Group of Twenty

Preventing corporate espionage

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Vidhi Khakhar

Forum	The Group of Twenty (G20)
Issue:	The question of preventing corporate espionage
Student Officer:	Vidhi Khakhar
Position:	President of G20.

Introduction

As the global economy becomes increasingly competitive and technological advancements continue to drive innovation and globalization, the risk of corporate espionage has intensified, posing significant threats to businesses, economies, and national security. In 1999, a reported 1,000 companies lost more than $45 billion from the theft of trade secrets, according to a survey by the American Society for Industrial Security and Price Waterhouse Coopers. Today, theft of trade secrets is estimated to be around $100 billion. The European Centre for International Political Economy (ECIPE), a Brussels-based think tank, describes in its latest report on cybercrime an economic impact caused by cyber theft of €60 billion loss in economic growth in the EU and a consequential potential loss of 289,000 jobs. The implications of corporate espionage are far-reaching and detrimental to businesses, economies, and international trade.

Companies invest substantial resources in research and development, creating innovative products and services that drive economic growth. When these proprietary assets are stolen or compromised, businesses face severe financial losses, diminished market share, and diminished trust among customers and partners. Corporate espionage undermines trust, distorts market competition, and hinders innovation, ultimately leading to economic losses for targeted companies and potential job cuts. It involves a range of illicit activities, including hacking, insider threats, industrial espionage, and the recruitment of insiders or third parties to gather sensitive information.

The G20, comprising the world's major economies, plays a crucial role in shaping global policies that promote economic growth, financial stability, and sustainable development. Addressing the issue of preventing corporate espionage within the G20 framework is imperative to safeguarding the interests of member nations and fostering a fair and transparent global business environment in order to continue innovation.

Definition of Key Terms

Corporate Espionage:

The covert and unauthorized acquisition of confidential information, trade secrets, or intellectual property from one company by another, with the intention to gain a competitive advantage or harm the targeted company's interests.

Economic Espionage:

Economic espionage involves the unauthorized acquisition of trade secrets or confidential business information acquired to benefit any foreign governments, instrumentalities, agents, or entities for economic or commercial advantage. It often targets industries or companies with strategic importance or advanced technologies.

Industrial Espionage:

Industrial espionage is the unlawful acquisition of trade secrets, proprietary information, or intellectual property from one company by another within the same industry or sector. It aims to gain a competitive advantage

Cyber Espionage:

The use of digital technologies and hacking techniques to infiltrate computer networks and steal sensitive information, including trade secrets and intellectual property.

Intellectual Property Rights (IPR):

Legally granted rights that protect intangible creations of the human mind, such as inventions, trademarks, copyrights, and trade secrets.

Trade Secrets:

Trade secrets refer to confidential and proprietary information that provides a competitive advantage to a company. These can include formulas, manufacturing processes, customer lists, marketing strategies, and other valuable business information that is not publicly known.

Insider Threat:

Insider threat refers to the risk posed by individuals within an organization who have authorized access to sensitive information but misuse or disclose it for personal gain or malicious purposes. This can include employees, contractors, or business partners.

Counterintelligence:

Counterintelligence involves the activities and measures taken by organizations, such as intelligence agencies or security services, to detect, prevent, and neutralize espionage threats, including corporate espionage. It focuses on gathering intelligence on adversaries and protecting sensitive information.

Insiders:

Refers to individuals who have authorized access to sensitive information within an organization. In the context of corporate espionage, insiders can be employees, contractors, or partners who exploit their privileged position to steal or leak valuable intellectual property.

Outsiders:

Refers to individuals or entities external to an organization who engage in corporate espionage activities. Outsiders may employ various tactics such as hacking, social engineering, or physical infiltration to gain unauthorized access to confidential information.

Kites:

In the context of corporate espionage, "kites" refers to intermediaries or intermediating companies that are used to conceal the true identity of the perpetrators. They act as a middleman, facilitating the transfer of stolen information between the insider and the outsider without directly linking them.

General Overview:

Corporate espionage has a long history that dates back to the cold war when spies were employed to gather intelligence on rivals and competitors. However, with the advent of modern technology and globalization, the methods and impact of corporate espionage have become more sophisticated and widespread. In recent decades, advancements in information technology, telecommunications, and cyber capabilities have greatly facilitated the unauthorized acquisition of sensitive business information.

Corporate Espionage- Who commits it?

"Insiders"

Insiders are usually employees: executives, IT personnel, contractors, engineers, or janitors who have legitimate reasons to access facilities, data, computers or networks. Insiders **that have immediate access to enormous amounts of valuable company information and can misuse their privileges** or impersonate someone else with higher privileges to plant a Trojan, copy information, or to taint research data.

Motives:
The basic reasons for insiders to "sell out" to competition are: lack of loyalty, disgruntled, boredom, mischievousness, blackmail, and most importantly, money.

"Outsiders"

Outsiders are spies, attackers, or hackers who enter from outside a company. Usually for competive advantage. Outsiders can enter from the Internet, dial-up lines, physical break-ins, or from partner (vendor, customer, or reseller) networks that are linked to another company's network. **They can either be a competitor itself or a hired contracter.**

Hired contracter are also known as "Kites". A kite also provides plausible deniability to his or her clients. If a covert operation is discovered and there is litigation or a criminal charge, the hiring company can deny all responsibility by denying all knowledge of the kite's actions, like cutting the string to a kite and letting it fly away by itself. Basically saying that the company had "no idea" what the consultant was doing.

An explanation of who carries out the crime of espionage.

The Problem:

The problem of modern-day corporate espionage arises from the intense competition between companies seeking to gain a competitive edge in the global marketplace. Businesses invest significant resources in research and development, innovation, and the creation of intellectual property. However, when these valuable assets are stolen through espionage, it not only undermines the efforts of the victimized company but also poses a threat to national security and economic stability. The consequences of corporate espionage can be severe, ranging from financial losses for victimized companies to compromised national security. Stolen intellectual property can be used to develop competing products, erode market share, or undermine the viability of targeted industries. Furthermore, corporate espionage undermines trust among businesses, disrupts international trade relations, and hampers innovation and technological progress.

Despite the prevalence of corporate espionage, it is often underreported due to various factors stemming from the concerns and priorities of the companies and organizations involved. One key reason for the lack of reporting is the fear of negative consequences that may arise from acknowledging a security breach.

Companies, particularly publicly traded ones, are apprehensive about notifying local authorities or disclosing incidents of corporate espionage publicly. The primary concern is the potential negative impact on their stock prices, investor confidence, and overall reputation. Publicly revealing a security breach could lead to a loss of investor trust, resulting in a decline in stock value and potential financial repercussions for the company. Financial institutions, such as banks, are notorious for their reluctance to report computer or network security breaches. They often fear that involving federal government agencies may lead to increased scrutiny of their systems, policies, and practices. The confidentiality of customer information and maintaining the public's trust in the institution are paramount for banks, and the potential consequences of reporting espionage incidents may outweigh the perceived benefits of disclosure. Similarly, small businesses, which often rely heavily on trade partnerships, may choose not to report incidents of corporate espionage for fear that their trade partners will not do business with them if they find out that their partner's systems are not secure. They fear that if their partners discover their systems' vulnerabilities, it may undermine trust and lead to a loss of business opportunities. Because ultimately, in the corporate field, a government or business' reputation is everything to the public.

The current situation:

The current situation regarding corporate espionage is characterized by an increasing number of incidents and the utilization of advanced technological methods. Due to Rapid globalisation, increased mobility, advancements in technology and the anonymous nature of the Internet, traditional espionage tactics, such as human intelligence gathering and physical theft, have been supplemented by cyber espionage, hacking, and social engineering techniques. Perpetrators employ a variety of tactics, including phishing attacks, malware infections, spear-phishing, ransomware, and

the exploitation of software vulnerabilities. These techniques are constantly evolving, as hackers continuously adapt to security measures and develop new ways to breach networks.

According to the European Commission, this is largely due to:

- Lack of awareness and competencies within businesses;
- Wider online exposure of companies, which are also moving to cloud platforms;
- The growing speed with which hackers create new malware and develop their skills in using advanced technological tools;
- Slow pace at which policymakers address the problem;
- Increase in the globalisation of markets;
- Global changes in geopolitical strategies;
- The development of new technologies, such as artificial intelligence.

Major Parties Involved

The United States of America (USA)

As one of the world's largest economies and a leader in technological advancements, the United States is heavily invested in combating corporate espionage. It has implemented legislation, such as the Economic Espionage Act, to prosecute offenders and protect trade secrets. The (FBI) continuously monitors and speaks out against corporate espionage as well as raises awareness through its website.

Furthermore, the USA plays a critical role in shaping global norms and policies related to cybersecurity and intellectual property rights. Through its participation in international forums, such as the United Nations and the World Trade Organization, the USA actively engages in discussions and negotiations on issues pertaining to corporate espionage. Its involvement and influence in these platforms make it a significant player in international efforts to combat cyber threats and enhance protection against corporate espionage.

China

China is one of the world's largest economies and a global leader in manufacturing, technology, and innovation. The country's rapid economic growth and development have resulted in a substantial demand for intellectual property and advanced technologies. However, there have been persistent allegations and concerns about state-sponsored corporate espionage and intellectual property theft originating from China.

China's strategic focus on achieving technological advancements and economic competitiveness has led to instances where companies and entities, both foreign and domestic, have been accused of engaging in illicit activities to obtain proprietary information and trade secrets. These allegations range from cyberattacks targeting foreign businesses to the use of non-traditional intelligence-gathering methods for economic and technological advantages.

The Chinese government has taken steps to improve intellectual property protection and has faced scrutiny and pressure from other countries to address the issue.

Germany

Between 2015 and 2017, the analysis reveals that German companies were most affected by corporate espionage with 17% of them declaring sensitive data stolen. Since then, Germany has vested interest in protecting its national security, economic interests, and the competitiveness of its industries by actively engaging in initiatives to prevent and address corporate espionage.

The country has implemented stringent regulations, such as the Federal Data Protection Act (BDSG) and the General Data Protection Regulation (GDPR) of the European Union, to safeguard personal and corporate information.

European Commission

The European Commission plays a significant role in combating corporate espionage, particularly in the context of cyber espionage. They have published multiple reports on cyber espionage and its impact on businesses and organizations. By producing such reports, the European Commission contributes to raising awareness, fostering dialogue, and shaping policies and strategies to enhance cybersecurity measures, protect intellectual property, and safeguard critical infrastructures within the European Union. The European Commission's active involvement positions it as a key stakeholder in the global efforts to prevent and mitigate the risks associated with corporate espionage, reinforcing its role as a major party in addressing this issue.

World Intellectual Property Organization (WIPO)

The World Intellectual Property Organization (WIPO) is a major party in combating corporate espionage due to its significant role in protecting intellectual property rights (IPR) globally. WIPO is a specialized agency of the United Nations dedicated to promoting and safeguarding intellectual property as a means to foster innovation, creativity, and economic development. It serves as a hub for international cooperation, policy development, and technical assistance in the field of intellectual property.

Timeline of Key Events

1980s-1990s: Economic Espionage by Japan: During this period, concerns rise about Japan's alleged economic espionage activities, particularly in acquiring advanced technologies from Western companies. Cases like the Toshiba-Kongsberg scandal in 1987 highlight instances of illicit technology transfer.

1996: Economic Espionage Act (USA): The U.S. Congress passes the Economic Espionage Act (EEA), which criminalizes trade secret theft and economic espionage. The EEA provides legal tools to prosecute individuals and entities involved in stealing trade secrets for economic or financial gain.

1996: Gillette vs Steven Louis Davis Case: A case that sheds light on the issue of corporate espionage and trade secret theft. The case involved a former Gillette employee, Steven Louis Davis, who was accused of stealing sensitive information related to Gillette's shaving products and selling it to a competitor, Warner-Lambert. This is one of the cases that birthed the term, “Insider”.

Late 1990s-2000s: Cyber Espionage Rise: The rapid growth of the internet and digital technologies leads to a significant increase in cyber espionage activities. State-sponsored actors and criminal organizations leverage cyber tools to infiltrate networks, steal intellectual property, and conduct espionage on governments and corporations.

2013: Mandiant Releases APT1 Report: Cybersecurity firm Mandiant releases a detailed report exposing a Chinese state-sponsored hacking group known as APT1 (Advanced Persistent Threat 1). The report highlights extensive cyber espionage activities targeting U.S. corporations and organizations, shedding light on the scale and sophistication of state-sponsored cyber espionage.

2015: U.S.-China Cyber Agreement: The United States and China reach a landmark agreement to address cyber espionage activities between the two countries. The agreement includes

commitments to refrain from conducting or supporting cyber-enabled theft of intellectual property for economic gain.

2017: Vault 7 Leaks: WikiLeaks publishes a series of documents collectively known as "Vault 7," revealing the cyber espionage capabilities and techniques of the U.S. Central Intelligence Agency (CIA). The leaks shed light on the advanced tools and methods employed by intelligence agencies for espionage purposes.

2018: EU General Data Protection Regulation (GDPR): The European Union implements the GDPR, which strengthens data protection and privacy rights within the EU. While not specifically targeting corporate espionage, GDPR provisions aim to enhance cybersecurity and protect personal data, reducing the risk of unauthorized access and data breaches that could facilitate espionage activities.

2020: U.S. Department of Justice Indictments: The U.S. Department of Justice indicts several individuals and entities, including Chinese hackers and intelligence officers, for cyber espionage and theft of intellectual property targeting corporations, universities, and governments.

Previous Attempts to Solve the Issue

Recognizing the gravity of corporate espionage, various international organizations, including the United Nations, have made efforts to address this issue. The UN Conference on Trade and Development (UNCTAD) has highlighted the importance of protecting intellectual property rights and promoting secure business environments. Additionally, several countries have enacted legislation to deter corporate espionage, enhance cybersecurity, and facilitate information sharing and cooperation among businesses and law enforcement agencies.

Such attempts include:

- The Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement (World Trade Organization): The TRIPS Agreement, which came into effect in 1995,

sets global standards for intellectual property protection, including trade secrets. It establishes obligations for member countries to provide legal frameworks, enforcement mechanisms, and remedies for intellectual property rights violations. The TRIPS Agreement has contributed to raising awareness and strengthening legal protections against corporate espionage at an international level.

- The Economic Espionage Act (EEA) (United States): The EEA, enacted in 1996, criminalizes theft or misappropriation of trade secrets related to products or services used in interstate or foreign commerce. It provides legal tools to prosecute individuals and entities involved in economic espionage activities and trade secret theft. The EEA has been instrumental in prosecuting cases related to corporate espionage and protecting trade secrets within the United States.

- European Union (EU) General Data Protection Regulation (GDPR): While not specifically targeted at corporate espionage, the GDPR, implemented in 2018, enhances data protection and privacy rights within the EU. It imposes strict regulations on how personal data is collected, processed, and stored, reducing the risk of unauthorized access and data breaches that could facilitate corporate espionage activities. The GDPR also includes provisions for mandatory reporting of data breaches, promoting transparency and accountability. Hence, many crimes related to (cyber) corporate espionage also breach GDPR laws.

However, despite these efforts, corporate espionage remains a persistent and evolving challenge. The rapid advancement of technology and the increasing interconnectedness of the global business landscape pose ongoing vulnerabilities. Therefore, it is essential for the G20

committee to discuss and formulate effective strategies and policies to prevent corporate espionage, promote international cooperation, and protect the interests of businesses and nations.

Possible Solutions

Enhance Cybersecurity Measures

Cybersecurity frameworks assist businesses in implementing preventive measures in all aspects of their operations, from the implementation of specific policies and procedures to the use of cutting-edge technologies. Although there is no common framework for cybersecurity in Europe, some significant initiatives have been undertaken at the national level in recent years:

- The CIIP ("Critical Infrastructures Information Protection") Framework in France;
- The "Cyber Assessment Framework" in the UK;
- The "Esquema Nacional de Seguridad" in Spain;
- The Italian National Cyber Security Framework (Based on the NIST Framework81) in Italy.

Create appropriate awareness and support

Since corporations are often afraid to admit they were a victim of corporate espionage, possible solutions could be to:

- Establish a confidential reporting platform where companies can share information about corporate espionage incidents without fear of negative consequences. This platform could be managed by a trusted third party, such as a government agency or an industry association, to ensure confidentiality and protection for the reporting entities.

- Provide legal protections for reporting entities by implementing legislation that offers legal protections for companies reporting corporate espionage incidents. This could include safeguards against retaliation, protection of trade secrets, and provisions to maintain

confidentiality throughout the reporting process. Companies should feel assured that reporting such incidents will not result in detrimental effects on their reputation, stock prices, or business relationships.

- Employee training and awareness. Perhaps corporate espionage can be prevented altogether if comprehensive training programs are provided to employees, educating them on cybersecurity best practices, social engineering threats, and the importance of maintaining strict data confidentiality.

Bibliography (MLA)

Beattie, Andrew. "Corporate Espionage: Fact and Fiction." Investopedia, 12 July 2022, www.investopedia.com/financial-edge/0310/corporate-espionage-fact-and-fiction.aspx#:~:text=Corp orate%20espionage%20is%20stealing%20proprietary. Accessed 27 June 2023.

"Corporate Espionage Is Entering a New Era." The Economist, 30 May 2022, www.economist.com/business/2022/05/30/corporate-espionage-is-entering-a-new-era. Accessed 27
June 2023.

European Commission. The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber. 2018, https://ec.europa.eu/docsroom/documents/34841/attachments/1/translations/en/renditions/native Accessed 27 June 2023.

Robinson, Shane W. "CORPORATE ESPIONAGE 101." Giac.org, Global Information Assurance Certification Paper, 2022, www.giac.org/paper/gsec/1587/corporate-espionage-101/102941. Accessed 27 June 2023.

"What Is Corporate Espionage? And How to Prevent It." Www.bluecube.tech, 12 Aug. 2022, www.bluecube.tech/blog/corporate-espionage-meaning-and-preventing-it. Accessed 27 June 2023.

Appendix or Appendices

Highly Recommended Reading!

A European Commission Report: The scale and impact of industrial espionage and theft of trade secrets through cyber

https://ec.europa.eu/docsroom/documents/34841/attachments/1/translations/en/renditions/native

A Research Report: CORPORATE ESPIONAGE 101

https://www.giac.org/paper/gsec/1587/corporate-espionage-101/102941