Cybersecurity and Economic Espionage: The Case of Chinese Investments in the Middle East

Sharon Magen

The utilization of emerging technologies for purposes of cyber espionage is the cornerstone of this paper. Although many have referred to cyber security risks that are directly connected to the security sphere, national security threats due to economic cyber espionage have not been dealt with to the same extent, and this oversight is rather puzzling. As cyberspace becomes increasingly utilized for espionage purposes, it is imperative to further examine the possibility of exploiting cyberspace for the purpose of espionage specifically in the international arena; economic globalization has made the international economic scene vastly interconnected, thus intensifying the vulnerability of the world economy to possible cyber security breaches.

Keywords: Cyber espionage, economic espionage, globalization, national security

Introduction

The recent usage of emerging technologies for the purposes of cyberattacks or acts of cyber espionage in general and the subsequent threat specifically posed to the national security interests of governments in the economic sphere is the focus of this paper. Although many have examined cybersecurity

Sharon Magen holds a Master's degree in Security Studies from Tel Aviv University and completed her internship at the Institute for National Security Studies (INSS) on China-Israel relations and the Gulf Cooperation Council (GCC).

risks that are directly connected to the security sphere, national security threats posed by cyberattacks or acts of cyber espionage in the economic sphere have not been dealt with to the same extent, and this lack of interest is rather puzzling.

As cyberspace is increasingly being utilized for espionage purposes in various fields, it is imperative to further examine the possibility of exploiting cyberspace specifically for the purpose of espionage in the international economic arena; globalization has made the international economy vastly interconnected, thus making the world economy more vulnerable to possible cybersecurity breaches, with such a breach rendering the possible repercussions on national security interests even more intense and on a much wider scale. This lack of contemporary research on the utilization of cyber means for conducting economic espionage and the subsequent consequences regarding national security has compelled me to examine this subject in this paper.

The growing importance of this phenomenon, in which foreign entities may utilize cyber means for carrying out economic espionage to achieve strategic goals, is the incentive for this research. The growing risk posed to national security by economic cyber espionage, coupled specifically with the economic and political rise of China, rather intensifies the importance of dealing with this issue. As a country seeking to become a game-changer in the global arena, it is highly likely that China—significantly more than other countries—fully engages in cyber espionage in the economic sphere so that it can achieve its goals in other fields, such as in the security and political spheres. This issue should be further studied, in order to determine whether cyber espionage in the economic sphere is a threat posed especially by China, and whether this threat should therefore be taken into consideration when considering integration with Chinese entities.

In this case, foreign governments, through private or state-owned companies, can target certain economies or foreign companies for making an investment. The government will then be able to obtain new technologies—an act that may tip the scale in favor of the investing country, which otherwise would not have been able to receive these technologies.

This phenomenon cements cyber espionage in the economic arena now as an undeniable threat to national security. The United States mostly directs this accusation against China, as Chinese companies, which are mostly state-owned, are suspected of utilizing global cyber and economic integration as

a vessel for conducting economic espionage; however, some contend that China is not the only country committing cyber espionage in the economic sector and therefore should not be targeted as such.

All countries today engage in cyber economic espionage to a certain degree; therefore, this paper will question the reason why the United States is spearheading the notion that China conducts gross economic espionage, even though it is maintained that other countries do so as well.

My methodology for examining this theoretical assumption entails the assessment of other countries' approaches toward China's supposed cyber economic espionage intentions. If other countries similarly claim that China is the main source of global cyber economic espionage, even though it has been asserted that other countries take part in such espionage acts as well, it would be vital to clarify the reasons for this type of behavior. In order to assess the attitudes of other countries toward China's cyber economic espionage, I contend that it would be most effective to focus on non-western countries, such as the Middle Eastern countries, which may contribute to a more balanced portrayal of other countries' attitudes toward China's cyber economic espionage intentions.

Consequently, in this paper I examine the approach of select Middle Eastern countries toward China's massive involvement in world trade and the possibility of its gross cyber economic espionage activities as a means of assessing the veracity of Washington's claim. Specifically, I examine the cases of the United Arab Emirates (UAE) and Turkey. The rationalization for choosing these two countries is such; the main nexus that binds Beijing to the Middle East region concerns economic security, as more than half of China's oil and natural gas imports are sourced from the countries of the region.

Regarding the UAE, it is important to note that it is only the third largest economy in the Middle East behind Saudi Arabia and Iran. Being a source of oil and natural gas imports for China but not one of China's principal suppliers, the UAE represents a significant case study in this sense as it cannot be characterized as being overly essential to Chinese interests. Therefore, the UAE's approach to Chinese cyber espionage intentions will not be tilted in favor of Beijing.

In contrast to most other actors in the region, hydrocarbons do not play a big role in Turkey's relations with China, thus making Ankara a meaningful choice for a study of relations with China within the Middle Eastern context.

If so, an outtake on the Turkish possible responses to Chinese alleged cyber economic espionage may provide an original contribution on investigating this matter.

The apprehension that through cyber economic espionage China could access key economic interests in a host country's economy and realize its own interests, regardless of the host country's interests, could propel the UAE and Turkey into taking action against Chinese economic transactions, thus initiating the suspension or cancelation of Chinese-backed investments and so on. In order to measure the approach of the governments of these two countries to possible Chinese cyber economic espionage, I will examine possible objections and restrictions made at a government level toward Chinese economic transactions and Chinese-funded projects within the two countries. Upon presenting a consistent trend of government level objections to projects funded by the Chinese, I contend that this is due to the tangible threat to national security posed by cyber economic espionage, and enabled by economic integration.

This research underlines the imperativeness of the need for further study of global cyber integration and the risks that economic espionage entails. Although global cyber integration may present an opportunity for growth, countries must take into consideration the risk of exposing their economy to cyber economic espionage.

Research on Economic Espionage Using Cyber

According to Mary Ellen Stanley, technological advancements and economic integration have vastly altered the perception of national security in the intelligence sphere, due to wide-ranging cyber economic espionage.[1] Similarly, Matthew Crosston argues that typical international economic activity may constitute an intelligence collecting structure by cyber means, designed to enhance military might.[2] Souvik Saha specifically stresses the US standpoint, which is concerned about the Chinese involvement in economic espionage,

1 Mary Ellen Stanley, "From China with Love: Espionage in the Age of Foreign Investment," *Brooklyn Journal of International Law* 40, no. 3 (2015): 1033–1079.

2 Matthew Crosston, "Soft Spying: Leveraging Globalization as Proxy Military Rivalry," *International Journal of Intelligence and Counterintelligence* 28, no. 1 (2015): 105–122.

and the undeniable national security threat it poses.[3] Furthermore, Magnus Hjortdal emphasizes that cyberspace is a pivotal element in China's strategy to ascend in the international system, and that one of the key means is by conducting economic espionage to gain strategic advantage.[4]

However, İbrahim Erdoğan argues that cyber economic espionage is an immensely lucrative industry in which all countries participate,[5] and therefore cannot be attributed to one specific country. Furthermore, when it comes specifically to the United States, Duncan Clarke contends that even allies of Washington, such as Israel, have been committing acts of economic espionage against the United States for years. According to Clarke, Israeli intelligence units continue to utilize existing networks for collecting economic intelligence, including computer intrusion,[6] thus rendering redundant the argument that cyber economic espionage against the United States is an act of war spearheaded by its foes. The assertion that many other countries in addition to China commit cyber economic espionage against Washington—including its allies who are not reprimanded—weakens the severity of China's acts and the argument of the US intelligence community that China is indeed at the forefront of cyber economic espionage.

Regarding the integrity of the assessments of the American intelligence agencies, John Yoo contends that US intelligence and national security agencies do not always depict an accurate portrayal of national security threats.[7] In other words, the United States may employ false claims to protect the nation's security, thus arguably sacrificing the integrity of the government's efforts. Robert Bejesky similarly throws into question the reliability of these organizations' assertions; according to Bejesky, allegations that the executive branch may induce intelligence assessments to support the position preferred by the executive branch are not without basis. The Central Intelligence

3 Souvik Saha, "CFIUS Now Made in China: Dueling National Security Review Frameworks as a Countermeasure to Economic Espionage in the Age of Globalization," *Northwestern Journal of International Law and Business* 33, no. 1 (2012): 199–235.

4 Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (2011): 1–24.

5 İbrahim Erdoğan, "Economic Espionage as a New Form of War in the Post- Cold War Period," *USAK Yearbook of International Politics and Law* no. 2 (2009): 265–282.

6 Duncan Clarke, "Israel's Economic Espionage in the United States," *Journal of Palestine Studies* 27, no. 4 (1998): 20–35.

7 John Yoo, "The Legality of the National Security Agency's Bulk Data Surveillance Programs," *Harvard Journal of Law and Public Policy* 37, no. 3 (2014): 901–930.

Agency (CIA), for instance, has a long history of politicizing intelligence; at a conference at Harvard in 2001, a panel of experts deliberating the account of the CIA maintained that the agency does not conduct its role faithfully when it comes to sharing unpleasant truths with the executive branch.[8]

If so, it is feasible to comprehend that even though cyber economic espionage may pose a national security threat, the formal accusation by the United States that China is the main perpetrator of cyber economic espionage may be biased. Although China may be committing acts of economic espionage by using cyber means, it cannot be confirmed at this point that it spearheads this area more than any other country.

Growing Interconnectedness

During the past few decades, technological developments have immensely changed the way that governments perceive national security. Conventional acts of espionage, which can be traced to a certain perceptible entity, have merged significantly with cybersecurity, thus rendering ambiguous the identity of the intelligence threat and exposing new domains in which harmful data collection may occur, such as the global marketplace.[9] Today, the world is moving toward a single global economy, due to financial integration.[10] This current reality of cutting-edge technology and worldwide economic integration has changed the face of espionage and has created a world in which national security can be harmed, inter alia, via cyber means in the global marketplace.

Today there is a need to balance a nation's economic affluence and its national security, as economic globalization may become a vessel for espionage through cyber means—the bedrock of connectivity in today's international market. The key methods through which international economic integration may enable cyber economic espionage are when a foreign, state-owned or government body conducts business in the host country, or when a foreign entity acquires a local business within the country.[11] It can be contended that

8 Robert Bejesky, "Politicization of Intelligence," *Southern University Law Review* no. 40 (2013): 243–292.

9 Stanley, "From China with Love: Espionage in the Age of Foreign Investment."

10 Lucyna Kornecki and Dawna Rhoades, "How FDI Facilitates the Globalization Process and Stimulates Economic Growth in CEE," *Journal of International Business Research* 6, no. 1 (2007): 113–126.

11 Stanley, "From China with Love: Espionage in the Age of Foreign Investment."

this type of activity is not merely a manifestation of economic policy but also functions as a well-planned intelligence collecting scheme intended to serve as an additional form of competition, in addition to military rivalry.[12] Although it cannot be affirmed that cyber espionage is the main incentive for pursuing economic integration, economic integration makes it possible to conduct cyber espionage activities. Countries may even abuse economic integration in order to conduct cyber economic espionage so that they can enhance their military might.

In this regard, many have claimed that China is leading the sphere of cyber economic espionage.[13] According to this approach, China intends to harness the possibilities of espionage offered by today's worldwide market as a means of enhancing its regional and global supremacy. Washington especially perceives Beijing's intention to commit economic espionage through cyberspace as a dire national security hazard, as China's success in conducting effective economic espionage may translate into a sharp increase in China's potential power relative to the United States. China's current investment policy in economies such as the United States consists of mergers and acquisitions, which enable opportunities for undesirable proliferation of intellectual property and trade secrets to Chinese firms via cyber means.[14]

This type of activity is particularly problematic when Chinese multinational corporations, which are mostly government owned, attempt to purchase American companies with strategic significance or which deal with critical infrastructure and assets. According to recent assessments from the US intelligence community, there is a heightened assertiveness within China's international policies, and as a result, it has resorted to massive cyber economic espionage.[15] Moreover, according to Pentagon reports, China will

12 Crosston, "Soft Spying: Leveraging Globalization as Proxy Military Rivalry."

13 Stuart Malawer, "Confronting Chinese Economic Cyber Espionage with WTO Litigation," *New York Law Journal*, December 23, 2014.

14 "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," *The Office of the National Counterintelligence Executive*, April 14, 2016, https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; Saha, "CFIUS Now made in China: Dueling National Security Review Frameworks as a Countermeasure."

15 Saha, "CFIUS Now made in China: Dueling National Security Review Frameworks as a Countermeasure."

continue to aggressively collect sensitive American technological information through cyber espionage.[16]

This assertion that China is the main global source of cyber economic espionage may also serve certain US political policies, rather than represent an accurate status of global cyber economic espionage. Although James Comey, the director of the FBI, had stated in May 2014 that the Chinese government blatantly sought to use cyber espionage to obtain an economic advantage for its state-owned industries, Robert Gates, then former US secretary of defense, openly stated that as many as fifteen countries at that time were conducting economic espionage in order to take possession of American trade secrets and technology,[17] thus shifting the focus from China as the leading perpetrator of this act. Furthermore, it has been contended that the US National Security Agency itself had committed cyber economic espionage activities against France.[18]

Given the circumstances, the main question that arises is why the majority of official American security and intelligence bodies spearhead the notion that China is currently the worldwide source of cyber economic espionage while other sources maintain that other countries have committed cyber economic espionage acts as well, including the United States itself. Although China does not actually lead the global cyber economic espionage, top security and intelligence institutions in the United States promote this claim in order to support the US political needs and policies toward China, whose growing regional and world ascendancy threatens the continuation of Washington's world dominance and strategic might. In other words, China's rise poses a political threat to the United States, a fact which has led to American prosecution of Chinese economic interests.

Another question is whether other countries similarly argue that China is at the global forefront of cyber economic espionage. If other countries equally claim that China is indeed the global leader of cyber economic espionage, then what are the reasons supporting this argument? If other countries contend

16 Geoff Dyer, "China in 'Economic Espionage'," *Financial Times*, May 19, 2012.

17 Zachary Keck, "Robert Gates: Most Countries Conduct Economic Espionage," *The Diplomat*, December 17, 2015, http://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/.

18 "WikiLeaks Reveals NSA's Economic Espionage against France," *Progressive Digital Media Technology News*, Jun 30, 2015, http://search.proquest.com/docview/1692699265?accountid=14765.

that China is the world leader of cyber economic espionage, even though many other countries in fact engage in cyber economic spying, then why do they make this claim? It is my assumption that this is due to security motives, related to China's economic rise and the security threat China poses via its economic growth. This would assist in asserting the assumption that China's rise de facto poses a threat to American strategic interests.

Therefore, it can be argued that the majority of official American security and intelligence bodies do not portray an accurate assessment of the case of global cyber economic espionage as other global actors also engage in cyber economic espionage and no single country spearheads it. However, I contend that the *formal approach* of most of the American intelligence institutions toward China in the cyber economic espionage sphere may be intended to serve the US grand strategy toward China's rise, in the belief that China's growth may threaten American strategic interests.

The hypothesis that the United States has advanced the global notion that China leads in international cyber economic espionage due to political, foreign policy, and security reasons can help clarify the gap between the popular claim within the American intelligence community and other entities regarding China's role in cyber economic espionage. Many contend that China's vast economic growth coupled with its enhancing military capabilities has placed it on a collision course with the United States.[19] As a way of challenging China's rise, the United States has depicted China as having minimal respect for intellectual property, sovereignty, and other critical factors that comprise the bedrock of global trade. International trade serves as China's bread and butter, fueling its growth and ability to expand its military capabilities. If the United States can damage China's ability to conduct global trade by asserting that it promotes cyber economic espionage, it would thus damage Beijing's capabilities in the security sphere.

To better understand the reasons why the United States claims that China leads the global cyber economic espionage, we will now look to the UAE and Turkey to see how they relate to China's massive involvement in world trade and the possibility of its gross cyber economic espionage activities, in order to assess the veracity of Washington's claim.

19 Saha, "CFIUS Now made in China: Dueling National Security Review Frameworks as a Countermeasure."

UAE

The UAE is a federation comprised of seven separate emirates, which together represent the third largest economy in the Middle East behind Saudi Arabia and Iran. The UAE has the seventh largest proven reserves in the world of both oil and gas, and in 2010 China imported 64,500 tons of liquefied natural gas from the UAE valued at more than 23 million dollars. Furthermore, the China Petroleum Engineering and Construction Corporation (CPECC) assisted with the construction of the Abu Dhabi Crude Oil Pipeline Project, which now enables the transport of 1.5 million barrels of crude oil per day from Abu Dhabi's collection point at Habshan to the export terminals at Fujairah. Oil transported through the pipeline bypasses the narrow Strait of Hormuz, which Iran repeatedly has threatened to block if it is attacked militarily. However, it is imperative to point out that the 3.3-billion-dollar project had experienced repeated delays, initiated by the UAE.[20]

Although it had been officially stated that construction problems forced the UAE to delay constructing the pipeline,[21] industry sources close to the project claimed another reason for the delay. Although the CPECC was already preparing to commission the pipeline, the Abu Dhabi Company for Onshore Petroleum Operations (ADCO) was not involved in this initial preparation process, a rather perplexing situation, as it would be expected that ADCO would first have to ensure that the commissioned pipeline design suited its standards prior to commencing production.[22]

The fact that the Chinese began designing the pipeline without the participation and involvement of ADCO—the UAE state firm in charge of the project—conceivably indicates that the Chinese intended to commit a sinister act regarding the construction of the pipes; such pipelines include highly sophisticated control software that can be hacked and even manipulated prior to its assembling. In 2004, for instance, Thomas C. Reed, a US Air Force secretary in the Reagan administration, wrote that the United States had effectively implanted a software trojan horse into computing equipment

20 Manochehr Dorraj and James English, "The Dragon Nests: China's Energy Engagement of the Middle East," *China Report* 49, no. 1 (2013): 43–67.

21 "UAE Delays Project to Bypass the Strait of Hormuz," *Al Bawaba*, January 9, 2012, http://www.albawaba.com/business/uae-delays-project-bypass-strait-hormuz-408210.

22 "UAE Delays Oil Pipeline to Bypass Hormuz to June," *Oil & Gas News*, January 16, 2012, http://search.proquest.com/docview/916274658?accountid=14765.

that the Soviet Union had bought from Canadian suppliers, which was used to control the Trans-Siberian gas pipeline.[23]

If so, it is quite plausible that the Chinese had begun the UAE-commissioned pipeline design without involving ADCO because they had something to hide, such as installing cyber espionage measures. This would not be an isolated incident for the Chinese; in 2013, Michael Hayden, the former head of the CIA, contended that the Chinese telecom giant Huawei was spying for Beijing,[24] which rather solidifies the argument that China indeed utilizes business transactions for conducting cyber espionage. In the case of the Abu Dhabi Crude Oil Pipeline Project, the numerous delays due to the ongoing exclusion of ADCO from the pipeline design process can be explained by the fact that CPECC had engaged in illicit activities during the manufacturing of the pipeline, namely the insertion of cyber espionage measures; however, in this case, even though China had engaged in cyber economic espionage, the UAE only delayed the project and did not opt to cancel it entirely.

Turkey

Although more than half of China's oil and natural gas imports are sourced from the countries of the Middle East region, thus deepening Beijing's dependence on the region, hydrocarbons do not play a pivotal role in Turkey's relations with China. Nonetheless, Turkey is a rising power in the region and has not directly experienced upheavals like the ones that were felt in the Arab world in the past few years; thus, Ankara is still one of Beijing's pivotal partners in the region, in the economic and political spheres alike.[25] Regarding the Turkish government's stance on possible Chinese cyber economic espionage activities, it is important to note that in November 2015, Ankara canceled

23 John Markoff, "Old Trick Threatens the Newest Weapons," *New York Times*, October 26, 2009, http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&ref=science&pagewanted=all.

24 "Huawei Spies for China, says Former NSA and CIA Chief Michael Hayden," *Business Insider*, July 19, 2013, http://www.businessinsider.com/huawei-spies-for-china-says-michael-hayden-2013-7.

25 Altay Atli, "A View from Ankara: Turkey's Relations with China in a Changing Middle East," *Mediterranean Quarterly* 26, no. 1 (2015): 117–136.

a tender of 3.4 billion dollars for a long-range missile defense system, provisionally awarded to a Chinese state-owned firm in 2013.[26]

Turkey had originally entered negotiations in 2013 with the China Precision Machinery Import-Export Corporation (CPMIEC) to finalize the billion-dollar contract. Even though the French-Italian consortium Eurosam and the American-listed Raytheon had also submitted offers, the Turkish government preferred talks with the Chinese company, which raised serious concerns over the compatibility of CPMIEC's systems with NATO's missile defenses, of which Turkey is a member. In its official statement given by a representative from the office of then prime minister Ahmet Davutoğlu, the Turkish government declared that it had canceled the deal with China mainly because Turkey had decided to launch its own missile project.[27]

Although the Turkish government officially maintained that the core reason for canceling the multibillion-dollar deal with the Chinese firm had been its decision to develop by itself the long-range missile defense system, concrete concerns within the Turkish government about Chinese cyber economic espionage may have led to the cancelation. As previously stated, Turkey had implemented a comprehensive process for choosing a foreign company to lead this project. If Turkey had indeed wished to self-develop this defense system, it would have done so from the beginning and would not have conducted a complete procedure for choosing a foreign firm to conduct this project.

In other words, it can be argued that after Turkey had decided to continue with CPMIEC in order to further this project, the Turkish government began to express serious concerns regarding possible exposure of sensitive NATO systems to the Chinese. Although the deal did not explicitly address the direct exposure of critical and classified systems to the Chinese, this transaction could have enabled Chinese access to systems through which harmful data collection could be conducted. Transactions such as this may inadvertently enable foreign penetration via cyber means, as foreign firms gain access and exposure to computerized systems through which such infiltration may be

26 "Turkey Says 'yes' to China's Trade Initiative, 'no' to its Missiles," *South China Morning Post*, November 15, 2015, http://www.scmp.com/news/china/diplomacy-defence/article/1879097/turkey-says-yes-chinas-trade-initiative-no-its-missiles.

27 "Turkey Cancels $3.4 Bln Missile Deal with China," *French Chamber of Commerce and Industry in China*, November, 15 2015, http://www.ccifc.org/fr/single-news/n/turkey-cancels-34-bln-missile-deal-with-china/.

conducted. Such harmful data collecting activities through cyber means—enabled by seemingly innocent business transactions—are especially perilous when these transactions involve critical infrastructure of the host country.

Although it can be argued that other motives caused the Turkish government to call-off the collaboration with the Chinese state-owned firm, such as the formal Turkish response that Turkey had decided to develop the long-range missile defense system itself, this argument, as stated, is problematic to comprehend as Turkey had already initiated a long process of selecting a foreign contractor. If so, it can be claimed that the Chinese cyber economic espionage threat was a pivotal motive in Turkey's decision to call off the deal, as it is perceived as a real danger by the Turkish government to its national security.

It is apparent that while the UAE and Turkey do not share Washington's vehement concern for the threat of Chinese cyber economic espionage, they do understand the possibility of a threat, as reflected by canceling or delaying business transactions with Chinese firms. Although neither of these countries have exclaimed—as the Americans have—that China uses cyber means as a means of carrying out economic espionage, their behavior toward major Chinese investments indicates that they understand, at least at the government level, that China's economic conduct differs from that of other countries and poses a heightened threat of cyber economic espionage.

The UAE and Turkey are not engaged in great power politics that characterize the United States and therefore lack the incentive as well as the protective means to denounce China's economic conduct. Although there is some government-level resistance to major business transactions with Chinese firms, it mainly occurs through inconspicuous "soft" methods such as project suspension; however, project suspension, coupled with cancelation of business transactions with Chinese firms, forms a stable foundation for the argument that Chinese business transactions specifically are not treated the same as transactions done with firms from other countries, therefore indicating that they pose a threat.

Nonetheless, given that the anti-China steps within the economic sphere are mostly discreet, it is speculative to assume that they are taken in light of China's intentions to engage in cyber economic espionage. Even when these two governments publicly announced the suspension or cancelation of Chinese-funded projects, they did not state that this was due to misconduct

rooted in cyber economic espionage. The indication that Chinese economic conduct is treated differently than economic transactions originating from other countries may also further solidify the American claim that China's economic behavior is not innocent; if the governments of Turkey and the UAE believed that China was innocent, they would not publicly announce the suspension or cancelation of major Chinese-funded projects in both countries.

In the literature review section of this paper, I noted Crosston's approach, who states that typical types of international economic activity may constitute an intelligence-collecting structure, designed to enhance military might. Additionally, according to Saha, recent assessments from the US intelligence community contend that China's international policies reflect an intensified decisiveness, and as part of this, China has resorted to substantial cyber economic espionage. The focus of China's business transactions and economic integration in the infrastructure, energy, and telecommunication sectors—all critical to national security—may indeed suggest that the Chinese intend to utilize cyber means for gaining information for their own strategic purposes. The suspension and cancelation of key Chinese-funded projects, prima facie due to technical reasons, suggest that these governments see further Chinese economic involvement in their countries as a threat.

Conclusion

In conclusion, it is possible to comprehend how global cyber interconnectedness and economic integration have affected a country's perception of its national security. While pertaining to be of economic nature only, typical international economic activities may constitute an intelligence-collecting structure, done through cyber means, and intended to aid in enhancing a nation's power. International economic conduct may facilitate opportunities for the proliferation of economic intelligence transmitted to the investing country via cyber espionage, thus compromising the national security of the country that receives the investments. The American claim that China currently spearheads cyber economic espionage worldwide through economic integration has been substantiated by other governments as well, in addition to the reaction of the governments of Turkey and the UAE to business transactions with Chinese firms. Although these countries' reaction is not as intense and straightforward as that of the American government, it is nevertheless apparent that they are striving to restrict or monitor Chinese investments, at the very least.

This research sought to answer why official American intelligence bodies claim that China is currently the main perpetrator of cyber economic espionage, even though other sources maintain that additional countries also commit economic espionage. Given the findings regarding the UAE and Turkey, it can be contended that the United States makes this claim because Chinese investments are perceived as a national security threat, a notion shared by other countries. As seen in the cases of Turkey and the UAE, the delay or suspension of Chinese projects point to the fact that business transactions with Chinese firms are indeed looked upon by these countries—and not only by the United States—as a source of peril, even though it could be said that China is no different than any other country when it comes to economic integration and cyber economic espionage.

This research has contributed to the further study of cyber interconnectedness, alongside economic integration and the espionage risk it entails. Even though the global market place has become increasingly interconnected via cyber means, countries must take into consideration the risk of exposing their country to national security risks, given that international economic integration may prove to be a vessel for cyber economic espionage. Indeed, the United States is not exaggerating when it describes the cyber economic espionage intentions of the Chinese; rather, as a superpower, it is one of the few countries that have the prerogative to openly state its opinion on the matter. It is therefore critical to assess Chinese business transactions differently than those from other countries, given the fact that the Chinese specifically use economic integration for conducting cyber espionage and enhancing Beijing's military and strategic might along the path in its rise.

As further research, I suggest monitoring the response of other powerhouses, such as the European Union and Russia, to China's cyber economic espionage acts, since the notion of China as the global leader of cyber economic espionage prevails within countries other than the United States. In the case of Russia, for instance, it is possible that the Russian government will not publicly support the claim regarding Chinese cyber economic espionage acts in order to solidify the Chinese position vis-à-vis that of the United States. However, the Russian government may also elect to use covert measures, thus protecting itself from the vast cyber economic espionage threat posed by China but in a discreet way, which neither harms its relations with Beijing nor supports the US agenda.

If the other great powers besides the United States perceive China's cyber economic espionage as a central threat to their national security, it would be vital to determine how this would affect world politics and trade. Although some of the great powers today use subtle measures to counter Chinese cyber economic espionage, in the future, as China continues to rise economically and militarily, these countries will have to join forces in order to contain China. To put an end to Chinese cyber economic espionage, the great powers may have to erect international cyber monitoring structures in the economic sphere as a means of decreasing the possibility of international cyber economic espionage.