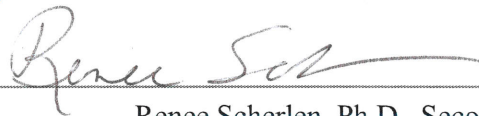
Bachelor of Science in Criminal Justice

August, 2023

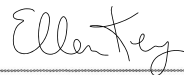
Approved by



Jeff Holcomb, Ph.D., Thesis Director



Renee Scherlen, Ph.D., Second Reader



Ellen Key, Ph.D., Departmental Honors Director

Chinese Espionage Threats to U.S. Security and Economic Interests

The last few decades have seen a sharp growth in China's economy, and it is widely recognized as the country who can best challenge the United States dominance as the world's strongest global power (Art, 2010; Ross, 2010; Punnoose & Vinodan, 2019). China's rise is largely credited to be the result of the government opening the economy to foreign investment in the 1980s (Punnoose & Vinodan, 2019; Khatoon et al., 2018). This allowed China access to modern technology and a market in need of cheap labor, which they could provide (Punnoose & Vinodan, 2019). Since then, China has taken further steps to expand economic and modernization progress with projects such as the Dream Policy initiatives which have sought to provide jobs and raise the standard of living (Khatoon, Rahim, & Ali, 2018). As well as an increasingly booming economy, China has also undertaken steps to modernize its military and military weapons system (Kwon, 2012). Both of these factors have contributed to what has been labeled the "rise of China" (Medeiros, 2009). This rise has led to an expansion in China's sphere of influence, not only in East Asia, but also in the larger global stage of international affairs (Medeiros, 2009; Art, 2010).

While China is now considered to be a global economic power with a large sphere of influence, its *Made in China 2025 Strategy*, a ten-year plan to reduce dependence on foreign nations' technology and increase domestically-made materials, reflects China's commitment to restoring itself as *the* dominant global power (Levine, 2020; Ross, 2010). Scholars have argued this rise in power will lead to China becoming more aggressive in pursuing their interests and might lead to an increase in illicit methods of obtaining information, such as through various forms of espionage (Shifrinson, 2020; Levine, 2020).

With China's stark rise, comes competition and tension with dominating states around the globe such as the United States (Art, 2010). Due to the country's rapid growth, China has now become the state best equipped to threaten the United States' dominance (Ross, 2010; Art, 2010). The progression and modernization of both the military and economic spheres in China are occurring at a more rapid pace than the United States, which has led to an ever-increasing Chinese sphere of influence that can be considered threatening to the United States' global position (Art, 2010; Ross, 2010). Many argue this pace of progression is due to the illicit gathering of foreign information which allows China to progress at a rate faster than normal (Levine, 2020). While China has experienced a steep and rapid progression in modernization and economic growth, its military capabilities have not undergone the same pace of expansion (Ross, 2010). This means that, for now, the United States is still the leading military power; however, with the ever-increasing economy, China could potentially funnel these funds into their military, lessening the gap in military capabilities between the two nations in maritime East Asia (Art, 2010). A top concern for the United States is the measures China will take and has taken to make up for the gap in technology and military capabilities between the two countries, as China has shown to have no qualms with obtaining this information illicitly (Levine, 2020). Even if China does not completely replace the United States as one of the top global powers, it is inevitable that the U.S.'s global influence will diminish. This notion has many Americans, especially conservative voices, concerned about being overtaken and replaced by China (Art, 2010; Kwon, 2012).

In the past, when one state's gaining of power has resulted in the loss of power and influence of another dominating power, this often led to high tensions and war (Art, 2010; Shiffrinson, 2020). Because the country's *Made in China 2025* plan directly states their goal

as returning China to its “rightful place” as top global power, tensions with the current dominating power are bound to be high (Levine, 2020). This is not to say that war between the United States and China is inevitable. Some argue that China’s rise is not a direct geopolitical threat and many of the country’s goals are not as dissimilar to the U.S. (Kwon, 2012). Therefore, it is not certain that tensions and competition will result in war (Art, 2010; Shiffrinson,2020; Kwon, 2012). Nevertheless, those who are worried about the rise of China and its impact on the United States have suggested measures that would thwart or decelerate progression such as preventing exports from China to the U.S., a tactic used against the Soviet Union during the Cold War (Art, 2010). Today, however, utilizing these methods could be construed as waging an unprovoked economic war against China, which could have negative consequences for the United States (Art, 2010).

While an all-out war between the United States and China is unlikely at this time, tensions have risen (Art, 2010; Shiffrinson, 2020). With China’s rapid rise and modernization has also come more aggressive acts taken by the Chinese to ensure its reinstatement as top global power (Levine, 2020). Some note that it is not a coincidence that the *Made in China 2025 Strategy’s* goal of increasing technology manufactures in the global marketplace coincided with an increase in hacking and espionage (Hough. & Malik, 2021; Eftimiades, 2019; Levine, 2020). The United States, in particular, has been the target of almost half of China’s espionage acts regarding military and space technology (Eftimiades, 2019). The United States has also encountered multiple breaches of government security through Chinese espionage and has subsequently faced increasing struggles with counterintelligence (Dorsett, 2014).

With the increase in Chinese espionage in the last two decades, the United States has suffered several infiltrations (Dorsett, 2014; Eftimiades, 2019). Some of these breaches include the infiltration of essential companies tasked with defense and aerospace operations (Eftimiades, 2019). This could have devastating consequences regarding United States security. The success of these espionage efforts has also exposed a weak point in the United States' Chinese intelligence and counterintelligence services (Dorsett, 2014). This emphasizes a need for reform in the intelligence and counterespionage-focusing agencies. Studies have also shown that the United States has been the target of upwards of twenty percent of all Chinese economic espionage efforts (Eftimiades, 2019). This theft of intellectual property has cost the United States roughly \$360 billion annually (Eftimiades, 2019; Levine, 2020). With the catastrophic consequences associated with Chinese espionage, it is essential to investigate these incidents further and determine suitable reform for United States counterintelligence methods.

This thesis will examine several critical issues related to the threats to U.S. security and intelligence posed by Chinese espionage. The first chapter gives an overview of the tension between China and the United States regarding the use of espionage and the rise of China. The second chapter reviews espionage committed by China and the various tactics and targets involved in these efforts. The third chapter examines the impact of Chinese espionage on the United States, specifically regarding the economy and national security. The final chapter assesses the diplomatic and counterintelligence efforts used by the United States in response to Chinese espionage and recommendations and reforms to increase the effectiveness of those efforts.

Chapter Two: Chinese Espionage Efforts

Before discussing Chinese espionage efforts, it is important to clarify what is meant by espionage. This chapter will begin with a focus on the various definitions of espionage and how espionage will be defined for the purposes of this paper. Next, the use of espionage throughout history will be detailed. Finally, a discussion on the targets and tactics of Chinese espionage will follow.

What is Espionage?

The term “espionage” is often used, but its meaning might differ depending on who is asked. “Espionage” was derived from the 14th to 16th century French language term “espionner”, meaning “to spy” (Merriam-Webster, n.d.). The most common definition aligns with the use of spies to collect information about a foreign nation (Merriam-Webster, n.d.). This is similar to the Spy Museum’s definition of espionage as “the act of spying or using spies, agents, assets, and intelligence officers, as well as technology, to collect secret information, usually through illegal means” (Spy Museum, n.d.). Not uncommonly, the use of spies is often thought of when discussing espionage; however, when diving into a more legal definition of the term, the meaning begins to broaden:

the practice of gathering, transmitting, or losing through gross negligence information relating to the defense of the U.S. with the intent that or with reason to believe that the information will be used to the injury of the U.S. or the advantage of a foreign nation. (Merriam-Webster, n.d.)

While the above quote distinguishes benefiting a foreign nation as the main objective, this is only the case for certain types of espionage. There are various kinds of espionage, such as

industrial and economic espionage, which is defined by the Federal Bureau of Investigation (n.d.c) as

a foreign power-sponsored or coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, designed to unlawfully or clandestinely influence sensitive economic policy decisions or to unlawfully obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies.

There are also variations in how espionage can be conducted. One major form of espionage that has increased significantly the past few decades is cyber espionage. Cyber espionage can be understood as using computer systems or networks to obtain confidential information (Melnitzky, 2012; Spy Museum, n.d.). This form of espionage is relatively new and is a reflection of the impact of technological advancements (Spy Museum, n.d.).

Perhaps the best place to look for a formal definition of espionage is the United States' Espionage Act of 1917. The Espionage Act was passed by Congress and was built off of the Defense Secrets Act of 1911 (Office of the Director of National Intelligence, hereafter ODNI, n.d.a). The Defense Secrets Act of 1911 criminalized the collecting and sharing of information regarding the military to those without security clearances (ODNI, n.d.a.; Edgar & Schmidt Jr., 1973). The Espionage Act of 1917 was developed from this in an attempt to prevent disloyal activities during what would become World War I (ODNI, n.d.a; Spy Museum, n.d.). The Act contains several sections but essentially prohibits the obtaining, copying, and distributing of sensitive information with the intent or belief that the information will be used against the United States (The Bill of Rights Institute, n.d.). The act does not have to be completed for an individual to be prosecuted under these statutes, as an

attempt is considered to be enough (Edgar & Schmidt Jr., 1973). The Espionage Act also criminalizes negligent acts that result in a foreign nation or party gaining sensitive material against the United States (The Bill of Rights Institute, n.d.). This act is still in use and has been used throughout the years to convict various offenders such as Julius and Ethel Rosenberg who were charged during World War II with distributing information regarding the atomic bomb and were both sentenced to death (ODNI, n.d.a; Spy Museum, n.d.). The Espionage Act was also used to convict Central Intelligence Agency mole Aldrich Ames who sold information to the Soviet Union, and later Russia, which resulted in the deaths of 10 intelligence workers (ODNI, n.d.a).

For the purpose of this paper, espionage will refer to both national security espionage, i.e., the traditional use of spies to obtain a foreign nation's classified information, as well as the economic espionage of stealing trade secrets and intellectual property to benefit a foreign organization or company.

History of Espionage

The use of clandestine operations to collect information on a foreign government or organization is not a novel idea. In fact, espionage has been around since the dawn of time and has even been referred to as one of the oldest professions (Eftimiades, 2019; The History Press, n.d.). Espionage has been used all over the world and has been used in all major wars including the American Revolution when George Washington established a network of spies known as the Culper Ring (Jeffreys-Jones, 2019; The History Press, n.d.). This network obtained information through clandestine means regarding Britain's New York City base which helped determine military strategy in response (Spy Museum, n.d.). Nearly a hundred years later during the Civil War, President Abraham Lincoln established the first United

States' institution for espionage, which would later become the Secret Service (Jeffreys-Jones, 2019). During World World I, the use of espionage increased exponentially with the creation of organizations such as MI5 and MI6 in the United Kingdom and the establishment of central intelligence units U-1 and subsequent subdivisions in the United States (The History Press, n.d.; Jeffreys-Jones, 2019). The onset of World War II brought even greater use of espionage with new technological means to do so (The History Press, n.d.). Organizations such as the infamous Special Operations Executive in the United Kingdom were created to obtain information and sabotage foreign organizations (The History Press, n.d.).

Not exclusive to just the United States and the United Kingdom, espionage was also being used around this time by the Soviet Union. Prior to the United States entering World War II, the Federal Bureau of Investigation unveiled a network of spies working for the Nazi regime (FBI, n.d.a). Throughout the 1930s and 40s, a number of reporters in the United States were determined to be Soviet spies sent to gather intelligence regarding military and government secrets (Lovelace, 2015). Many of these spies remained hidden in the United States while the country went through the first Red Scare (Lovelace, 2015). With the onset of the Red Scare and the Cold War, the United States established the Central Intelligence Agency in 1947 with its main focus centered on foreign operations (Jeffreys-Jones, 2019). The Cold War between the United States and the Soviet Union sharply increased espionage efforts between the two nations and led to the creation of the Venona Project, which gathered Soviet communications, including espionage efforts to obtain information on the Manhattan Project (National Security Agency, n.d.). This program led to the identification of Julius and

Ethel Rosenberg who were later convicted and sentenced to death (National Security Agency, n.d.).

Espionage and clandestine operations have been in use for centuries, but it has not been until fairly recently that organizations and careers have been dedicated to espionage (The History Press, n.d.; Javers, 2011). Many people are against the use of espionage and feel that it is dishonest and underhanded. This was the general feeling in the United States following the Cold War until the attacks on 9/11, which led to a widely-backed expansion of espionage and intelligence efforts (Jeffreys-Jones, 2019). Since then, however, citizens have expressed disdain towards espionage, especially after the release of National Security Agency documents by Edward Snowden in 2013 (Jeffreys-Jones, 2019). These documents, which detailed surveillance efforts on United States citizens, has led to many Americans demanding limits on internal espionage and surveillance efforts (Jeffreys-Jones, 2019).

Chinese Espionage

A 2010 article found that close to 50 cases of Chinese espionage have been prosecuted in the United States in recent years (Davis, 2010). With China's announcement of their Made in China 2025 plan, many government officials are worried that Chinese espionage will increase and that Chinese espionage should be considered one of the top U.S. security concerns (Davis, 2018). As mentioned previously, espionage is not limited to just the use of spies in foreign nations gathering intelligence on matters regarding national security and military equipment. The targets and tactics of espionage vary widely.

Targets

While top-secret military and national security information might be what comes to mind when thinking about the targets of Chinese espionage, the range of targets is actually

much larger and can vary from classified defense documents to corporations' intellectual property (Eftimiades, 2019; Javers, 2011). This can have a powerful impact on both national security and the economy (Eftimiades, 2019). Many scholars have noted a significant increase in espionage efforts following the announcement of the Made in China 2025 Plan (Hough. & Malik, 2021; Eftimiades, 2019; Levine, 2020). With the plan detailing the nation's objective of restoring itself as the top dominating power, this might have served to expand the spectrum of targets for espionage. Currently, the primary targets of Chinese espionage in the United States include technology companies, defense and aerospace companies, universities, and pharmaceutical firms (Eftimiades, 2019).

The Made in China 2025 Plan established a clear focus on reducing dependency on foreign technology, as well as improving and expanding Chinese industry (Levine, 2020). This coincides with how nearly a quarter of China's espionage efforts in the United States have been directed towards commercial interests (Eftimiades, 2019). This is commonly referred to as industrial or economic espionage (Kabay, 2005; Kim, 2018). An example of this is the 2001 incident consisting of two Chinese nationals working for Lucent Technologies who stole software information with the intent to build a networking company in China (CSIS, n.d.; Kabay, 2005). A similar case took place in the same year with two Chinese nationals, backed by the PRC, stealing trade secrets from Sun Microsystems and Transmeta Corporation with the intent to create competitive technology in China (Kabay, 2005). Other cases involving the theft of trade secrets from General Motors, NetLogics Microsystems, Ford Motor Company, Motorola, and various oil companies have also taken place throughout the 2000s (CSIS, n.d.). Just last year, Xiang Haitao, a Chinese national was caught with electronic copies of trade secrets in his luggage (Department of Justice, 2022).

He was later sentenced for conspiring to commit economic espionage through the theft of The Climate Corporation's Nutrient Optimizer in order to benefit the PRC and the academy at which he worked in China (Department of Justice, 2022).

Another large target for Chinese espionage is military technology (Gilli & Gilli, 2019). China's military, while exceedingly large, does not have the same technological abilities as the United States (Gilli & Gilli, 2019). Due to the large technological gap, this has made the United States a target for espionage concerning military technology and weapons designs (Gilli & Gilli, 2019; Davis, 2010). The Department of Defense has often been victim to Chinese espionage (Gilli & Gilli, 2019; Davis, 2010). One major example of this took place in 2005 in an operation called "Titan Rain" when Chinese hackers were able to bypass the Department's networks and obtain information regarding U.S. defense contractors, the Defense Information Systems Agency, the Naval Ocean Systems Center, and more (CSIS, n.d.). This Department of Defense was attacked again in 2007, 2009, and 2011 when hackers were able to obtain online blueprints for stealth fighters (Gilli & Gilli, 2019). Other means of espionage have also been used to obtain military technology information, such as the 2010 incident with Noshir S. Gowadia, which will be discussed further in the next section (Davis, 2010). Another case of Chinese espionage targeting military technology took place in 2005 when Chinese operatives were able to collect information on warship technologies from the Navy (CSIS, n.d.). Scholars are worried that the increase in espionage targeting the military will cause the technological gap between China's and the United States' militaries to close (Gilli & Gilli, 2019).

Tactics

The People's Republic of China encourages the obtaining and sharing of information that can be used to better the country; moreover, it is required that Chinese citizens and companies comply with government requests to provide intelligence (Eftimiades, 2019; Silver, 2015). There are four main entities used to conduct foreign espionage: The Chinese Ministry of State Security, The Central Military Commission, state-owned enterprises, and private companies, and individuals (Eftimiades, 2019). For all but the final listed entity, these organizations and agencies are all committed to serving the nation's best interests (Eftimiades, 2019; Silver, 2015). These entities all specialize in different forms of intelligence they collect. For example, the Central Military Commission's espionage efforts primarily target military technology and information, while the private companies and individuals conduct mainly economic espionage (Eftimiades, 2019). The following section will review key tactics of Chinese espionage efforts and highlight a real-world example of each.

Cyber Espionage. The use of cyber espionage against the United States has increased exponentially in recent decades and is regarded as a top security concern (Melnitzky, 2012; Javers, 2011; Davis, 2018). Currently, the nation identified as the top perpetrator of cyber espionage against the United States is China (Nakashima, 2013). Following a series of cyber attacks targeting companies and government entities, President Barack Obama and Chinese President Xi Jinping came to an agreement in 2015 to not engage in cyber espionage (Mouillard & Proud, 2017). Unfortunately, this agreement has not been followed. There are various ways cyber espionage can be accomplished, and the most known form of cyber espionage is hacking. In 2017, Chinese hackers were able to breach the

National Foreign Trade Council, which included board members of various large companies such as Amazon and IBM (Mouillard & Proud, 2017). The following year, the Justice Department reported repeated hacking efforts and successes into private companies' online databases with the intention of stealing trade secrets and intellectual property (Davis, 2018). Due to a substantial number of attacks targeting Google's source codes and Gmail accounts, the company began partnering with the National Security Agency to help defend itself from Chinese hacking attempts (Javers, 2011; Nakashima, 2013). Another form of cyber espionage is the sending of fraudulent emails. One such instance occurred in 2008 when defense and technology companies' employees received emails suggesting job opportunities and asking for information regarding their access to technologies (Javers, 2011). Cyber espionage efforts and success have increased to the extent that former National Security Director Keith Alexander even commented that it could lead to the "greatest transfer of wealth in history" (Gilli & Gilli, 2019).

A more recent case of Chinese cyber espionage took place between 2011 and 2018 and involved four members of the Hainan State Security Department, a branch of the Chinese Ministry of State Security (Department of Justice, 2021a). It has been determined that the major targets of this operation were companies and government entities both within and outside of the United States. Like many other acts of Chinese espionage, this operation was backed by the state government. The four conspirators created a front technology development company and coordinated hacking attempts with its main methodologies being the creation of malware and the hacking of computer systems. Some schemes included the sending of fraudulent emails designed to look as authentic as possible by mimicking legitimate companies, as well as the use of customized malware which could obtain access to

computers and networks. Steps were taken to conceal the activities by storing information in programs such as Dropbox and GitHub. The victims consisted of aviation, defense, education, and government industries in a number of different countries, including the United States, with information and trade secrets such as technologies, foreign information, and research relating to various diseases being targeted. At the time of publication, the defendants were charged with conspiracy to commit computer fraud and conspiracy to commit economic espionage (Department of Justice, 2021a).

Pay Offs. Pay-offs are a form of espionage that many people might not consider; however, following the Espionage Act of 1917, the sharing of classified information that can be used against the United States or to the advantage of a foreign entity constitutes espionage (The Bill of Rights Institute, n.d.). There have been a number of government employees who received money from Chinese entities in exchange for information (Davis, 2010; Mouillard & Proud, 2017). In 2008, two cases involving Chinese pay-offs and government employees were brought to court (Davis, 2010). The first incident consisted of a Defense of Defense agent, Gregg William Bergersen, receiving payment from a Chinese agent in exchange for Secret-level national defense documents (Davis, 2010). The second incident, much like the first, involved another Department of Defense official, James Fondren Jr., who sold classified information to a PRC agent (Davis, 2010). In 2010, Noshir S. Gowadia, a former Defense contractor, was found guilty of espionage after he took multiple trips to China to provide services regarding United States' weapons designs (CSIS, n.d.; Davis, 2010). More recently, a State Department employee, Candance Marie Claiborne, was convicted on a reduced charge of conspiracy to defraud and lying to the FBI after it was discovered she had received

payments and gifts from Chinese agents in exchange for information regarding Sino-American relations (Mouillard & Proud, 2017).

An example of Chinese espionage in the form of pay-offs is the 2020 Alexander Yuk Ching Ma case (Cadman, 2020; Department of Justice, 2020a). Ma was a former officer for the Central Intelligence Agency (CIA) who worked with a Top Secret Clearance (Barnes, 2020; Department of Justice, 2020a). Upon exiting the CIA, Ma moved to Shanghai for a number of years before moving once again to Hawaii in 2001 (Department of Justice, 2020a). After moving to Hawaii, Ma was hired by the Federal Bureau of Investigations (FBI) as a linguist where he had access to Chinese documents with secret classification (Barnes, 2020; Cadman, 2020; Department of Justice, 2020a). It was at this time that Ma met with one of his relatives, who was a fellow former CIA officer, as well as People's Republic of China intelligence officials and began a conspiracy to communicate classified information (Department of Justice, 2020a). Ma photographed and stole multiple documents containing sensitive information regarding personnel, concealment technology, and operations with the PRC during his trips to China in exchange for money and gifts (Barnes, 2020; Department of Justice, 2020a). The Honolulu and Los Angeles Field Office conducted an investigation, and in 2019, an undercover FBI agent impersonating a PRC intelligence officer obtained proof that he was committing espionage when he was caught on video receiving payment in exchange for the intelligence (Barnes, 2020; Cadman, 2020; Department of Justice, 2020a). In a following meeting between the two, Ma provided further evidence of his activities by declaring his wish for "the motherland to succeed" (Barnes, 2020; Department of Justice, 2020a). In 2020, Ma was charged with conspiracy to communicate national defense information (Department of Justice, 2020a).

Citizen Exploitation. The last Chinese espionage tactic that will be discussed is the exploitation of Chinese citizens and Chinese-Americans. This can be understood as enticing Chinese citizens or citizens with ties to China who have access to companies or organizations to steal information and trade secrets (Nakashima, 2013; Kabay, 2005). This is often accomplished through email or flash drives (Nakashima, 2013). An example of this is the previously mentioned Lucent Technology company which had information stolen by two Chinese nationals who worked in the company (Kabay, 2005; CSIS, n.d.). This form of espionage can also be seen in the 2004 Yan Ming Shan case (CSIS, n.d.). In this incident, a Chinese employee stole sensitive information and technology from the software company at which she worked and attempted to bring it back to China (CSIS, n.d.). While a great deal of this form of espionage targets industrial and commercial enterprises, this tactic has also been used to infiltrate government facilities. This was seen in 2015 when Xiwen Huang stole classified information regarding military technologies from government research facilities that employed him (CSIS, n.d.; United States Attorney's Office, 2015).

A recent example of Chinese espionage in the form of citizen exploitation is the 2020 case regarding Wei Sun (Department of Justice, 2020b). Wei Sun, a Chinese national, worked as an electrical engineer for Raytheon Missiles and Defense, a company that developed missile systems for the military (Department of Justice, 2020b). As an employee of the organization, he was entrusted with sensitive material related to defense technology including information on missiles (Department of Justice, 2020b; Center for Development of Security Excellence, hereafter CDSE, n.d.a). Wei Sun gathered this information on a company laptop and asked permission to travel outside the United States with the laptop, which the company refused (CDSE, n.d.) He later traveled to China with the laptop, and upon his return, was

questioned by the company (Department of Justice, 2020b; CDSE, n.d.). Wei Sun admitted to traveling with the laptop to China after originally declaring he had traveled to Singapore (CDSE, n.d.). Wei Sun was later sentenced to 38 months in federal prison for exporting information that is prohibited under the International Traffic in Arms Regulations (Department of Justice, 2020b).

Chapter Three: Impact on the U.S.

With the increase in Chinese espionage in the last two decades, the United States has suffered several infiltrations (Dorsett, 2014; Eftimiades, 2019). As discussed in the previous chapter, these efforts have targeted both security and economic sectors. This has resulted in severe consequences for U.S. economic and security interests (Frazier, 2020). Tensions caused by these infiltrations, have also affected international relations between the two nations as well as complicated U.S. relations with other nations.

Economic

As mentioned previously, Chinese espionage has exponentially increased since in the last few decades, especially upon the release of the *Made in China 2025* plan (Levine, 2020; Schiffrinson, 2020). This plan highlights the country's strategy to reduce their dependence on foreign nations' technology and increase domestically-made materials (Levine, 2020; Ross, 2010). In order to decrease their independence on foreign technology, however, China must either funnel massive amounts of time and money into research and development or pursue advanced technology in more illicit ways (Levine, 2020). Levine (2020) puts it simply by stating,

The plan prioritizes acquisition of advanced technology from foreign companies, with the intent of assimilating the technology locally, digesting it, and innovating it - tweaking or advancing existing technology so it can become a global industry leader (p.6)

By gathering advanced technology and information from other sources, China can produce modern technology while saving time and money, and this is exactly what has been done (Levine, 2020). Out of all of the world's pirated goods, it is estimated that approximately

85% are from Chinese or Hong Kong efforts (Eftimiades, 2019). The percentage of counterfeit and pirated goods that are presumed to come from China varies by region. In Canada, this amount is estimated to be 80%. In the European Union, 83%. In the United States, the estimate jumps to 87% (Eftimiades, 2019). The United States has proven to be the largest target for Chinese economic espionage and is estimated to be the victim of 20% of all Chinese espionage efforts (Eftimiades, 2019). In fact, in the past decade, the Federal Bureau of Investigation has seen an increase in Chinese economic espionage cases by approximately 1300% (Department of Defense, 2021).

Chinese espionage has primarily targeted intellectual property and other information for economic gain (Bateman, 2022; Eftimiades, 2018). Intellectual property is described by the National Crime Prevention Council (n.d.) as,

any innovation, commercial or artistic; any new method or formula with economic value; or any unique name, symbol, or logo that is used commercially. Intellectual property is protected by patents on inventions; trademarks on branded devices; copyrights on music, videos, patterns, and other forms of expression; and state and federal laws.

Thus, intellectual property is an essential component of the U.S. economy (Mouillard & Proud, 2017). As of 2019, industries based on intellectual property comprise over 40% of domestic economic activity and about 45% of all employment in the United States (Toole et al., n.d.). This is the equivalent to upwards of 60 million jobs (Toole et al., n.d.). Technology and innovation play a large part in keeping the United States competitive in the global market, which means that these intellectual property-based industries are vital to the success of the economy (Mouillard & Proud, 2017). In fact, a 2019 report indicated that intellectual

property-intensive industries accounted for close to 80% of commodity exports from the United States (Miller, 2022).

Why does this theft impact the United States' economy? The global market currently operates under free market principles. This means that there is competition between goods and services, and consumers will find goods such as advanced technology at lower costs to be the most attractive (Levine, 2020). By avoiding the costs associated with creating and manufacturing their own technology, China has enabled itself to sell products at lower prices, which manipulates the market in their favor (Levine, 2020). This manipulation has resulted in a significant economic loss for the United States including a loss of consumer markets and millions of jobs (Eftimiades, 2019; Levine, 2020). When trade secrets and intellectual property are stolen, it costs the United States their competitive advantage in the global market by leading many companies to go out of business, downgrade, or contract due to losing out on profitable markets (Levine, 2020; Eftimiades, 2018). The total costs associated with this loss are estimated to be in the trillions of dollars with an annual cost ranging anywhere from \$200 billion to \$600 billion (Eftimiades, 2018; Frazier, 2020; Levine, 2020).

One example that showcases the cost of Chinese economic espionage is the Hongjin Tan case (Department of Justice, 2020c). Hongjin Tan, a Chinese national, worked as a scientist at Phillips 66 Petroleum Company developing new battery and storage technologies (CDSE, n.d.b; Department of Justice, 2020c). Tan told the company he would be moving to China to take care of his parents but that he did not have a job lined up; however, he later revealed to a coworker that he planned on working at Xiamen Tungsten, a company that creates materials for batteries (CDSE, n.d.c). Upon his resignation, the company looked into Tan's activity in the workplace and found that over the course of a year, Tan had copied and

downloaded secrets and restricted files from the company (CDSE, n.d.b; Department of Justice, 2020c). While nothing tangible was stolen from the company, the information illicitly taken held the research and developmental material for “next-generation battery technology” whose total value came to more than \$1 billion (CDSE, n.d.b). This technology coincides with the technological goals listed in the *Made in China 2025* plan (Levine, 2020; CDSE, n.d.b). By stealing this information from Phillips 66 and giving it to a Chinese company to replicate, the competitive advantage of this company becomes in jeopardy (Department of Justice, 2020c).

Defense and Security

Chinese espionage is also a threat to U.S. national security; however, this threat is not as direct as people think (Bateman, 2022). Much like the threat to the United States’ economy, the main threat to security comes from the diminishing competitive and strategic edge over China’s military capabilities (Eftimiades, 2019; Bateman, 2022; Kania, 2020).

The United States military is widely regarded as one of the most powerful, if not *the* most powerful, militaries in the world. This is in part due to the massive amount of spending dedicated to the military, as well as a large technological advantage in areas such as communications, computers, and surveillance (Sawant, 2021; Gill & O’Hanlon, 1999). There is a noticeable difference between the United States’ military capabilities and China’s. When looking at both nations’ naval capabilities in 2021, the People’s Liberation Army Navy (PLAN) has almost half the amount of warships with only about 20% of the number of missiles as the United States’ Navy (Sawant, 2021). Turning to aircraft, the United States has over 2,000 fixed-wing aircraft and over 1,000 helicopters; the PLAN has less than 500 and 120, respectively (Sawant, 2021). When looking at nuclear capabilities, China has around

200 warheads, while the United States has about 20 times this amount (Sawant, 2021). The only area in which the Chinese militaries lead is in serving member numbers (Gill & O'Hanlon, 1999). In total, the People's Republic of China's military has over 2.5 million serving members, making it the largest military in the world (Gill & O'Hanlon, 1999). However, a majority of these members serve on the ground protecting borders and keeping order domestically (Gill & O'Hanlon, 1999).

With China's strength in numbers, technology has played a crucial role in maintaining the gap between military capabilities (Bateman, 2022; Eftimiades, 2019; Gilli & Gilli, 2019; Levine, 2020). An increase in these kinds of technologies, however, is allowing the People's Republic of China to slowly close this gap (Eftimiades, 2019; Levine, 2020; Kania, 2020). A substantial amount of this information technology has been gathered by China through espionage (Eftimiades, 2019; Bateman, 2022; Department of Defense, 2021). Recent decades have seen a sharp increase in Chinese espionage stealing U.S. military trade secrets including aircraft design, naval warfare technologies, and hypersonic weapons technologies (Bateman, 2022; Department of Defense, 2021; Melnitzky, 2012). These espionage efforts have included targeting dozens of universities in the United States which were involved in maritime technology research and Navy defense secrets (Frazier, 2020). The technology and information stolen coincides with an increase in Chinese military technology as the People's Republic of China uses the information to build their own weapons and advance their military (Department of Defense, 2021).

There is evidence of an increase in Chinese military spending in recent decades (CSIS, 2015). While the official increase in spending puts the Chinese defense at about \$230 billion, many believe the number is actually much higher (CSIS, 2015). In addition, Chinese

espionage efforts targeting defense technology may allow the Chinese to use more of that budget on productions and less on research and development. Furthermore, the increased military budget could be supported by economic espionage efforts which have boosted China's economy by eroding the United States' competitive economic edge. Regardless, as China continues to develop and improve technologies such as intercontinental ballistic missiles, hypersonic weapons systems, and cruise missiles, its military investment is beginning to shorten the technological gap with the United States (Eftimiades, 2019; Department of Defense, 2021). This lessening gap could have severe consequences regarding regional, and even global, power. Many scholars are worried that this eroding gap could cause the United States to lose their dominance and strategic advantage in Asia and around the world (Eftimiades, 2019; Townshend & Crabtree, 2022; Kania, 2020).

International Relations

Chinese espionage has affected the international sphere in two major ways: a shift in the balance of power and increased tensions between nations. The loss of U.S. economic and military advantage has brought the potential for a shift in the balance of power (Eftimiades, 2019; Townshend & Crabtree, 2022; Kania, 2020; Araya, 2022). The United States' hegemony and influence in world affairs has likely been weakened in recent decades (Araya, 2022). As Chinese economic espionage persists, the PRC's economy continues to grow at the expense of the United States, and there is a possible shift in which nation is considered the center of world trade (Araya, 2022). Those at the center are able to deepen ties with other nations and influence international policies (Eftimiades, 2019; Araya, 2022). In other words, if China becomes the center of world trade, their sphere of influence would grow substantially to combat the United States (Araya, 2022; Eftimiades, 2019). This influence is

not strictly tethered to economic success. Military power also has a strong effect on influence. The continuation of Chinese espionage efforts targeting military and defense information allows the PRC to expand and modernize its military capabilities (Eftimiades, 2019). As this happens, its ability to coerce and threaten other nations increases, which broadens China's sphere of influence in Asia (Townshend & Crabtree, 2022; Eftimiades, 2019). If this continues to grow, it could eventually expand out of the region (Department of Defense, 2021). If this happens, the United States will not be in as strong of a position to fight for their interests, and the People's Republic of China will be in a better position to advance their foreign policy agenda (Department of Defense, 2021).

There is no doubt that the increase in espionage efforts has caused tensions between the United States and China. With the recent Chinese spy balloon escapade in February of 2023, arguments between the two nations have risen regarding use of espionage with neither country wishing to reveal the full extent of their operations (Wang et al., 2023). Chinese espionage has reached such heights that the Federal Bureau of Investigation declared these intrusions as their number one counterintelligence priority (FBI, n.d.b). The organization even goes as far as to state that "the counterintelligence and economic espionage efforts emanating from the government of China and the Chinese Communist Party are a grave threat to the economic well-being and democratic values of the United States" (FBI, n.d.b). FBI Director Christopher Wray supported this message and added that espionage is the underlying reason for ongoing tensions between the two nations (Tucker, n.d.). Tensions are already high in the South China Sea with the China-Taiwan crisis and the United States' involvement. The increase in espionage could lead tensions to escalate to their breaking point. The potential results of this range from exclusionary foreign policies to all-out conflict.

Chapter Four: U.S. Response

With the high impact and risks associated with Chinese espionage, the United States has been unwilling to let these efforts go without response. There are a variety of ways for a country targeted by espionage to respond, including with diplomatic policy reforms and counterintelligence efforts.

The initial reaction of American citizens to the increase in Chinese espionage has not been unlike the “Red Scare” with fear, paranoia, and hostility building up towards China and Chinese Americans (Kim, 2018). Director of the Federal Bureau of Investigation, Christopher Wray, spoke out against this behavior at the Department of Justice China Initiative Conference (2020) stating that:

confronting this threat effectively does not mean we shouldn't do business with the Chinese. It does not mean we shouldn't host Chinese visitors. It does not mean we shouldn't welcome Chinese students or co-exist with China as a country on the world stage. What it does mean is that when China violates our criminal laws and international norms, we're not going to tolerate it, let alone enable it. The Department of Justice and the FBI are going to hold people accountable for that and protect our nation's innovation and ideas.

A delicate balance must be struck in order to deter future espionage efforts while simultaneously not alienating China and compelling a hostile response.

Diplomatic and Legislative Efforts

The United States has attempted to enact legislation both domestically and abroad to prevent and punish acts of espionage. Some of these policies address all foreign nations, and some agreements specify China and Chinese espionage. These legislative efforts have not

been confined to the United States. In fact, after being targeted several times by China, including having intellectual property stolen and malware spread through companies, Australia passed laws to prevent future actions by the country (Eftimiades, 2019; Kendall, 2019).

Previous Efforts

While there have been diplomatic and political attempts with China to stop the invasion of espionage, it appears that these have not been entirely successful. One such attempt was the 2020 “Phase One” trade deal which included intellectual property safeguards (Frazier, 2020). These assurances guaranteed that U.S. companies would be subject to forced technology transfers while operating in China, that requests for information during licensing procedures will be reduced, and that U.S. trade secret protections against electronic instructions will be respected (Frazier, 2020). Experts have argued that this trade deal offers no real change due to its lack of specificity towards what constitutes a trade secret, as well as China’s history of violating espionage laws and agreements (Frazier, 2020).

Another attempt at diplomatically encouraging China to halt espionage efforts is the Special 301 Report (Liu, 2018). The Special 301 Report is a list of foreign countries that have exhibited instability regarding IP protection and enforcement (Office of the United States Trade Representative, hereafter OUSTR, n.d.; Liu, 2018). This can include countries whose IP protection policies’ effectiveness are decreasing, countries who are violating copyright piracy and counterfeit policies, and more (OUSTR, n.d.). Every year, the United States puts China on the priority watch list within the Special 301 Report in an effort to shame the nation into changing their ways (Liu, 2018). This tactic has not yielded significant results.

A more direct approach taken by the Trump administration was trade sanctions on Chinese goods (Pettis, 2021; Uchechukwu, 2019). While previous tariffs under the Administration were designed to affect various countries, including allies, the memorandum under the *Trade Act of 1974* specifically targeted Chinese goods by applying a \$50 billion tariff (Uchechukwu, 2019; Hass & Denmark, 2020). Trump justified these tariffs by claiming it was retaliation for intellectual property theft as well as a means to lessen American debt with China (Uchechukwu, 2019; Hass & Denmark, 2020). Some experts have spoken out against this approach. For example, Lester (2020) argued that sanctions are not effective methods for changing behavior of foreign nations. In fact, the resulting Chinese response which placed sanctions on American products created a trade war between the countries that resulted in economic losses on both sides and no real change in Chinese economic or espionage practices (Uchechukwu, 2019; Hass & Denmark, 2020).

A second approach taken under the Trump administration is the creation of the Department of Justice's China Initiative (Lucas, 2022; Lewis, 2020). The program, launched in 2018, sought to counter and deter Chinese espionage through identification, prosecution, and education, and has overseen hundreds of investigations including the cases of Alexander Yuk Ching Ma, Hongjin Tan, and Wei Sun (Department of Justice, 2021b; Lucas, 2022; Gerstein, 2022; Lewis, 2020). While the program is considered by many to be successful, the Justice Department ended the initiative in February 2022 due to concerns raised by a National Security Division review regarding the framework of the initiative as purely "Chinese" (Lucas, 2022). Scholars and civil rights groups provided feedback on this framework arguing the grouping of cases under the China Initiative has caused an "us versus them" mentality and has provoked a sharp rise in hate crimes and racial profiling against

Asian Americans (Gerstein, 2022; Lucas, 2022; Kim, 2018; Lewis 2020). The Department of Justice plans on continuing investigating and prosecuting cases of Chinese espionage, however, the framework will be broadened to include Russia, Iran, and North Korea so as not to single out China (Lucas, 2022; Gerstein, 2022).

Recommendations

Several diplomatic policy recommendations have been suggested by scholars; however, there is not universal agreement on how aggressive these policies should be. Several bills have been introduced to Congress targeting Chinese espionage and influence (Eftimiades, 2019). One such bill was H.R.5431 which was introduced September 30, 2021 (Designating the CCP, 2021). The bill, sponsored by Scott Perry, sought to designate the Chinese Communist Party as a transnational organized crime group (Designating the CCP, 2021). As a member of the United Nations Convention against Transnational Organized Crime, if this bill had been passed, the United States might have been compelled to take steps against China and Chinese operations in a more drastic way (United Nations, n.d.). The bill did not pass a vote and died in Congress (Designating the CCP, 2021). Another bill introduced to Congress was H.R. 824 which sought to prevent certain members of the Chinese Communist Party from traveling to the United States until cessation of U.S. intellectual property theft (Stop China's IP Theft Act, 2021). Within this bill, senior officials of the CCP and their family members, as well as members of the cabinet of the Government of the PRC and active duty members of the People's Liberation Army would be prohibited from entering the country (Stop China's IP Theft Act, 2021). This bill also died in Congress.

The *Stop Higher Education Espionage and Theft Act*, known as the SHEET Act, has been introduced to Congress numerous times over the last several years (*Sen. Cruz*

Introduces Bill, n.d.; SHEET Act, 2021). The bill, sponsored by Texas Representative Ted Cruz, attempts to address espionage and theft against universities by designating foreign actors who have attempted, successfully or not, to commit these actions as a foreign intelligence threat (SHEET Act, 2021). This would result in a revoked visa, removal from the United States, and judicial review (SHEET Act, 2021). The current status of this bill remains as “introduced”.

Another more recent case of suggested legislation to prevent Chinese espionage is the proposed ban on the entertainment app, TikTok. TikTok, a popular app for creating, watching, and sharing short videos has been taking the world by storm since its launch in 2016 (Espada & Popli, 2023). The app, which currently has over 150 million users in the United States alone, has been called into question regarding its company origins (Espada & Popli, 2023; Rascoe, 2023). ByteDance, the parent company of TikTok, is headquartered in China and has led many in the United States’ government to worry the app could be a gateway to Chinese espionage (Rascoe, 2023; Espada & Popli, 2023; Thorebecke & Fung, 2023). As discussed previously, companies in China are required to turn over data to the government when requested (Eftimiades, 2019; Silver, 2015). Government officials and those involved in intelligence organizations are worried about the information that could be gathered from hundreds of millions of Americans that might be subject to surrender to the Chinese government (Thorebecke & Fung, 2023; Espada & Popli, 2023; Rascoe, 2023). There are additional concerns surrounding how the app could potentially spread Chinese influence through its massive platform (Rascoe, 2023; Thorebecke & Fung, 2023). Because of this, the Biden administration and the Committee on Foreign Investment in the United States has offered the owner and CEO of TikTok, Singaporean Shou Chew, an ultimatum -

sell his stake in the company or face a nationwide ban (Espada & Popli, 2023; Thorebecke & Fung, 2023). A similar ban was threatened by President Donald Trump in 2020 (Thorebecke & Fung, 2023). Shou Chew, who testified in front of Congress on March 23, 2023, has stated several times that the Chinese government has never asked for American data and that they would never share that information with any foreign government (Rascoe, 2023). The CEO also offered up a plan called Project Texas which would allow only American TikTok employees to have access to data related to the United States (Rascoe, 2023). Whether or not the ban is passed, these actions by Congress and the Biden administration indicates an increasingly aggressive strategy towards Chinese espionage.

Many scholars and experts have recommended that the United States become more aggressive with prosecuting and punishing those involved in Chinese espionage efforts (Frazier, 2020; Sims, 2009; Melnitzky, 2012; Lester, 2020). Frazier (2020) suggests a National Trade Secret Protection and Remedy Strategy (NTSPS) which would allow the United States to better pursue “cyber-intellectual-property-theft-related litigation” against Chinese companies who have engaged in espionage. This strategy would theoretically deter future attacks while compensating companies and the U.S. government for losses (Frazier, 2020). Unfortunately, an increase in prosecutions against Chinese companies and actors could result in increased tensions and possibly lead to retaliatory actions such as severe reductions in trade, which is what FBI Director Christopher Wray advised against (Frazier, 2020; FBI, 2020).

Counterintelligence Efforts

While many people immediately think of spies and covert operations when discussing intelligence, a large component of every intelligence agency is dedicated to counterintelligence (Rudman & Brown, 1996).

Previous Efforts

Counterintelligence involves taking action to protect intelligence agencies and the nation from foreign intelligence efforts (Rudman & Brown, 1996; Dorsett, 2014; Lowenthal, 2012). Intelligence agencies are sources of large amounts of information which makes them prime targets for espionage (Lowenthal, 2012). Counterintelligence actions can be both defensive and offensive and are not considered to be separate from the rest of the intelligence process (Lowenthal, 2012; Dorsett, 2014; Rudman & Brown, 1996). The offensive side focuses on monitoring and disrupting foreign intelligence services (Dorsett, 2014; Lowenthal, 2012). Offensive actions include recruiting foreign intelligence agents, monitoring and disrupting the activities of foreign agents, and carrying out operations to uncover targets and methods of foreign intelligence agencies (Rudman & Brown, 1996). Defensive actions include investigating foreign espionage cases, preventing foreign agents from infiltrating, and reducing fallout from successful infiltrations (Dorsett, 2014; Rudman & Brown, 1996; Lowenthal, 2012).

The birth of counterintelligence is largely attributed to John Jay (ODNI, n.d.b; National Counterintelligence Center, hereafter NCC, n.d.). John Jay is most well-known for his contribution to the drafting and ratification of the Constitution; however, he is also recognized for saving the life of George Washington (NCC, n.d.). In 1776, the Committee for Detecting and Defeating Conspiracies was created by the New York State Legislature

followed by the appointment of John Jay as its leader (ODNI, n.d.b; NCC, n.d.). Much like the name suggests, the purpose of the Committee was to uncover and destroy conspiracies against the United States (ODNI, n.d.). One of these conspiracies included the 1776 plot against George Washington (ODNI, n.d.). While investigating the movements of British Loyalists, the Committee discovered several of Washington's bodyguards had plotted with the British to assassinate George Washington in a surprise attack (NCC, n.d.; ODNI, n.d.). John Jay would go on to co-author many of *The Federalist Papers* including *Federalist Number 64* where Jay argued the need for secrecy and protection of information (ODNI, n.d.). This paper is considered to be foundational to subsequent intelligence agencies (ODNI, n.d.).

In the United States, the Federal Bureau of Intelligence is tasked with countering espionage efforts within the nation, while the Central Intelligence Agency focuses their counterintelligence activities on operations outside the country (FBI, n.d.d; Rudman & Brown, 1996; Kristlik, 2016). This is not to say that these are the only agencies to take on counterintelligence programs. Every intelligence agency and all military departments, at a minimum, have the capability to investigate their employees or prospective employees for signs of involvement with a foreign nation (Rudman & Brown, 1996; Lowenthal, 2012). In fact, one of the major mechanisms in place to prevent infiltrations via employees is a lengthy (approximately 9-month long) application process (Lowenthal, 2012). Within this process, an extensive background check is conducted which reviews a candidate's history for any signs of motivation for espionage against the country (Dorsett, 2014). Interviews of close associates are also conducted, and in addition to this, many federal agencies require applicants to undergo a polygraph test (Lowenthal, 2012). This test measures physiological

responses associated with deception and dishonesty such as heart rate, temperature, and breathing frequency while applicants are asked questions regarding their personal and work history (Lowenthal, 2012; American Psychological Association, 2004). Another counterintelligence initiative in place is the compartmentalization of intelligence agencies (Lowenthal, 2012). This separation effectively assures that no singular person has access to all intelligence information save for the Director of National Intelligence who facilitates the sharing and implementation of intelligence (Lowenthal, 2012). In other words, when an employee receives the highest level of security, they are still not given access to all information at their intelligence agency (Lowenthal, 2012).

Despite these counterintelligence efforts, infiltrations, as discussed previously, still occur. This is because it is exceedingly difficult and nearly impossible for a single agency to discover, monitor, and thwart all espionage activities (Dorsett, 2014).

Reform

With the continuance of Chinese espionage efforts, many scholars and experts are advocating for serious reform in the counterintelligence field. The main modification involves transforming counterintelligence programs from reactive to proactive (Dorsett, 2014).

A substantial number of experts have alluded that United States' counterintelligence operations are not operating to their full potential (Kristlik, 2016; Dorsett, 2014; Sims, 2009). It has been suggested that not enough attention has been given to these efforts, and that is why there continues to be mass infiltrations (Sims, 2009; Dorsett, 2014). Attention towards counterintelligence often decreases during times where no immediate danger has been declared (Kristlik, 2016; Sims, 2009). This is partly because Americans are more likely to

advocate for privacy rights, which lowers political endorsements towards developing intelligence and counterintelligence abilities (Kristlik, 2016). Labeling China as an immediate and dangerous threat, however, would be inadvisable as there is a large possibility of retaliatory actions and increased hostility.

Some experts have argued that in order to better our counterintelligence strategies against China, agencies must evaluate Chinese intelligence methods and goals (Dorsett, 2014; Bateman, 2022). It is only when we fully understand an adversary that we can begin to formulate a proper and effective response and counter-strategy. This includes looking into the various ways Chinese intelligence organizations recruit agents (Dorsett, 2014). For example, some studies have shown that Chinese intelligence are more likely to reach out to native Chinese people in the U.S. than to those born outside the country (Dorsett, 2014). Knowing this information can help the United States recognize what to look for and narrows down the list of potential spies. Another aspect of Chinese intelligence that should be studied is the numerous marks that are targeted. While the list is large and includes diplomats, academics, schools, and companies, we can still better narrow down the list of targets and provide additional security (Eftimiades, 1994). By looking at the methods Chinese intelligence organizations use to recruit government officials, usually blackmail, we can better understand what signs to look for to prevent extensive damage (Eftimiades, 1994).

Some experts believe more needs to be done to vet prospective intelligence employees. It is argued that coworkers are more likely to trust other members of the organization which lowers their guard to deception (Lowenthal, 2012). It has been suggested that intelligence agencies move away from or lessen their dependence on polygraph tests for this reason, as they give people false confidence that the participant can be trusted (Dorsett,

2014; Lowenthal, 2012). The test is not entirely accurate at detecting lies and deception, and staking such high risks on such an unreliable technology is considered risky and unsound counterintelligence (Dorsett, 2014; American Psychological Association, 2004). One recognizable spy who passed a polygraph test while engaging in espionage against the United States is none other than Aldrich Ames (Lowenthal, 2012). Another operative within the field of intelligence who successfully passed a polygraph examination was Larry Wu Tai Chin (Kristlik, 2016; Lowenthal, 2012). Wu Tai Chin was born in Beijing and was recruited by the U.S. Army during World War II for a translator position (Sulick, 2013; Kristlik, 2016). He later transferred to the U.S. Consulate in Shanghai where it is said he became in contact with members of Chinese intelligence (Kristlik, 2013). Wu Tai Chin continued work throughout the Korean War where he interviewed Chinese prisoners of war with the State Department (Kristlik, 2016; Sulick, 2013). He successfully managed to work his way up the ladder of U.S. intelligence by joining the CIA and being promoted to a prominent position in the Foreign Broadcast Information Service where he was allowed access to highly confidential information (Sulick, 2013; Kristlik, 2016). A caveat to the promotion was passing a polygraph test, which Chin did (Kristlik, 2016). It would not be until after Wu Tai Chin's retirement that a tip would come in indicating his involvement with Chinese intelligence (Kristlik, 2016; Sulick, 2013). He was later arrested, found guilty, and committed suicide in prison (Sulick, 2013).

While agreement on how to best address the situation with China has yet to be reached, efforts and proposals are still being made by both parties. The question that remains, however, is whether or not bipartisan agreement can be reached in time to create successful policies and initiatives before irreparable damage to the economy and security is done.

Conclusion

The People's Republic of China has seen considerable expansion in their economy and modernization in recent decades (Art, 2010; Ross, 2010; Punnoose & Vinodan, 2019). The expansion, along with the nation's *Made in China 2025 Strategy*, has been significant enough to provoke fears of China rivaling the United States' power and sphere of influence (Medeiros, 2009; Art, 2010; Levine, 2020). China's extensive growth and modernization has also coincided with a significant rise in espionage against the United States as a result of the country gathering information and technology through illicit means (Shifrinson, 2020; Levine, 2020).

There are various types of espionage including the notorious use of spies as well as the use of computers, commonly known as cyber espionage (Merriam-Webster, n.d.; Spy Museum, n.d.; Melnitzky, 2012). While espionage efforts have been conducted by virtually every nation throughout history, Chinese espionage is notable for its sheer volume of efforts (Eftimiades, 2019). The targets of these attacks include both the industrial and economic sector of the United States, as well as areas of defense and national security, such as the Department of Defense (Eftimiades, 2019; Gilli & Gilli, 2019; Davis, 2010). The PRC mainly employs tactics such as cyber espionage, pay-offs, and citizen exploitation (Mouillard & Proud, 2017; Melnitzky, 2012; Nakashima, 2013; Kabay, 2005).

Increases in economic espionage against the United States has resulted in a massive theft in intellectual property which has cost the U.S. their technological advantage, as well as consumers, resulting in an annual loss of trillions of dollars (Frazier, 2020; Eftimiades, 2018; Levine, 2020). The rise in espionage targeting U.S. defense and security technology and information has caused the country's military edge to diminish and China's capabilities to

grow (Bateman, 2020; Kania, 2020; Eftimiades, 2019). International tensions have also increased as a result of China's espionage, and many experts believe a shift in the balance of power is occurring (Eftimiades, 2019; Townshend & Crabtree, 2020; Araya, 2022).

The United States has responded with various diplomatic and legislative efforts to deter Chinese espionage; however, the attacks have not ceased (Eftimiades, 2019). Intelligence agencies have put forth defensive and offensive counterintelligence efforts to thwart espionage attacks, and many initiatives have been successful; nonetheless, reform and recommendations have been made to make these endeavors more effective (Lowenthal, 2012; Dorsett, 2014). There is still widespread debate regarding how best to handle the espionage issue with China without provoking a hostile reaction.

Reflection

When discussing Chinese espionage, fear and alarm from citizens appears to come from a focus on espionage attacks targeting the military and national security agencies. The picture painted of Chinese espionage is one of secret agents infiltrating the U.S. government's top security organizations and pilfering documents specifying the locations of U.S. military bases to later be used in offensive attacks against our country. However, this is largely not the case. While there have been multiple invasions by Chinese hackers, as well as pay-offs of government workers in the field of defense, the information stolen is most often military technology documents, which is being used to help modernize China's People's Liberation Army (PLA). This might not fully assuage fears, but it is important to remember that the gap between Chinese and U.S. military capabilities is enormous. China is far from closing this gap. In 1999, scholars from the Brookings Institute (1999) suggested it would take decades before the nation represents a threat to the United States. Several decades have

passed since that report and, while China's military has advanced, the U.S. still retains superiority in terms of technology and size of physical assets such as warplanes and naval ships (Sawant, 2021).

The real concern lies with the ever-increasing economic espionage attacks against U.S. industries and companies. This is not just because of the trillions of dollars the nation loses every year to intellectual property theft (Eftimiades, 2018; Frazier, 2020; Levine, 2020); the deeper concern lies with consequences of a shift in the balance of economic power and influence. Intellectual property theft often results in U.S. companies losing their competitive edge and consumers to Chinese corporations. This bolsters the Chinese economy, which has been rapidly growing for decades, while simultaneously lessening the United States' earnings and sphere of influence. As discussed previously, it is often the wealthiest and most successful nations that are the most powerful with the largest sphere of influence. As the Chinese economy continues to grow, it is slowly beginning to shift the United States out of its position as the dominating global power, subsequently causing China's sphere of influence to grow. The effects of this could potentially be monumental. The United States has largely been considered a dominating global power since the end of World War II, when it was said an era of Pax Americana began which consisted of the U.S. exacting its influence on surrounding nations. Many scholars are declaring this era to be in decline with the United State's global influence deteriorating more and more every year. With China's continued economic growth, the nation could one day be what the United States is now. Under this new status, China would be a heavily influential party to international policies and decisions. Because China is a nation which strongly opposes Western influence, there is a good possibility that these policies and decisions would not benefit the United

States. There is already evidence that this has begun with the People's Republic of China facilitating a peace agreement between Iran and Saudi Arabia and causing the two nations to consider joining the BRICS alliance, an alliance known for its opposition to Western-dominated institutions (Gallagher et al., 2023). Some countries are even considering backing a switch to the Chinese currency, yuan, instead of the U.S. dollar (Gallagher et al., 2023). This could cause devastating consequences for the United States. In short, while military capability is important, the consequences of continued economic espionage against the United States are more severe in the long-run.

The most effective strategy to combat economic espionage appears to be building up an efficient counterintelligence cyber-taskforce. A great deal of economic espionage attempts are through cyber means including hacking operations and the sending of malware. Consistent with arguments of those such as Dorsett (2014), counterintelligence programs must be reconstructed to a more proactive and aggressive approach rather than reactive. While privacy infringement is an understandable and real concern, citizens' fear of this often leads to less advocating for counterintelligence programs (Kristlik, 2016). Without attention and reform in these programs, there will most likely continue to be mass infiltrations. A balance must be struck between the government and citizens so that counterintelligence programs can operate more effectively without encroaching on the rights of citizens. The best way to accomplish this is through a system of checks and balances. If citizens know an agency or organization is looking out for their rights, they will be more likely to give their approval to increased counterintelligence reach. Unfortunately, instead of focusing attention on counterintelligence, many government agencies have continued to add more and more security measures in the employee application process. While these measures and procedures

are beneficial and aid in preventing the infiltration of Chinese agents, they distract from the problems with more priority and urgency.

Policies and diplomatic efforts have not been entirely successful at preventing Chinese espionage; nevertheless, such endeavors should not be abandoned. While counterintelligence programs are more likely to be effective, the ideal approach to putting an end to these attacks and infiltrations would be mutually agreed upon legislation between the United States and China. Counterintelligence programs should act as a backup plan for the infrequent cases of espionage that slip through the cracks of the policies which the two nations have agreed to. It is true that China has a history of ignoring legislation; however, the U.S. should not give up yet.

A concern that is not receiving enough attention is the increase in hate crimes against Asian Americans due to inflated fears of Chinese espionage. As mentioned previously, the Department of Justice's China Initiative was terminated after several civil rights organizations raised concerns about the rise in racial profiling and harassment of Asian Americans by American citizens. The China Initiative, as well as the repeated rhetoric that Chinese agents want to infiltrate the government and destroy us, has amped up the "us versus them" mentality. As a country with a long history of mistreatment towards minorities, the United States cannot afford to let this rhetoric continue. Director of the Federal Bureau of Investigation, Christopher Wray, has already advocated for not ostracizing China and Chinese citizens; however, this discussion needs to be had at a more broad level and addressed to the American people as opposed to just those in the defense field. Labeling, ostracizing, and harassing Asian Americans and Chinese citizens will not solve any problems and will only serve to make matters worse.

Chinese espionage has become an ever-pressing concern and will continue to be for the foreseeable future. It is only with reform and legislation that we can hope to combat the resulting consequences and prevent future espionage efforts.

References

American Psychological Association. (2004, August, 5). *The truth about lie detectors (aka*

Polygraph tests). <https://www.apa.org/topics/cognitive-neuroscience/polygraph>

Araya, D. (2022, October 5). *America's global dominance is ending: What comes next?*

Center for International Governance Innovation.

<https://www.cigionline.org/articles/americas-global-dominance-is-ending-what-comes-next/>

Art, R. J. (2010). The United States and the rise of China: Implications for the long haul.

Political Science Quarterly, 125(3), 359-391.

Barnes, J. (2020, August 17). Ex-CIA officer is accused of spying for China. *The New York*

Times.

<https://www.nytimes.com/2020/08/17/us/politics/china-spying-alexander-yuk-ching-ma.html>

Bateman, J. (2022). *U.S.-China technological "decoupling": A strategy and policy*

framework. Carnegie Endowment for International Peace.

Cadman, D. (2020). The curious case of Alexander Yuk Ching Ma: A multi-agency failure,

including the naturalization vetting process. *Center for Immigration Studies*.

<https://cis.org/Cadman/Curious-Case-Alexander-Yuk-Ching-Ma>

Center for Strategic and International Studies. (n.d.). Survey of Chinese espionage in the

United States since 2000.

<https://www.csis.org/programs/strategic-technologies-program/archives/survey-chinese-espionage-united-states-2000>

Center for Strategic and International Studies. (2015, December 28). What does China really spend on its military?

[https://www.csis.org/analysis/what-does-china-really-spend-its-military#:~:text=The%20Chinese%20government%20announces%20expenditure,1.36%20trillion%20\(%24209.2%20billion\).](https://www.csis.org/analysis/what-does-china-really-spend-its-military#:~:text=The%20Chinese%20government%20announces%20expenditure,1.36%20trillion%20(%24209.2%20billion).)

Center for Development of Security Excellence. (n.d.a). Case study: Hongjing Tan.

<https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-hongjin-tan.pdf>

Center for Development of Security Excellence. (n.d.b). Case study: Wei Sun.

<https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-sun.pdf>

David, W. (2011). *Tiger trap: America's secret spy war with China*. Boston: Houghton Mifflin Harcourt.

Davis, P. (2018). Chinese spies, thieves, and hackers: Two cases expose China's campaign to steal America's trade secrets. *Journal of Counterterrorism and Homeland Security International*, 24(3), 16-18

Davis, P. (2010). Chinese espionage is on the rise in the United States. *Journal of Counterterrorism & Homeland Security International*, 16(4), 12-14.

Department of Defense. (2021). Military and security developments involving the People's Republic of China: Annual report to Congress. *Office of the Secretary of Defense*.

<https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>

[E](#)

Department of Justice. (2022). Chinese national sentenced for economic espionage conspiracy. *Office of Public Affairs*.

<https://www.justice.gov/opa/pr/chinese-national-sentenced-economic-espionage-cons piracy>

Department of Justice. (2021a). Four Chinese nationals working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including infectious disease research. *Office of Public Affairs*.

<https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>

Department of Justice. (2021b). Information about the Department of Justice's China Initiative and a compilation of China-related prosecutions since 2018. *Department of Justice Archives*.

<https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related>

Department of Justice. (2020a). Former CIA officer arrested and charged with espionage. *Office of Public Affairs*.

<https://www.justice.gov/opa/pr/former-cia-officer-arrested-and-charged-espionage>

Department of Justice. (2020b). Former Raytheon engineer sentenced for exporting sensitive military related technology to China. *Office of Public Affairs*.

<https://www.justice.gov/opa/pr/former-raytheon-engineer-sentenced-exporting-sensitive-military-related-technology-china>

Department of Justice. (2020c). Chinese national sentenced for stealing trade secrets worth \$1 billion. *Office of Public Affairs*.

<https://www.justice.gov/opa/pr/chinese-national-sentenced-stealing-trade-secrets-worth-1-billion>

Designating the Chinese Communist Party as a transnational organized crime group act, H.R. 5431, 117th Cong. (2021).

<https://www.govinfo.gov/content/pkg/BILLS-117hr5431ih/xml/BILLS-117hr5431ih.xml>

Dorsett, M. (2014). U.S. Counterintelligence and the problem posed by Chinese intelligence. *Global Security Studies*, 5(4), 44-50.

Edgar, H. & Schmidt, B.C. (1973). The Espionage Statutes and publication of defense information. *Columbia Law School*, 73(5), 930-1087.

Eftimiades, N. (2019). On the question of Chinese espionage. *Brown Journal of World Affairs*, 26(1), 125-142.

Eftimiades, N. (2018, December 4). The impact of Chinese espionage on the United States: What is the cumulative impact of China's espionage activities for the United States' economy, security, and politics? *Trans-Pacific View*.

Espada, M. & Popli, N. (2023, March 16). *Why the U.S. and other countries want to ban or restrict TikTok*. Time Magazine.

<https://time.com/6263851/why-us-wants-to-ban-tiktok/>

Federal Bureau of Investigation. (2020). *Responding effectively to the Chinese economic espionage threat*.

<https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat>

Federal Bureau of Investigations. (n.d.a). *Duquesne Spy Ring*.

<https://www.fbi.gov/history/famous-cases/duquesne-spy-ring>

Federal Bureau of Investigations. (n.d.b). *The China Threat*.

<https://www.fbi.gov/investigate/counterintelligence/the-china-threat>

Federal Bureau of Investigations. (n.d.c). *What is “economic espionage”?*

<https://www.fbi.gov/about/faqs/what-is-economic-espionage>

Federal Bureau of Investigations. (n.d.d). *What we investigate*.

<https://www.fbi.gov/investigate/counterintelligence>

Frazier, G. (2020). Taming the paper tiger: Deterring Chinese economic cyber-espionage and remediating damage to U.S. interests caused by such attacks. *Southern California Interdisciplinary Law Journal*, 30(1), 33-68.

Gallagher, A., Hamasaeed, S., & Nada, G. (2023, March 16). What you need to know about China’s Saudi-Iran deal. *United States Institute of Peace*.

<https://www.usip.org/publications/2023/03/what-you-need-know-about-chinas-saudi-iran-deal>

Gerstein, J. (2022, February, 23). *DOJ shuts down China-focused anti-espionage program*. Politico.

<https://www.politico.com/news/2022/02/23/doj-shuts-down-china-focused-anti-espionage-program-00011065>

Gill, B. & O’Hanlon, M. (1999, June 1). *China’s Hollow Military*. Brookings Institute.

<https://www.brookings.edu/articles/chinas-hollow-military/>

- Gilli, A. & Gilli, M. (2019). Why China has not caught up yet: Military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. *International Security*, 43(3), 141-189. https://doi.org/10.1162/isec_a_00337
- Hass, R. & Denmark, A. (2020, August 7). *More pain than gain: How the US-China trade war hurt America*. Brookings Institute.
<https://www.brookings.edu/blog/order-from-chaos/2020/08/07/more-pain-than-gain-how-the-us-china-trade-war-hurt-america/>
- Hough, P. & Malik, S. (2021). China: Security and threat perceptions. In P. Hough, A. Morgan, B. Pilbeam, & W. Stokes (Eds.), *International security studies: Theory and practice* (pp. 391-398). Routledge.
- Javers, E. (2011). Secrets and lies: The rise of corporate espionage in a global economy. *Georgetown Journal of International Affairs*, 12(1), 53-60.
- Jeffreys-Jones, R. (2019). American espionage: Lessons from history. *Brown Journal of World Affairs*, 26(1), 93-106.
- Kabay, M. E. (2005) Industrial espionage. *Network World Fusion Security Newsletter*.
- Kania, E.B. (2020). Minds at war: China's pursuit of military advantage through cognitive science and biotechnology. *PRISM Security Studies Journal*, 8(3) 82-101.
- Kendall, S. (2019). Australia's new espionage laws: Another case of hyper-legislation and over-criminalisation. *University of Queensland Law Journal*. 38(1), 125-161.
- Khatoon, A., Rahim, N., & Ali, B. (2018). A historical perspective of China's peaceful policies and its rise as world economic power. *Liberal Arts and Social Sciences International Journal*, 2(1).

- Kim, A.C. (2018). Prosecuting Chinese “spies”: An empirical analysis of the Economic Espionage Act. *Cardozo Law Review*, 40(2).
- Kristlik, T. (2016). A structural assessment of the U.S. counterespionage vis-à-vis Chinese espionage efforts. *Historie Otazky Problemmy*, (2), 130-140.
- Kwon, E. (2012). Invisible anxiety: Would the rise of China really be a security threat to the United States? *Pacific Focus*, 27(3), 369-392.
<https://doi.org/10.1111/j.1976-5118.2012.01088.x>
- Lester, S. (2020). U.S. policy options toward China: An appraisal. *CATO Journal*, 42(3), 701-712.
- Levine, D. A. (2020). Made in China 2025: China’s strategy for becoming a global high-tech superpower and its implications for the U.S. economy, national security, and free trade. *Journal of Strategic Security*, 13(3), 1-16.
<https://doi.org/10.5038/1944-0472.13.3.1833>
- Lewis, M.K. (2020). Criminalizing China. *Journal of Criminal Law and Criminology*, 111(1), 145-225.
- Liu, H. (2018). In the shadow of criminalisation: Intellectual property criminal law, enforcement institutions and practices in China and the United States. *Information & Communications Technology Law*, 27(2), 185-220.
<https://doi.org/10.1080/13600834.2018.1458451>
- Lovelace, A.G. (2015). Spies in the news: Soviet espionage in the American media during World War II and the beginning of the Cold War. *Journal of Slavic Military Studies*, 28(2), 307-327. <https://doi.org/10.1080/13518046.2015.1030265>
- Lowenthal, M. (2009). *Intelligence: From secrets to policy*. CQ Press.

- Medeiros, E. S. (2009). The new security drama in East Asia: The responses of U.S. allies and security partners to China's rise. *Naval War College Review*, 62(4), 37-52.
- Melnitzky, A. (2012). Defending America against Chinese cyber espionage through the use of active defenses. *Cardozo Journal of International Comparative Law*, 20(20), 537-570.
- Merriam-Webster. (n.d.). *Espionage*. <https://www.merriam-webster.com/dictionary/espionage>
- Miller, R. (2022). IP policy and international affairs: Economic note. *United States Patent and Trademark Office*.
- Mouillard, C. & Proud, M. (2017). The great leak forward: Chinese economic espionage in the U.S. *Journal of Counterterrorism & Homeland Security International*, 23(1), 16-20. \
- National Counterintelligence Center. (n.d.). *American Revolution to World War II*.
<https://irp.fas.org/ops/ci/docs/ci1/ch1a.htm>
- Office of the Director of National Intelligence.(n.d.a).*The Espionage Act of 1917*.
<https://www.intelligence.gov/evolution-of-espionage/world-war-1/america-declares-war/espionage-act>
- Office of the Director of National Intelligence. (n.d.b) *The birth of American Counterintelligence*.
<https://www.intelligence.gov/evolution-of-espionage/revolutionary-war/birth-of-american-counterintelligence>
- Office of the United States Trade Representative. (n.d.) *Intellectual property: Special 301*.
<https://ustr.gov/issue-areas/intellectual-property/special-301>

Nakashima, E. (2013). US target of massive cyber-espionage campaign. *Washington Post*.

[https://ctcitraining.org/docs/US Target of Massive Cyber Espionage Campaign.pdf](https://ctcitraining.org/docs/US_Target_of_Massive_Cyber_Espionage_Campaign.pdf)

National Security Agency. (n.d.). *Venona*.

<https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/Venona/>

Pettis, M. (2021, January 28). How Trump's tariffs really affected the U.S. job market.

Carnegie Endowment for International Peace.

<https://carnegieendowment.org/chinafinancialmarkets/83746>

Punnoose, S.K. & Vinodan, C. (2019). The rise of China and power transition in contemporary international relations. *IUP Journal of International Relations*, 13(1), 7-27.

Rascoe, A. (2023, February 5). *People are calling for TikTok to be pulled from app stores in the U.S.* NPR Weekend Edition.

Ross, R.S. (2010). The rise of Chinese power and the implications for the Regional Security Order. *Orbis*, 54(4), 525-545.

Rudman, W.B. & Brown, H. (1996). *Preparing for the 21st century: An appraisal of U.S. intelligence*. Diane Publishing.

Sawant, M. (2021). Why China cannot challenge the US military primacy. *Journal of Indo-Pacific Affairs*.

Sen. Cruz introduces bill to counter Chinese espionage at American universities. (n.d.). Ted Cruz U.S. Senator for Texas.

- <https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-introduces-bill-to-counter-chinese-espionage-at-american-universities>
- Shiffrinson, J. (2020). The rise of China, balance of power theory, and US national security: Reasons for optimism? *Journal of Strategic Studies*, 43(2), 175-216.
- Silver, J. (2015). China's asymmetric intelligence advantage: The state security law. *Orbis*, 59(3), 380-397. <https://doi.org/10.1016/j.orbis.2015.05.005>
- Sims, J.E. (2009). *Vaults, mirrors, and masks: Rediscovering U.S. counterintelligence*. Georgetown University Press.
- Spy Museum. (n.d.). *Espionage Facts*.
<https://www.spymuseum.org/education-programs/spy-resources/espionage-facts/>
- Stone, R. (2013). A call to cyber arms. *Science*, 339(6123), 1026-1027.
<https://doi.org/10.1126/science.339.6123.1026>
- Stop higher education espionage and theft act, S. 676, 117th Cong. (2021).
<https://www.congress.gov/bill/117th-congress/senate-bill/676/text>
- Stop Chinese IP theft act, H.R. 824, 117th Cong. (2021).
<https://www.congress.gov/bill/117th-congress/house-bill/824/text?r=6&s=1>
- Sulick, M.J. (2013). *American spies: Espionage against the United States from the Cold War to the present*. Georgetown University Press.
- The Bill of Rights Institute. (n.d.). *The Espionage Act of 1917*.
<https://billofrightsinstitute.org/activities/the-espionage-act-of-1917>
- The History Press. (n.d.). *Espionage*.
<https://www.thehistorypress.co.uk/espionage/?p=1&ps=9>

Thorbecke, C. & Fung, B. (2023, March 23). *The US government is once again threatening to ban TikTok. What you should know.* CNN Business.

<https://www.cnn.com/2023/03/18/tech/tiktok-ban-explainer/index.html>

Toole, A., Miller, R., & Rada, N. (n.d.). Intellectual property and the U.S. economy: Third edition. *United States Patent and Trademark Office.*

Townshend, A. & Crabtree, J. (2022, June 15). *The U.S. is losing its military edge in Asia, and China knows it.* The New York Times.

<https://www.nytimes.com/2022/06/15/opinion/international-world/us-military-china-asia.html>

Tucker, W. (n.d.). Message from the director - Chinese espionage cases. *Society of Former Special Agents of the FBI.*

Uchechukwu, Nwoke. (2019). Imposition of trade tariffs by the USA on China: Implications for the WTO and international trade law. *Journal of International Trade Law & Policy*, 19(2), 69-84. <https://doi.org/10.1108/JITLP-01-2019-0003>

United Nations. (n.d.). *United Nations convention against transnational organized crime and the protocols thereto.*

<https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>

United State's Attorney's Office. (2015). Chinese businessman charged with theft of trade secrets.

<https://www.justice.gov/usao-wdnc/pr/chinese-businessman-charged-theft-trade-secrets>

Wong, E., Sanger, D.E, Barnes, J.E., & Schmitt, E. (2023, February 13). *Tensions rise over spy programs as U.S. investigates downed craft*. New York Times.

<https://www.nytimes.com/2023/02/13/us/politics/ufo-spy-balloon-china.html>