ATATÜRK ÜNİVERSİTESİ YAYINLARI
ATATURK UNIVERSITY PUBLICATIONS

Research Article *Araştırma Makalesi* DOI: 10.5152/JIRS.2023.23014

Economic Cyber Espionage: The US-China Dilemma

Ekonomik Siber Casusluk: ABD-Çin İkilemi

Juma Mdimu RUGINA

Ankara Social Sciences University, Graduate School of Social Sciences, Political Science and International Relations, Ankara, Turkey

ABSTRACT

This paper provides an overview of the acceptance of the multi-faceted phenomenon of economic cyber-espionage among great powers by taking into account different perspectives. The paper illuminates the disagreement of the US on economic cyber espionage, especially China, and the widespread perception that China is conducting cyber espionage activities to steal intellectual property from the US military, private companies, and other nations with the goal of surpassing the US as the global superpower. The US advocates for the development of new standards that limit the use of cyber espionage for traditional intelligence purposes concerning national security decisions. This paper argues that, since China is now among the countries advocating technology licensing, the country also advocates for the development of these standards because they would not dare to lose more than they would gain from cyber espionage. The paper also highlights the need for further study to refine existing definitions and develop widely accepted monitoring mechanisms.

Keywords: Cyberspace, Espionage, Cyberespionage, Economic cyber Espionage

ÖZ

Bu makale çok yönlü bir olgu olan ekonomik siber casusluğun büyük güçler arasında nasıl kabul gördüğü konusunda birçok perspektifi dikkate alarak genel bir bakış açısı sunmaktadır. Makale ABD'nin özellikle Çin ile ekonomik siber casusluk konusundaki anlaşmazlığını ve Çin'in ABD'yi küresel süper güç olarak geçmek amacıyla ABD ordusu, özel şirketler ve diğer uluslardan fikri mülkiyet çaldığına ilişkin yaygın algıyı aydınlatmaktadır. ABD, ulusal güvenlik kararları için geleneksel istihbarat amaçlarıyla kullanılan siber casusluğu sınırlayan yeni standartların geliştirilmesi gerektiğini savunmaktadır. Makalede, Çin'in artık teknoloji lisanslamasını savunan ülkeler arasında yer almasıyla birlikte, siber casusluktan kazanacağından daha çok kaybetmeyi göze alamadığı için bu standartların geliştirilmesini savunduğunu ileri sürmektedir. Makale ayrıca mevcut tanımların iyileştirilmesi ve yaygın olarak kabul gören izleme mekanizmalarının geliştirilmesi için daha fazla çalışma yapılması gerektiğinin altını çizmektedir.

Anahtar Kelimeler: Siber uzay, Casusluk, Siber casusluk, Ekonomik siber casusluk

Introduction

Relations between the US and China have worsened following various accusations in recent years involving these two countries with espionage matters, particularly those involving the theft of intellectual property (Boylan et al., 2021). United States government officials believe that China's objective is its economic development, achieved by stealing intellectual property and quickly producing cheaper goods than those made in the US and other countries (Brander et al., 2017). They warn that cyber espionage could have devastating consequences for the US economy and global competitiveness over the next decade. Furthermore, certain military and corporate leaders in the US suspect that China's long-term goal is to engage in "preemptive reconnaissance" to surpass the US economy. Reports suggest that Chinese hackers have illicitly obtained data from over 20 US weapons programs, encompassing critical systems such as the F-35 Joint Strike Fighter, Patriot missile system, and the Navy's new littoral combat ship (Lara, 2022).

China has consistently posed a significant digital threat to the United States. In a classified National Intelligence Estimate from 2009, which reflects the consensus of all 16 US intelligence agencies, China and Russia were identified as top online adversaries (Lindsay, 2015). China was considered the more immediate threat due to the extent of its industrial trade theft.

Received/Geliş Tarihi: 21.07.2023
Accepted/Kabul Tarihi: 08.12.2023
Publication Date/Yayın Tarihi: 29.12.2023

Corresponding Author/Sorumlu Yazar: Juma Mdimu RUGINA
E-mail: jumamdimu@gmail.com

Cite this article as: Rugina, J.M. (2023). Economic cyber espionage: The US-China dilemma. *Journal of International Relations Studies*, 3(2), 77-90.

Subsequently, White House officials negotiated an agreement wherein China committed to cease its hacking activities targeting American companies and interests for industrial gains (Roper, 2013). During the Obama administration, for 18 months, security researchers and intelligence officials observed a noticeable decline in Chinese hacking.

However, with the onset of President Donald J. Trump's administration and the escalation of trade conflicts and other tensions with China, the hacking activities resumed (Larres, 2020). The breaches aimed at acquiring intellectual property to benefit China's economic objectives were not attributed to the People's Liberation Army, but rather to a more loosely connected network of front companies and contractors, including engineers affiliated with some of China's prominent technology firms (Enoru, 2022).

With the world's largest online community, a burgeoning economic presence, and an increasingly formidable military and intelligence apparatus, China is employing these resources to pursue a deliberate and assertive foreign policy (Nathan & Scobell, 2015). This strategy aims to shape the governance and deployment of information and communication technologies on a global scale.

These cyberattacks linked to the Chinese Government, labeled as cyber-espionage or cyber spying, involve unauthorized access to sensitive or classified data, intellectual property, and trade secrets (Ulsch, 2014). The primary motivations behind such activities are economic gain, competitive advantage, and political objectives. President Biden is particularly concerned that the persistence of these attacks could undermine the economic strength of the United States. He asserts that China is specifically seeking diplomatic and military secrets from government databases and potentially lucrative industrial secrets held by American corporations. China's preference for cyberspace as a means of espionage is attributed to its cost-effectiveness and reduced risk compared to traditional espionage methods.

Despite allegations from the United States, Chinese officials deny engaging in state-sponsored cyber-espionage. They contend that China is, in fact, a frequent target of various cyberattacks and accuse the US of being a prominent actor in hacking activities. In response to hacking reports, a spokesperson for China's Foreign Ministry, Mao Ning, dismissed them as a "collective disinformation campaign" orchestrated by the US and its allies.

While efforts have been initiated by Washington to collaborate with Beijing on cyber issues, a fundamental question remains: Can the two nations mitigate the risk of destructive cyber conflict while simultaneously pursuing espionage against each other? Both China and the United States share a common interest in safeguarding national infrastructure from external attacks, yet neither appears willing to relinquish the practice of cyber espionage (Skinner, 2013).

While physical attacks between nations are universally condemned and often result in strong reactions, the United Nations Group of Governmental Experts declared in 2013 that cyberspace falls under existing international law, originally designed for conventional conflicts. Historically, nation-state espionage has been considered a lawful state behavior, and this understanding has extended to cyberspace as well (Brown & Poellet, 2012). Cyber espionage, involving the violation of a system's confidentiality, is deemed acceptable among responsible nations, whereas cyberattacks that compromise the availability or integrity of a system are prohibited (Von Solms & Van Niekerk, 2013).

However, the US and other like-minded nations have recently expressed concerns about the legitimacy of all forms of cyber espionage as state actions. As early as 2010, the US raised concerns about Chinese industrial cyber espionage, eventually leading to a high-level agreement between China and the US to prohibit such activities (Hjortdal, 2011).

It is important to acknowledge that the ongoing debate surrounding cyberspace norms reflects the current geopolitical realities, where the US and its allies are in conflict with China, a rising global power aiming to maximize its national advantages within the international community (Flint, 2021).

According to the majority of US analysts, China is extensively involved in cyber espionage activities, including the theft or replication of significant amounts of intellectual property from US government institutions, the military, and private businesses (Lindsay et al., 2015). The prevailing belief in the US is that modern espionage constitutes a large-scale operation orchestrated from Beijing, with the ultimate goal of China surpassing the US as the global superpower, primarily through technological advancements (Pillsbury, 2015). It is believed that China is doing so by providing an unfair economic advantage to its state-owned businesses through sharing gathered information with them. In contrast, while the US also engages in cyber espionage against China and other nations, it refrains from sharing the acquired information and intellectual property with its own industries (Lotrionte, 2014). This disparity in strategy could potentially put the US at an economic disadvantage and fuel misconceptions about China's capabilities for economic warfare.

Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency, argues that Chinese cyber espionage goes beyond conventional espionage conducted for national security purposes and is carried out for the benefit of their state-owned firms. The targets of cyber espionage align with China's strategic and economic objectives (Hjortdal, 2011). For instance, it has been claimed that a group of engineers working for private companies in Guangzhou, China, stole designs and technical data for missile, satellite, and nuclear propulsion systems from companies in the US, Canada, Europe, Russia, and Africa (Miller, 2022). This blurs the line between traditional espionage for national security protection and economic theft of intellectual property aimed at businesses and the government (Halbert, 2016).

China has also accused the US and other nations of conducting cyber espionage, claiming that the US has long employed the internet for covert theft and accusing the US of hacking its systems (Wilson & Drumhiller, 2016). Reports suggest that the National Security Agency (NSA) monitored conversations of senior officials at Huawei, a Chinese telecom company with connections to the Chinese military and government. The NSA's surveillance program aimed to exploit Huawei's technology so that they could later hack into the phone

and computer networks of nations to which Huawei sold equipment, including US allies and potentially hostile one's, for surveillance or offensive cyber operations (Cartwright, 2020).

The US response to China's allegations provides insight into how the US perceives its own behavior during cyber espionage activities (Iasiello, 2016). According to reports, US officials have stated that they do not provide the intelligence they gather to US companies to enhance their international competitiveness or increase their profits. The US maintains a distinction between public and private affairs, which is seen as beneficial for business and innovation and requires less regulation.

While a legitimate and legal commercial practice known as "competitive intelligence" involves acquiring information about competitors from public sources, the ease of stealing sensitive data through computers and the internet has complicated matters. Under US laws such as Title 18 USC, the National Infrastructure Protection Act, and the Economic Espionage Act of 1996, the theft or transfer of trade secrets, intellectual property, or proprietary information through industrial espionage, including industrial cyber espionage, is considered unlawful (Halligan, 2007).

It is increasingly evident that China, along with many other nations, does not share the American perspective on distinguishing between commercial and government espionage (Lindsay et al., 2015). This difference in philosophy presents challenges, particularly regarding intellectual property, for American businesses operating in China. American companies often have to disclose their intellectual property and manufacturing know-how to Chinese competitors to compete in China's state-run economy.

China is not the only nation that promotes cyber espionage information to benefit its own industries. Many other World Trade Organization (WTO) members also support state- owned or mostly state-owned businesses considered crucial to their economies (Lindsay et al., 2015). Governments own the majority of the world's largest oil companies. These nations do not draw as strict a line as the US does between government and private enterprise.

Understanding the historical differences in growth between China and the West is crucial to comprehending the various strategies employed in cyber espionage and the varying levels of protection for intellectual property rights (Bernik, 2014). Ancestral knowledge and a shared legacy hold greater importance than viewing intellectual activities as private property for personal gain. These societal differences contribute to the divergent interpretations of information in each region, fueling the rivalry between the US and China over the global boundaries of cyber theft and espionage (Lindsay et al., 2015).

To delve further into these issues, it is essential to enhance understanding of the social and cultural differences between the US and China, particularly in economics, military threats, and the evolving nature of industrial cyber espionage (Halbert, 2016). The author examines whether cyber espionage involving the US against China and other countries in the world, as well as the decision of the US not to provide its intellectual property and the data it has collected to domestic companies, puts the US at a great competitive disadvantage. Also, this paper highlights the possibility of the US misinterpreting China's cyber espionage as a threat of cyber warfare. Additionally, the article highlights the role that cultural differences between nations play in intolerance and how the US and China use cyber-espionage as a weapon in their economic warfare. The economic impact on these two major nations is assessed along with case studies of cyberattacks that targeted trade secrets and intellectual property.

This paper also looks to assess the effectiveness of current international legal standards governing economic cyber-espionage, which includes industrial cyber-espionage. Although this study focused mainly on China and the US, it manages to provide an overall picture of how government officials use technology and the Internet for cyber espionage to achieve their goals.

Literature Review

The tensions between the US and China regarding intellectual property infringements, concerns about cyber espionage, raise the question of whether both countries perceive these actions as genuine acts of aggression (Lucas, 2017). Gathering intelligence or information about other countries or non-state entities is a common practice in politics to protect one's national interests.

The practice of acquiring and compiling intelligence has a long history, with origins dating back thousands of years. In China, the pursuit of intelligence can be traced back to the legendary general and strategist Sun Tzu during the "Warring States" era (Sun, 1994). Sun

Tzu emphasized the use of intelligence in his renowned book "The Art of War," which outlines strategies for achieving victories even before entering the actual battlefield. Understanding one's enemy becomes crucial before engaging in combat.

Sun Tzu provides examples to illustrate his point, highlighting the importance of knowing the enemy and oneself to ensure success in battles (Wey, 2014). These teachings have broad implications and are studied by leaders in business and the military. Similarly, companies and non-state entities engage in competitive intelligence (CI) to gather information about their competitors. Competitive intelligence typically refers to the proactive process of learning about competitors and the competitive environment, with the aim of enhancing corporate performance through informed planning and decision-making (Olszak et al., 2006).

Although CI is still relatively new in China, efforts are being made to improve CI capabilities to support the developing market economy (Chen & Xie, 2004). In the digital age, intelligence gathering has expanded to online platforms and global cyber networks. However, the laws governing intelligence gathering are evolving more slowly.

When dealing with cultural differences, especially in the context of US-China relations, the understanding of concepts such as "intellectual property" becomes a crucial factor, as it influences perceptions and can lead to disagreements over accusations of cyberattacks or cyber warfare (Berrell & Wrathall, 2006). Cultural disparities may arise due to differing views on the proprietary nature of scientific knowledge.

The Society of Competitive Intelligence of China conducted a study on Chinese CI practices, which revealed that CI practitioners in China ranked technological uncertainty as relatively low, while economic, consumer, and international factors were perceived to have significant degrees of uncertainty (Tao & Prescott, 2000). This finding may be attributed to the respondents' scientific backgrounds and their close monitoring and analysis of technological advancements.

The divergent views on intellectual property create additional challenges in diplomatic relations between the US and China (Wang, 2010). China's historical perspective is rooted in a communal understanding of property rights, while the Western definition is individual-based. Consequently, institutional factors shape perceptions of ethical behavior in this context.

When addressing concerns about China's "cyber warfare" against the US, it is crucial to consider the divergence in perspectives. Chinese organizations have gained unauthorized access to American energy, petrochemical, and oil companies, stealing valuable information. Hackers compromised internal IT systems, corporate financial and energy data, and even the PCs of top executives (Rudner, 2013). They utilized the internet to connect to various business systems, allowing them to download data directly. This granted the attackers access to sensitive company information, including details on offers, operations, and control of Supervisory Control and Data Acquisition (SCADA) systems used in the energy sector.

Our perception of cyber operations is heavily influenced by media terminology and professional literature. Offensive cyber operations can be categorized into instrumental and strategic types to facilitate discussions on cyber espionage operations and information campaigns (Limnéll, 2015). Instrumental operations serve as facilitative measures to achieve goals beyond the cyberspace domain, while strategic operations aim to influence perceptions of security rather than actively supporting military efforts.

Conceptual Examples

In November 2021, Yanjun Xu, a Chinese national and Deputy Division Director of the Sixth Bureau of the Jiangsu Province Ministry of State Security, was found guilty by a federal jury of conspiring to commit economic espionage and attempting to steal trade secrets (Wilson, 2023). Notably, Xu is the first Chinese intelligence officer to be extradited to the United States for trial. This conviction underscores the integral role of trade secret theft in the Chinese government's efforts to modernize its industries. Xu collaborated in a plot to engage in economic espionage on behalf of the Chinese government, attempting to pilfer valuable innovations and trade secrets from prominent American aviation technology companies.

Being state-sponsored economic espionage by the People's Republic of China (PRC), Xu employed multiple aliases to target specific companies in the United States and abroad, particularly those recognized as leaders in aviation. He identified experts within these companies and recruited them to travel to China, often under the pretext of giving presentations at universities. Xu and his associates not only covered travel expenses but also provided stipends to these experts. According to the conviction, Xu sought to steal technology related to General Electric Aviation's exclusive composite aircraft engine fan—an innovation unmatched by any other company worldwide— -with the intention of benefiting the Chinese state (United States Department of Justice [DOJ], 2021).

Likewise, In January 2022, a 44-year-old Chinese national Xiang Haitao was sentenced to 29 months in prison, followed by three years of supervised release and a $150,000 fine for his involvement in a conspiracy to commit economic espionage. The economic espionage conspiracy was directed against Monsanto and The Climate Corporation. Xiang, who had developed digital online farming software aimed at collecting, storing, and visualizing crucial agricultural field data to enhance productivity, admitted to stealing a predictive algorithm (Nasheri, 2023). He then provided this stolen algorithm to the Chinese Academy of Science's Institute of Soil Science. Xiang conspired to steal a trade secret from The Climate Corporation, a Monsanto subsidiary. The objective of this act was to benefit a foreign government, specifically the PRC. Xiang's actions aimed at gaining an unfair advantage for the PRC by stealing a vital trade secret, which the victim companies had invested significant time and resources in developing.

The gravity of economic espionage as an offense lies in its potential to jeopardize the competitive advantage of US companies. Exploiting his residence and work in the United States, the defendant illicitly appropriated a valuable trade secret for the benefit of Chinese entities. Such conspiracies to transfer technology from US businesses to China inflict substantial economic harm on the country.

Furthermore, In May 2022, a prolonged and malicious cyber operation led by the well-known Chinese state actor, APT 41, resulted in the illicit acquisition of an estimated trillions worth of intellectual property from around 30 multinational companies operating in the energy, manufacturing, and pharmaceutical sectors. This Chinese hacking group engaged in intellectual property theft from US and European companies starting in 2019 and managed to operate largely undetected (Kapoor, 2022). Researchers strongly suspect the group is sponsored by the Chinese government. The cyber operation involved the extraction of hundreds of gigabytes of intellectual property and sensitive data, encompassing diagrams, blueprints, formulas, and proprietary manufacturing-related information. The intrusions targeted technology and manufacturing firms across North America, Europe, and Asia, focusing on acquiring blueprints for advanced technologies, including helicopters, fighter jets, and missiles. Most notably, the stolen information also included data from the energy industry, encompassing designs related to solar panels and edge vacuum system technology.

The Federal Bureau of Investigation (FBI) estimated that the annual cost to the US economy resulting from counterfeit goods, pirated software, and trade secret theft ranges between $225 billion and $600 billion. However, the long-term consequences of depriving multinational companies of crucial research and development building blocks make it difficult to quantify the full extent of the operation's economic impact.

Additionally, In May 2022, Peter Kisang Kim, a former engineer at Broadcom Inc., was sentenced to eight months in prison for engaging in trade secret theft related to Broadcom's proprietary information. Shortly after departing Broadcom, Kim assumed the role of IC

Design Verification Director at a startup in the PRC. In his plea agreement, Kim acknowledged that the startup aimed to emerge as a leading chip designer specifically targeting the PRC's domestic networking chip market ("Former Broadcom Engineer Sentenced," 2022).

Throughout his employment at the new company, Kim admitted to accessing and utilizing Broadcom's trade secrets. His plea agreement acknowledges that he took Broadcom's trade secrets for reference, recognizing that possessing them could enhance the quality of his work and provide economic benefits to the new company. Kim further admitted to being aware that his actions could harm Broadcom, particularly as his new employer sought to become a competitor by developing competing products internationally (Newland, 2023).

Another case involves a high-ranking National Aeronautics and Space Administration (NASA) official who faced legal consequences after being convicted of providing false information about his involvement in the Chinese Thousand Talents Program. During questioning by investigators, he misled them about his affiliation and position as a professor in Chinese universities. The Thousand Talents Program, funded by the Chinese government, recruits individuals with access to foreign technologies and intellectual property. Among its participants was Meyya Meyyappan, a senior NASA scientist with privileges to sensitive and classified US government technologies and intellectual property. In June 2021, Meyya Meyyappan was sentenced to a 30-day prison term for giving inaccurate statements to the FBI. Meyyappan was not only a member of the Thousand Talents Program but also held a professorship at a Chinese university, supported by Chinese government funding (Biase & Margolin, 2021).

The Chinese government has consistently denied any involvement in these cyberattacks, but there is widespread belief that the hackers were acting on behalf of the Chinese government or military. These incidents raised significant concerns for the US government and military, highlighting the vulnerabilities in their computer systems and the potential for foreign powers to gain access to sensitive information.

In response to these attacks, the US government implemented various measures aimed at enhancing the security of its computer systems and fortifying defenses against future attacks. These initiatives encompassed the adoption of more robust cybersecurity protocols, the deployment of advanced technologies for detecting and preventing cyber threats, and the training of personnel to identify and mitigate the risks associated with cyberattacks. Despite these concerted efforts, the US government and military have remained targets of cyberattacks.

Conflicting Perceptions

There is a fundamental contrast between Eastern and Western perspectives when it comes to distinguishing between cyber espionage for national security reasons and cyber espionage for economic gains (Lindsay et al., 2015). While the US typically observes this boundary, China may not. One nation may view economic growth and national security as separate entities, while the other sees them as interconnected. The traditional requirement for physical presence in technology transfer has been replaced by internet-based access, raising concerns over copying sensitive intellectual property, such as designs from Department of Defense contractors, which some US authorities consider akin to stealing state secrets (Finklea & Theohary, 2015, January).

In the eyes of American officials, cyber espionage can be seen as a new form of warfare that sets the stage for battle by promoting technology transfer (Lasiello, 2016). They may view the theft of intellectual property from companies supporting military technology as a form of warfare. On the contrary, China may perceive war as a business and view cyber espionage and intellectual property theft through the lens of natural rules aligned with Confucian principles.

The US has several reasons to view China's pursuit of aggressive cyber capabilities with concern. Firstly, China may view it as a means to alleviate political and military pressure from the West, particularly the US. Secondly, China aims to strengthen its armed forces. Lastly, China seeks to close its technological gap in order to advance economically. Cyber operations are seen by China as a crucial asymmetric weapon for information warfare that can effectively counter US influence. China's cyber capabilities are described as a form of "acupuncture warfare," targeting weaknesses in command, control, communications, and information systems to paralyze adversaries (Billo & Chang, 2004).

China expresses significant concerns about American intervention and interference in other countries' sovereignty (Chung, 2004). China contends that such involvement frequently occurs under the pretext of the United Nations, and when Western nations cannot advance their interests through the UN, they unite under The North Atlantic Treaty Organization (NATO). Western nations are perceived as seeking to maintain their dominance in the world by relying on economic, scientific, and technological superiority while resisting cultural diversity and balanced human civilization growth.

Given China's historical experiences with Western imperialism, it is not surprising that China is apprehensive about Western engagement in regions such as Tibet or Taiwan (Barr, 2011). Narrowing the economic, scientific, and technical gap between China and the West is a high priority driven by China's national interests. China seeks to position itself as a leader and supporter of emerging nations, emphasizing peaceful development and adhering to the five principles of peaceful coexistence, as it did in the 1950s, to dispel the notion of being a growing threat. These principles include non-interference in others' affairs, equality and mutual benefit, non-aggression, peaceful coexistence, and respect for national sovereignty and geographical boundaries (Carty & Lone, 2011).

China aims to project the idea that modernization is a peaceful process, as the opposite perception would be detrimental (Zheng, 1999). Additionally, China reassures emerging nations, particularly its neighbors, that their economies will benefit from China's progress. China's government follows the concept of comprehensive national power (CNP), which aims to unite all aspects of the state to achieve its

goals alongside ongoing economic growth. Under this paradigm, China does not clearly distinguish between military and non-military means. The idea of CNP is inspired by ancient Chinese military strategists who emphasized the integration of military and non-military forces to outperform adversaries (Office of the Secretary of Defense, 2007, January). This understanding clarifies China's strategy in cyber conflict and resource allocation to gain an advantage.

China blurs the lines between military and non-military resources instead of separating them, aiming to gain an advantage over its competitors (Hoffman, 2007). Business is often viewed as a form of warfare in China, with national policy and nationalist sentiment influencing business decisions. Despite being a significant global commercial partner, China's business relationships can be simultaneously cooperative, competitive, and antagonistic. Those engaged in business with China must also be cautious about the covert removal of their online information. Business travelers to China frequently experience computer eavesdropping and searches of hotel rooms. In China, cyberspace is simply another tool for information warfare (Cheng, 2016).

The Western world's laws, religious doctrines, and political ideologies are based on the premise that peace and war are fundamentally opposed and cannot coexist. China challenges this notion by recognizing that even positive interactions can involve conflict.

Any relationship with China based on mutual support will always involve an ongoing Competition for personal gain will also entail fundamentally different ideas about societal institutions and personal freedoms. Therefore, it is expected that China will engage in cyber espionage while the West works to uphold a global system that protects property rights and individual liberties. Western countries may prioritize safeguarding these rights over any potential benefits that could arise from weakening legal norms and blurring the distinction between public and private enterprise. Chinese officials remain committed to narrowing the economic and technological gap between the East and the West, even if they currently have less to steal than more advanced Western nations (Alford, 1995).

Historical Development of Intellectual Property

Political and business practices are influenced by a range of factors, including historical events and cultural norms. Therefore, it is important to examine the historical development of intellectual property to understand how different interpretations of this concept have evolved over time, which paints a picture of the motivations behind industrial cyber espionage (Wangen, 2015). During the Song Dynasty (AD 960–1279) in imperial China, as printing technology advanced, government authorities witnessed an increase in literacy. They sought to control the dissemination of printed literature that they deemed disrespectful to the imperial family. Works that referenced imperial ancestors or copied astronomical charts, both considered matters of state, were prohibited.

To prevent unauthorized duplication of certain works that were under sole state control, private printers needed prepublication authorization by 1009 (Alford, 1995). The consequences for breaking these rules ranged from severe physical punishment to exile. Authorized printers often included notices of governmental approval in their works to discourage illicit reproductions. Subsequent dynasties also restricted the use of emblems associated with the imperial family or officials to protect trademarks, especially when those marks identified goods exclusively created for the imperial family. These protective measures aimed to preserve imperial rule and the hierarchical ties within society. The establishment of individual property rights or the guarantee of financial success through intellectual property rights were not major concerns. Reproduction of registered printed works without authorization was seen as a violation of governmental monopolies and a disruption of social order.

In contrast, Chinese imperial history did not witness a comparable development and protection of intellectual property as exists today. There was no recognition of property rights for writers or inventors in their works. The Chinese authorities prioritized political power, law, and order, and stability over concerns of private property. There were no legal frameworks supporting individuals or groups in asserting claims to protect their intellectual property rights, even if the state may have granted monopoly rights to specific families or guilds. Instead of compensating the aggrieved party, state responses to such claims often focused on maintaining fairness, harmony, and peace.

Influenced by Confucian teachings, Chinese philosophy placed greater emphasis on the transfer of knowledge and intellectual endeavors as gifts from the past rather than their individual creation. Ideas were not considered purely human inventions but imitations of natural principles. Therefore, state authorities had limitations in censoring access to or imitation of expressions closely associated with China's common ancestors. Instead, people were encouraged to engage with and inherit the shared past and heritage from their ancestors. It is inevitable that traditional European notions of fairness and private autonomy over intellectual property earnings would clash with Chinese ideals.

Writing and other intellectual pursuits often require an ongoing chain of invention, which one culture may perceive as an expensive and time-consuming activity while another sees it as a perpetual supply of gifts from ancestors. While cyber espionage, through the swift duplication of digital blueprints for military weapons, can rapidly erode strategic advantages without the need for equivalent investments in time and resources, potentially disrupting the global balance of power, the Western copyright regime may be seen as unnaturally restricting or limiting this flow of ideas.

This clash of cultural viewpoints underscores the importance of a nuanced understanding of intellectual property concerns in a global context, taking into account diverse beliefs, practices, and their implications for economic and strategic dynamics.

A Note on Methodology

This paper employs analytical, comparative, and descriptive methods to examine recent developments in economic cyber espionage within the context of US-China relations. The study relies on a remote-based content analysis of primary and secondary sources, including academic journals, books, expert testimonies, official statistics, current public information, and media interpretations. Government

documents and official doctrines are also considered, with the state-run Daily Graphic newspapers serving as key sources for leaders' and government figures' views and opinions. The objective is to qualitatively analyze current trends in cyber espionage and provide easily understandable information about economic espionage warfare, particularly the one involving the US and China.

The analysis draws on the author's personal observations of the negative impacts of international relations and cybersecurity in the context of economic conflict between the US and China. These perspectives and experiences are informed by discussions with senior colleagues in the fields of international relations, cybersecurity, and economic studies, as well as a review of relevant scholarly literature. To provide a comprehensive analysis, the paper gathers, evaluates, and synthesizes data from multiple information sources.

The focus on the foundational countries of the US and China supports the study's justification and emphasis. It examines case studies of espionage operations from 1990 to 2022, offering a historical perspective on contemporary industrial espionage efforts employed by these countries. By drawing on contemporary international relations theories, the analysis explores the interaction between cyber espionage activities and foreign policy decision-making, affecting the economic advantage of countries.

China Sneaks out America's Technology Secrets

A former employee of GE Power, Zheng Xiaoqing, an American citizen, faced various charges from DOJ, accused of concealing confidential files taken from his place of work, in the form of a binary code of a digital image (Johnson, 2021). He then sending the information to his own email address, using a technique known as steganography, which involves hiding one data file inside another. Zheng was accused of using this method repeatedly to take confidential information from the GE Company.

General Electric, a prominent multinational company involved in various industries such as healthcare, energy, and aerospace, is known for its wide range of products, from refrigerators to aircraft engines. Zheng targeted sensitive information related to the development of gas and steam turbines, including details about blades and seals. These stolen files, worth millions of dollars, were sent to an accomplice in China. Ultimately, they would benefit the Chinese government, businesses, and educational institutions.

In a series of related cases, US authorities have prosecuted individuals involved in these activities. One such case involved Chinese national Xu Yanjun, who received a 20-year prison sentence for attempting to steal trade secrets from multiple US aviation and aerospace companies, including GE. Yanjun is believed to be a professional spy. These incidents are viewed by US government sources as part of a broader conflict, with the US aiming to prevent the emergence of a strong rival to its dominance, while China seeks to acquire technological knowledge to bolster its economy and challenge the geopolitical order.

The theft of trade secrets is appealing because it allows nations to quickly advance within global value chains without the time and cost associated with relying solely on domestic capabilities. The FBI Director Christopher Wray warned business executives and academics in London about China's intentions to steal intellectual property from Western companies, as part of its efforts to accelerate industrialization and gain control over crucial industries (Wu, 2020). He highlighted China's extensive spying operations, targeting businesses of all sizes and spanning various sectors, including aviation, artificial intelligence, and pharmaceuticals.

China on knocking Down America's Status

According to DOJ statement regarding Zheng, Alan Kohler Jr. of the FBI reportedly suggested that China specifically targeted American ingenuity in an effort to undermine the US' position as the world's leading power (Kissinger, 2012).

Zheng, an engineer specializing in steam turbines and turbine sealing technology, was involved in the development of leakage containment techniques. These seals play a crucial role in enhancing turbine performance by increasing power, efficiency, and lifespan, particularly in gas turbines used in the aviation sector. China has identified aerospace and aviation equipment as one of the key industries for rapid growth, aiming to reduce dependence on foreign technology and eventually surpass it (Wübbeke et al., 2016).

Previously, economic espionage was a significant concern involving countries like Japan, South Korea, Taiwan, and Singapore (Thurbon & Weiss, 2006). As these nations emerged as innovators and sought to protect their intellectual property, their governments enacted legislation to address the issue more seriously. China has witnessed a similar trend, strengthening domestic intellectual property rights over the past decade as Chinese businesses became more inventive. This development coincided with China's rise as a major economic power.

Furthermore, China has gained expertise through joint venture agreements that require international companies to share technology in exchange for access to the Chinese market (Mu & Lee, 2005). Despite allegations of coercion, the Chinese government has consistently denied such claims.

These factors demonstrate the evolving landscape of industrial espionage and the protection of intellectual property, as nations with emerging innovation capacities prioritize safeguarding their own intellectual property rights.

Hacking Deal

Efforts have been made in the past to address hacking and intellectual property theft, specifically between the US and China. In 2015, both countries reached an agreement pledging not to engage in cyber espionage to gain financial advantages by stealing intellectual property, trade secrets, or private company information (Iasiello, 2016). However, the following year, the US National Security Agency accused China of violating the agreement, despite acknowledging a decrease in hacking attempts targeting corporate and government data.

The overall impact of the agreement has been widely criticized for its lack of enforcement, with some considering it a mere "joke." According to experts, Chinese cyber espionage in the US has been pervasive, infiltrating academic laboratories and affecting various

aspects of Western companies. The extent of this phenomenon remains disputed, as different opinions exist. Some argue that Chinese cyber espionage temporarily declined before resurging, while others believe that the agreement failed due to deteriorating US-China relations.

Simultaneously, the US is actively taking steps to impede China's progress in the crucial semiconductor industry, perceiving it as a national security threat (Allen, 2019). Strict export regulations were implemented in October, requiring licenses for companies exporting chips to China that employ US equipment or software. Additionally, these regulations limit the employment of US green card holders and citizens by certain Chinese semiconductor firms.

While these measures may hinder China's technological development, they could also accelerate its efforts to reduce reliance on imported goods in its technology supply chains, a long-standing goal with mixed outcomes (Liu et al., 2020). Experts suggest that recent US controls have intensified the urgency of these policy objectives.

Considering the mention of national security concerns by both nations, it is expected that the two largest economies will further compete for technological superiority. However, some analysts believe that the US still holds an advantage, as reports indicate that US intellectual property remains the most sought-after technology in hacking attempts against Chinese websites, as pointed out by Mr. Wang.

Cyber Espionage Network

The realm of cyber espionage has long been a source of frustration for officials in Washington, and recent revelations of extensive data mining have brought this issue into the public eye (Lyon, 2015). While China's aggressive cyber theft attempts targeting American military and commercial secrets have received significant media coverage in the West, Chinese President Xi Jinping countered at the 2013 summit by highlighting China's own experiences as a victim of cyber espionage.

The US also possesses a team of hackers who are well-versed in China's networks. In a strategic move, White House officials strategically leaked information to the media prior to the summit, disclosing President Obama's intention to privately address the highly contentious issue of China's extensive use of computer hacking to acquire US government, military, and commercial secrets. Senior Chinese officials responded by publicly accusing the US government of hypocrisy and admitting their active engagement in cyber espionage (Lasiello, 2016).

It turns out that the claims made by the Chinese government are largely accurate. According to multiple media reports, the National Security Agency's highly classified division known as the Office of Tailored Access Operations (TAO) has successfully infiltrated Chinese computer and telecommunications systems for nearly 15 years, gathering invaluable intelligence on the inner workings of the People's Republic of China (Harris, 2014). Due to the sensitive nature of its activities, TAO remains highly secretive and is accessible to only a limited number of individuals within the NSA.

By breaching the computers and telecommunications systems of foreign targets, bypassing passwords, undermining computer security measures, extracting data from hard drives, and intercepting all messages and data traffic within targeted email and text-messaging systems, the TAO covertly collects intelligence on foreign targets. These operations are referred to as "computer network exploitation" by the NSA.

Additionally, TAO is responsible for gathering the intelligence required by the US to conduct cyberattacks, which, if authorized by the president, can disrupt or destroy foreign computer and telecommunications systems. The US Cyber Command (Cybercom), whose commander also serves as the head of the NSA, is the entity legally authorized to engage in such cyber warfare.

With a staff of over 1000 military and civilian experts in target acquisition, computer hacking, intelligence analysis, computer hardware and software design, and electrical engineering, TAO currently represents the largest and arguably the most crucial component of the NSA's expansive Signal Intelligence Directorate. Since its establishment in 1997, TAO has gained a reputation for providing the US intelligence community with high-quality intelligence, not only on China but also on foreign terrorist organizations, espionage operations against the country, global ballistic missile and weapons of mass destruction developments, as well as the latest political, military, and economic developments worldwide.

The Challenge of Attribution

According to Chinese authorities, cyberspace holds strategic value and can be utilized to bridge the military gap between China and the dominant world power, particularly the US (Akdag, 2019). They recognize the significance of cyberspace as the foundation for American military and economic superiority.

However, it is incorrect and misleading to claim that all Chinese malware is a result of intentional or planned intelligence collection efforts by the Chinese government. Data indicates a different story. With the world's largest internet population and a substantial number of digitally savvy young individuals, China currently leads the world in terms of internet usage. The increase in Chinese malware can be attributed to the large number of internet users in the country. It is only logical that as more creative individuals gain access to computers, China's population may contribute to a higher incidence of cybercrime.

In recent years, there have been increasing claims linking Chinese hackers to high-level intrusions into computer networks across Europe, North America, and Asia. Nations such as the US, Britain, France, Germany, South Korea, and Taiwan have accused Chinese hackers of compromising their government computers. Chinese hackers have also been alleged to steal data from computers belonging to international governments, businesses, and financial organizations. The US Department of Defense confirms ongoing Chinese targeting, particularly through the "Titan Rain" attacks that have targeted the Department of Defense and various defense firms since 2003.

Furthermore, claims have been made regarding attacks originating from China that specifically target non-governmental organizations supporting China's national objectives. These groups include the Falun Gong, Tibetan organizations operating in India, and advocacy groups for the Darfur conflict in Sudan. Many of these attacks involve website defacements, denial-of-service attacks, or virus propagation. While some of these attacks align with official Chinese aims and interests, none have been directly linked to Chinese state authorities or specific individuals to date.

Attributing cyberattacks to specific actors is a challenging task, often referred to as the attribution problem. The internet was not initially designed with security as a top priority. The current intellectual property (IP) V4 address assignment system has flaws and hacking techniques that allow perpetrators to hide their true identities and locations. Online identities and servers can be expertly concealed, and traffic flows and connections can be masked and diverted through multiple servers. Even a machine belonging to a reputable organization can be compromised by a skilled attacker, who can then use it as a base for their attacks.

The challenge of determining the motivations behind cyberattacks is closely tied to the attribution issue. Individuals engaging in internet-based attacks and exploits do so for various reasons, ranging from monetary gain to fear of prosecution or strong emotional motives such as nationalism and religion. Many cyberattacks and exploits, even those that appear to benefit nations, may actually be the work of third-party actors with diverse objectives. Due to the complexity involved, it is difficult to separate the individual's intent from the potential motivations of the party on whose behalf the attacks were conducted or a potential client to whom the offender is trying to sell their services. Identifying the perpetrators and understanding their intentions allows state actors to maintain plausible deniability and formally distance themselves from the attacks in any given scenario.

Cyber campaigns can sometimes take on a life of their own. Even if a state covertly supports a particular campaign or refrains from enforcing laws or prosecuting offenders, these campaigns are inherently chaotic and unpredictable in terms of their scope and outcomes (Kadish et al., 2016). The primary goals of a Cyber campaign may be surpassed by the phenomenon of spontaneous cyber riots. With minimal barriers to entry in this field, anyone with a computer and an internet connection can engage in cyberattacks (Denning, 2009). Despite the inherent uncertainty of the results, governments generally appear to tacitly benefit from online expressions of nationalistic and patriotic enthusiasm.

Authorities in China likely perceive specific attackers and their online behavior as useful tools of state power. However, governments may not always exercise strict control over these activities (Nye, 2010). Groups can operate independently and autonomously, carrying out their own cyber projects that may not necessarily be approved by authorities or serve national interests.

Cyber Espionage and International Law

While intelligence-related operations are widely recognized as a characteristic of modern governments, it is important to note that there are no specific treaties or customary international laws that explicitly regulate espionage during times of peace (Lotrionte, 2014). This intentional ambiguity and lack of regulation demonstrate the complex nature of addressing this behavior within the realm of international law. As a result, the legality of espionage under international law is neither clearly established nor explicitly criminalized in the absence of specific laws addressing peacetime espionage.

The Lotus principle, which asserts that in the absence of prohibitive norms, states have the discretion to adopt principles they consider appropriate, contradicts the notion that international law does not regulate espionage. In other words, the Lotus principle maintains that state behavior is either legal and permitted or illegal and prohibited under international law, leaving no room for a non liquet (dekker & Werner, 1999). This principle continues to hold legal standing and has been upheld by the International Court of Justice, despite criticisms of it as an outdated interpretation of international law. Therefore, if espionage is not explicitly prohibited, it should be considered a legal practice under international law.

Furthermore, while espionage itself may find justification under the Lotus principle, it would be overly simplistic to conclude that international law has minimal relevance to information gathering activities. Espionage and international law are intertwined in complex ways (Brown & Poellet, 2012). International law consists of a "checkerboard" of general legal principles and specific frameworks that indirectly govern espionage by addressing the underlying behaviors involved in espionage activities. Certain behaviors related to espionage are restricted under international law in specific contexts and in relation to specific individuals (Demarest, 1995).

The perception that espionage and international law do not intersect is held by some international lawyers. However, this perspective is challenged by scholars who argue that international lawyers deliberately abstain from applying international law to espionage, viewing it as the "elephant in the room" rather than a legal loophole (Margulies, 2016). This agnosticism can be attributed to concerns about the effectiveness of laws in safeguarding state sovereignty and maintaining global peace and security in an unpredictable and dangerous international system. Consequently, international lawyers have been hesitant to endorse laws that prohibit states from conducting espionage, which is considered necessary for national security (Scott, 1999). Espionage provides states with valuable insights into the goals and capabilities of other actors in the international system. International lawyers find themselves in a challenging position. On one hand, they cannot deny that intrusive actions like espionage are subject to international legal norms without undermining the legitimacy of international law (Roth, 1999). On the other hand, they are unwilling to relinquish espionage as a tool of statecraft due to the perceived advantages it offers for national security. Thus, the way out of this dilemma has been to claim that international law is silent on the subject and avoid probing whether espionage aligns with it (Broeders et al., 2022).

However, with the significant increase in political espionage, particularly in the realm of cyber-enabled activities, it is no longer possible to simply overlook the issue (Borghard & Lonergan, 2021). International lawyers should no longer disregard cyber-enabled political espionage, and there has been a growing body of international legal literature addressing this topic. Nonetheless, experts influenced

by realist theory continue to emphasize the national security benefits of political cyber espionage and argue that it operates in a legal gray area. Some argue that international law does not apply to cyber surveillance or cyber spying conducted by a government outside its own borders in most cases (Lotrionte, 2014).

Interestingly, international lawyers have shown reluctance to examine how international law applies to economic espionage (Finnemore & Hollis, 2020). Economic espionage violates the sovereignty of the host country when trade secrets of targeted companies are stolen, negatively impacting the national economy. Economic espionage, unlike political espionage, does not provide immediate and direct benefits to the perpetrating state in terms of national security (Lotrionte, 2014). Instead, it benefits the perpetrating state's national security in the long run by bolstering its economic strength and providing domestic businesses with advantages over foreign competitors.

The reluctance of international lawyers to explore the governance of economic espionage under international law may stem from concerns that it would open a Pandora's box and raise questions about how political espionage is governed (Skinner, 2013). By focusing on protecting political espionage from international legal scrutiny, international lawyers have disregarded the dangers posed by economic espionage. However, there is a growing demand from both the public and private sectors to address economic cyber espionage within the framework of international law (Skinner, 2013). Despite this, international lawyers have paid limited attention to investigating how international law can effectively counter commercial cyber espionage.

Many still argue that international law remains a bystander in the realm of espionage, characterized by stealth, deception, and greed. Once again, it appears that international lawyers fear that subjecting political cyber espionage to close scrutiny may also restrict politically motivated espionage and deny the national security benefits it offers (Geers, 2011).

Norm against Economically-Motivated Cyber Espionage

The contestation between the US and China regarding cyber espionage rules exemplifies the complexity of the issue. Around 2009, US officials and their allies argued that while cyber espionage for national security reasons was acceptable, it crossed the line when motivated by economic gain, especially if the stolen information was shared with corporations to give them an unfair trade advantage (Lindsay, 2013). The Director of National Intelligence in 2013 emphasized that the US does not engage in stealing trade secrets or provide gathered intelligence to American businesses for their profitability or competitiveness.

However, the US could not credibly use the threat of engaging in economically motivated cyber espionage. They needed a way to identify intellectual property within private Chinese organizations that American businesses could utilize, and they would violate the law if they shared the information with a single US competitor without doing the same for all of them (Lam, 2009). Moreover, even if the US took such measures, China would still have the upper hand as US corporations have far more intellectual property at risk than Chinese companies. The WTO, of which China is a member, amended its Agreement on Trade-Related Aspects of Intellectual Property Rights to prohibit intellectual property theft, which gained widespread consensus (Shu Shang & Shen, 2021). However, it didn't provide sufficient justification for a rule explicitly banning economically motivated cyber espionage.

Initially, the rule against cyber espionage was portrayed as a prohibition on targeting specific entities. Essentially, the US argued that by refraining from eavesdropping on for-profit organizations, it was reasonable to expect others to do the same. However, this argument became challenging to defend after the Snowden revelations revealed US cyber espionage activities targeting for-profit organizations. These efforts were aimed at identifying vulnerabilities in commercial products that could potentially compromise the systems of their clients (who might be legitimate targets for national security), tracking terrorists using commercial systems (especially in telecommunications), or enhancing the US's negotiating position with other countries.

Consequently, the US changed its stance to emphasize that it didn't engage in espionage on for-profit organizations to support US businesses' competitiveness. In other words, the US position was refined to narrow the application of the outcomes.

China has never officially claimed that cyber espionage for commercial gain is equivalent to espionage for national security purposes. Instead, it has increasingly implausibly denied any evidence of Chinese involvement, as stated by the US and other accusers. However, the credibility of China's position was undermined by the Mandiant study in February 2013 and subsequent information from other US cybersecurity firms. By May 2015, few in Beijing made efforts to deny China's involvement in cyber espionage with commercial objectives.

Ultimately, the US achieved its objective. In September 2015, President Xi Jinping pledged that China would not participate in or tolerate such cyber espionage. There is evidence that China has mostly adhered to this commitment. For instance, FireEye, after acquiring Mandiant, reported a significant decline in the number of monthly investigations into Chinese cyber espionage for corporate clients, dropping from 35 per month before the acquisition to 3 to 10 per month afterward. Although China became more adept at avoiding detection following the agreement, the decrease in espionage activities cannot be solely attributed to enhanced tradecraft. The US successfully established the first standard: cyber espionage is permissible as long as its outcomes are not used to aid a nation's businesses in competition.

China privately criticized the US' position on intellectual property theft, considering it hypocritical given how stolen innovations had contributed to US industrial growth in the past (Kania & Laskai, 2021). However, with China now among the leaders in technology licensing, the country advocated for these standards because it stood to lose more from such theft than to gain (Peng et al., 2017). Perhaps the Chinese were beginning to realize that their own businesses would struggle to develop technology only to have it stolen if intellectual property, including internal thefts, were not respected.

Public and Private Sectors in China

Throughout China's history, the economic system has been controlled by the government. And there is no sign of changing this system to follow the capitalist system run by Western countries. Contrary to some expectations, China's commitment to the model of state-owned enterprises has strengthened, especially following the global financial crisis of 2008. At that time, the free market system was highly criticized, leading many countries to admire the Chinese government system, where state-owned companies are the only way to strengthen the country's economy. Since then, the Chinese government has prioritized an economic system controlled by the state-owned companies.

Understanding the historical context of espionage in China is crucial, as it carries different moral implications and connotations compared to Western perceptions of spying. China's political history and popular culture have long been intertwined with examples of shifting allegiances, profiteering, deception, and espionage. This pattern has remained remarkably stable over the centuries, from ancient times during the Warring States period to the Chinese Revolutionary Civil War in the 20th century.

Notable works like "Unrestricted Warfare" (Chaoxian Zhan), written by members of the People's Liberation Army (PLA), challenge Western notions of conflict by advocating for a broader definition of warfare that includes tactics like economic warfare during peacetime or cyber operations (Wither, 2016). This perspective makes it challenging for Chinese officials to keep distinct boundaries between the public and private sectors or to engage in espionage without involving both spheres. Considering this historical lack of separation is crucial when attempting to understand or predict Chinese political behavior regarding espionage.

Western countries often misinterpret Chinese concerns about repeating past mistakes that led to numerous disasters in the previous century or becoming victims of foreign exploitation (Westad, 2003). This can sometimes lead to a misunderstanding of Chinese attitudes as ignorance. In reality, these concerns reflect China's awareness of its rapid growth and the precariousness it has faced (and perhaps still faces) on its path. Therefore, from the Chinese perspective, ideas such as not strictly adhering to international laws, seizing opportunities whenever and wherever they arise, and rapidly enhancing national strength are rational responses. Economic espionage has never been stigmatized in China due to its historical approach to blending state and private firms in the market strategy (Lasiello, 2016).

Conclusion

There is a general consensus among observers that China engages in extensive cyber espionage to steal IP from the US military, private companies, and other nations. United State officials claim that China's operations go beyond traditional cyber espionage, which typically focuses on national defense and military preparedness, and accuse China of sharing the stolen IP with its government-controlled domestic companies (Ball, 2011).

The competition between the US and China over cyber espionage laws underscores the complexity of this problem. This discrepancy is brought about by the cultural and historical differences that exist between these two countries. China's economic system has been controlled by the government for a long time, and the system of state-owned enterprises is largely supported.

The historical context of espionage in China differs from Western perceptions and is deeply rooted in the country's political history and culture. Chinese officials view espionage as a tool of state power and often blur the boundaries between the public and private sectors (Deibert & Rohozinski, 2010). The blending of state and private firms in the market strategy has contributed to the acceptance of economic espionage in China.

However, the US accuses China of going beyond traditional cyber espionage by sharing stolen intellectual property with government-controlled domestic companies, providing them with an unfair economic advantage. Cultural differences further contribute to the perception gap, as China views intellectual property as communal and business and conflict as intertwined, while the US emphasizes protection and sees peace and conflict as incompatible.

The US argued that cyber espionage for national security reasons is acceptable, but not for financial gain that provides unfair trade advantages (Lotriont e, 2014). World Trade Organization addressed intellectual property theft but did not explicitly ban financially motivated cyber espionage. The US refined its stance to emphasize not engaging in espionage on for-profit organizations to support US businesses' competitiveness. China initially denied involvement but later pledged to refrain from cyber espionage. The US aimed to establish a standard that permits cyber espionage as long as it does not aid a nation's businesses. China criticized the US position but eventually recognized the importance of respecting intellectual property.

While there are no specific treaties or customary laws governing espionage during times of peace, the Lotus principle suggests that in the absence of prohibitive norms, states have the discretion to adopt appropriate principles. This principle, upheld by the International Court of Justice, implies that espionage should be considered legal unless explicitly prohibited.

Hakem Değerlendirmesi: Dış bağımsız.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.

Declaration of Interests: The author declare that they have no competing interest.

Funding: The author declared that this study has received no financial support.

References

Akdag, Y. (2019). The likelihood of Cyberwar between the US and China: A neorealism and power transition theory perspective. *Journal of Chinese Political Science*, *24*(2), 225–247. [CrossRef]

Alford, W. P. (1995). *To steal a book is an elegant offense: Intellectual property law in Chinese civilization*. Stanford University Press.

Allen, G. C. (2019). *Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security*. Center for a New American Security. (http://www.globalhha.com/doclib/data/upload/doc_con/5e50c522eeb91.pdf)

Ball, D. (2011). China's cyber warfare capabilities. *Security Challenges*, *7*(2), 81–103.

Barr, D. M. (2011). *Who's afraid of China?: The challenge of Chinese soft power*. Bloomsbury Publishing.

Bernik, I. (2014). *Cybercrime and cyber warfare*. John Wiley & Sons.

Berrell, M., & Wrathall, J. (2006). Between Chinese culture and the rule of law: What foreign managers in China should know about intellectual property rights. *Management Research News*, *30*(1), 57–76. [CrossRef]

Biase, N., & Margolin, J. (2021). *Senior NASA scientist sentenced to prison for making false statements related to the Chinese thousand talents program*. https://www.justice.gov/usao-sdny/pr/senior-nasa-scientist-sentenced-prison-making-false-statements-related-chinese-thousand

Billo, C., & Chang, W. (2004). Cyber warfare. *An Analysis of the means and motivations of selected nation states*. ISTS.

Borghard, E. D., & Lonergan, S. W. (2021). Deterrence by denial in cyberspace. *Journal of Strategic Studies*, 46(3), 535–569.

Boylan, B. M., McBeath, J., & Wang, B. (2021). US–China relations: Nationalism, the trade war, and COVID-19. *Fudan Journal of the Humanities and Social Sciences*, *14*(1), 23–40. [CrossRef]

Brander, J. A., Cui, V., & Vertinsky, I. (2017). China and intellectual property rights: A challenge to the rule of law. *Journal of International Business Studies*, *48*(7), 908–921. [CrossRef]

Bresciani, U. (2023). *Reinventing Confucianism*. Passerino Editore.

Broeders, D., de Busser, E., Cristiano, F., & Tropina, T. (2022). Revisiting past cyber operations in light of new cyber norms and interpretations of international law: Inching towards lines in the sand? *Journal of Cyber Policy*, *7*(1), 97–135. [CrossRef]

Brown, C. S. D. (2015). Cyber-attacks, retaliation and risk: Legal and technical implications for nation-states and private entities. In *Cybersecurity policies and strategies for Cyberwarfare prevention* (pp. 166–203). IGI Global. [CrossRef]

Brown, G., & Poellet, K. (2012). The customary international law of cyberspace. *Strategic Studies Quarterly*, *6*(3), 126–145.

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3), 1–18. [CrossRef]

Carty, A., & Lone, F. N. (2011). Some New Haven international law reflections on China, India and their various territorial disputes. *Asia Pacific Law Review*, *19*(1), 93–112. [CrossRef]

Chen, J., Zhu, Z., & Yuan Xie, H. Y. (2004). Measuring intellectual capital: A new model and empirical study. *Journal of Intellectual Capital*, *5*(1), 195–212. [CrossRef]

Cheng, D. (2016). *Cyber dragon: Inside China's information warfare and cyber operations: Inside China's information warfare and cyber operations*. abc-clio.

Chung, C. P. (2004). The Shanghai Co-operation organization: China's changing influence in Central Asia. *China Quarterly*, *180*, 989–1009. [CrossRef]

Coe, N. M., & Yeung, H. W. C. (2015). *Global production networks: Theorizing economic development in an interconnected world*. Oxford University Press.

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, *21*(4), 43–57. [CrossRef]

Deibert, R., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. (2009). Tracking ghostnet: Investigating a cyber espionage network. *Tracking GhostNet: Investigating a cyber espionage network*. (https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5f-e7708d543651/download_file?safe_filename=Gh0stNet.pdf&file_format=application%2Fpdf&type_of_work=Report)

dekker, & Werner (1999). The completeness of international law and Hamlet's dilemma. *Nordic Journal of International Law*, *68*(3), 225–247. [CrossRef]

Demarest, G. B. (1995). Espionage in international law. *Denver Journal International Law & Policy*, *24*, 321.

Denning, D. E. (2009). Barriers to entry: Are they lower for cyber warfare? *IO Journal*, *1*(1), 4.

Dotson, J. D. (2011). On the Front Line of Chinese Espionage: A New Lexicon for Understanding Chinese Front Companies? *American Intelligence Journal*, *29*(2), 55–69.

Enoru, D. O. (2022). *The rise of the People's Republic of China poses a potential strategic challenge to the United States* (Doctoral Dissertation). National American University.

Finklea, K. M., & Theohary, C. A. (2015, January). *Cybercrime: Conceptual issues for congress and US law enforcement*. Congressional Research Service, Library of Congress.

Finnemore, M., & Hollis, D. B. (2020). Beyond naming and shaming: Accusations and international law in cybersecurity. *European Journal of International Law*, *31*(3), 969–1003. [CrossRef]

Fleisher, C. S., & Wright, S. (2009). Examining differences in competitive intelligence practice: China, Japan, and the West. *Thunderbird International Business Review*, *51*(3), 249–261. [CrossRef]

Flint, C. (2021). *Introduction to geopolitics*. Routledge.

Friedman, E., & Lee, C. K. (2010). Remaking the world of Chinese labour: A 30-year retrospective. *British Journal of Industrial Relations*, *48*(3), 507–533. [CrossRef]

Fukuyama, F. (1995). Social capital and the global economy. *Foreign Affairs*, *74*(5), 89. [CrossRef]

Geers, K. (2011). *Strategic cyber security*. Kenneth Geers.

Halbert, D. (2016). Intellectual property theft and national security: Agendas and assumptions. *Information Society*, *32*(4), 256–268. [CrossRef]

Hall, P. A., & Soskice, D. (Eds.) (2001). *Varieties of capitalism: The institutional foundations of comparative advantage*. Oxford University Press.

Halligan, R. M. (2007). Protection of US trade secret assets: Critical amendments to the economic Espionage Act of 1996. *The John Marshall Review of Intellectual Property Law*, *7*, i.

Harris, S. (2014). *@ War: the rise of the military-internet complex*. Houghton Mifflin Harcourt.
Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. *Journal of Strategic Security*, *4*(2), 1–24. [CrossRef]
Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars* (p. 51). Potomac Book Company Institute for Policy Studies.
Iasiello, E. (2016). China's three warfares strategy mitigates fallout from cyber espionage activities. *Journal of Strategic Security*, *9*(2), 47–71. [CrossRef]
Ikenberry, G. J. (2020). *A world safe for democracy: Liberal internationalism and the crises of global order*. Yale University Press.
Johnson, J. (2021). Securing secrets: The need for a treaty addressing state-sponsored economic espionage. *West Virginia Law Review*, *124*, 327.
Joshi, S. C., & Sheikh, A. A. (2015). 3D printing in aerospace and its long-term sustainability. *Virtual and Physical Prototyping*, *10*(4), 175–185. [CrossRef]
Kadish, S. H., Schulhofer, S. J., & Barkow, R. E. (2016). *Criminal law and its processes: Cases and materials*. Aspen Publishing.
Kania, E. B., & Laskai, L. (2021). *Myths and realities of China's military-civil fusion strategy*. Center for a New American Security.
Kapoor, P. (2022). Intellectual property & the challenge of a digital world. *Jus Corpus Law Journal*, *3*, 67.
Kissinger, H. A. (2012). The future of US-Chinese relations: Conflict is a choice, not a necessity. *Foreign Affairs*, *91*, 44.
Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: Some economic and institutional considerations. *Electronic Commerce Research*, *13*(1), 41–69. [CrossRef]
Lam, M. L. L. (2009). Beyond credibility of doing business in China: Strategies for improving corporate citizenship of foreign multinational enterprises in China. *Journal of Business Ethics*, *87*(S1), 137–146. [CrossRef]
Lara, C. (2022). *An analysis of China's cyber espionage against the United States defense industrial base* (Doctoral Dissertation). Utica University.
Larres, K. (2020). Trump's trade wars: America, China, Europe, and global disorder. *Journal of Transatlantic Studies*, *18*(1), 103–129. [CrossRef]
Lasiello, E. (2016). China's three warfares strategy mitigates fallout from cyber espionage activities. *Journal of Strategic Security*, 9(2), 45-69.
Layne, C. (2006). *The peace of illusions: American grand strategy from 1940 to the present*. Cornell University Press.
Limnéll, J. (2015). The exploitation of cyber domain as part of warfare: Russo-Ukrainian war. *International Journal of Cyber-Security and Digital Forensics*, *4*(4), 521–532. [CrossRef]
Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404. [CrossRef]
Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security*, *39*(3), 7–47. [CrossRef]
Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.) (2015). *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. Oxford University Press.
Lindsay, J. R., & Gartzke, E. (2016). Coercion through cyberspace: The stability- instability paradox revisited. In: *The Power to Hurt: Coercion in Theory and in Practice*, 176–204. (https://deterrence.ucsd.edu/_files/LindsayGartzke_CoercionThroughCyberspace_DraftPublic1.pdf)
Liu, Y., Lee, J. M., & Lee, C. (2020). The challenges and opportunities of a global health crisis: The management and business implications of COVID-19 from an Asian perspective. *Asian Business and Management*, *19*(3), 277–297. [CrossRef]
Lotrionte, C. (2014). Countering state-sponsored cyber economic espionage under international law. *North Carolina Journal of International Law and Commercial Regulation*, *40*, 443.
Lucas, G. R. (2017). *Ethics and cyber warfare: The quest for responsible security in the age of digital warfare*. Oxford University Press.
Lyon, D. (2015). *Surveillance after Snowden*. John Wiley & Sons.
Margulies, P. (2016). Surveillance by algorithm: The nsa, computerized intelligence collection, and human rights. *Florida Law Review*, *68*, 1045.
McKnight, B. E. (1992). *Law and order in Sung China*. Cambridge University Press.
Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017). Detection of unauthorized IoT devices using machine learning techniques. *arXiv preprint arXiv:1709.04647*.
Miller, C. (2022). *Chip war: The fight for the world's most critical technology*. Simon and Schuster.
Mu, Q., & Lee, K. (2005). Knowledge diffusion, market segmentation and technological catch-up: The case of the telecommunication industry in China. *Research Policy*, *34*(6), 759–783. [CrossRef]
Nasheri, H. (2023). State-sponsored economic espionage in cyberspace: Risks and preparedness. In *Cybercrime in the pandemic digital age and beyond* (pp. 87–107). Springer International Publishing.
Nathan, A. J., & Scobell, A. (2015). *China's search for security*. Columbia University Press.
Newland, S. A. (2023). Teaching Chinese politics in the "new Cold War": A survey of faculty. *PS: Political Science and Politics*, 1–8. [CrossRef]
Nye, J. S. (2010). *Cyber power* (pp. 1–24). Harvard Kennedy School, Belfer Center for Science and International Affairs.
Office of the Secretary of Defense (2007). Military power of the People's Republic of China 2007. In Annual Report to US Congress. (https://apps.dtic.mil/sti/pdfs/ADA495514.pdf)
Oguamanam, C. (2008). Local knowledge as trapped knowledge: Intellectual property, culture, power and politics. *Journal of World Intellectual Property*, *11*(1), 29–57. [CrossRef]
Olszak, C. M., Ziemba, E., & Koohang, A. (2006). Business intelligence systems in the holistic infrastructure development supporting decision-making in organisations. *Interdisciplinary Journal of Information, Knowledge, and Management*, *1*, 47–58. [CrossRef]
Peng, M. W., Ahlstrom, D., Carraher, S. M., & Shi, W. S. (2017). History and the debate over intellectual property. *Management and Organization Review*, *13*(1), 15–38. [CrossRef]
Pillsbury, M. (2015). *The hundred-year marathon: China's secret strategy to replace America as the global superpower*. Henry Holt and Company.
Rogoff, B. (2003). *The cultural nature of human development*. Oxford University Press.
Roth, B. R. (1999). *Governmental illegitimacy in international law*. Oxford University Press.
Roper, C. (2013). *Trade secret theft, industrial espionage, and the China threat*. CRC Press.
Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counterintelligence*, *26*(3), 453–481. [CrossRef]
Scott, R. D. (1999). Territorially intrusive intelligence collection and international law. *AFLRev*, *46*, 217.
Shu Shang, C., & Shen, W. (2021). Beyond trade war: Reevaluating intellectual property bilateralism in the US–China context. *Journal of International Economic Law*, *24*(1), 53–76. [CrossRef]
Skinner, C. P. (2013). An international law response to economic cyber espionage. *Connecticut Law Review*, *46*, 1165.
Sun, T. (1994). *The art of war*. Hachette UK.
Tao, Q., & Prescott, J. E. (2000). China: Competitive intelligence practices in an emerging market environment. *Competitive Intelligence Review*, *11*(4), 65–78. [CrossRef]
Thurbon, E., & Weiss, L. (2006). Investing in openness: The evolution of FDI strategy in South Korea and Taiwan. *New Political Economy*, *11*(1), 1–22. [CrossRef]

Ulsch, M. (2014). *Cyber threat! how to manage the growing risk of cyber-attacks*. John Wiley & Sons.
United States Department of Justice (DOJ) (2021). *Jury convicts Chinese intelligence officer of espionage crimes for attempting to steal trade secrets*. https://www.justice.gov/opa/pr/jury-convicts-chinese-intelligence-officer-espionage-crimes-attempting-steal-trade-secrets
United States Department of Justice (2022). *Former Broadcom engineer sentenced to eight months in prison for theft of trade secrets*. https://www.justice.gov/usao-ndca/pr/former-broadcom-engineer-sentenced-eight-months-prison-theft-trade-secrets
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. [CrossRef]
Wang, D. (2010). China's trade relations with the US in perspective. *Journal of Current Chinese Affairs*, *39*(3), 165–210. [CrossRef]
Wangen, G. (2015). The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information*, *6*(2), 183–211. [CrossRef]
Westad, O. A. (2003). *Decisive encounters: The Chinese Civil War, 1946–1950*. Stanford University Press.
Wey, A. L. K. (2014). Principles of special operations: Learning from Sun Tzu and Frontinus. *Comparative Strategy*, *33*(2), 131–144. [CrossRef]
Wilson, C., & Drumhiller, N. (2016). US-China relations: Cyber espionage and cultural bias. In *National security and counterintelligence in the era of cyber espionage* (pp. 28–46). IGI Global. [CrossRef]
Wilson, S. (2023). *Firm capabilities, great power competition, and the structural reshaping of globalization*. Doctor of Philosophy (PhD), Dissertation, Management, Old Dominion University. (https://digitalcommons.odu.edu/businessadministration_etds/150)
Wither, J. K. (2016). Making sense of hybrid warfare. *Connections: The Quarterly Journal*, *15*(2), 73–87. [CrossRef]
Witzel, M. (2016). *Doing business in China*. Routledge.
Wu, X. (2020). Technology, power, and uncontrolled great power strategic competition between China and the US. *China International Strategy Review*, *2*(1), 99–119. [CrossRef]
Wübbeke, J., Meissner, M., Zenglein, M. J., Ives, J., & Conrad, B. (2016). Made in china 2025. *Mercator Institute for China Studies. Papers on China*, *2*(74), 4.
Zheng, Y. (1999). *Discovering Chinese nationalism in China: Modernization, identity, and international relations*. Cambridge University Press.