A Growing Cybersecurity Threat in Taiwan and the EU: A Content Analysis and Policy Assessment Towards Multi-Level Cooperation

By

Manuel Preda Herrera

王博

Submitted to the Faculty of
Department of International Affairs in partial fulfillment of
the requirements for the degree of
Bachelor of Arts in International Affairs

Wenzao Ursuline University of Languages
2022

WENZAO URSULINE UNIVERSITY OF LANGUAGES
DEPARTMENT OF INTERNATIONAL AFFAIRS

This senior paper was presented

by

Manuel Preda Herrera
王博

It was defended on

November 19th 2022

and approved by

Reviewer 1: Yu-Hsuan Lee Assistant Professor, Department of International Affairs

Signature: _____ Date: _____

Reviewer 2: Yuan-Ming Chiao, Assistant Professor, Department of International Affairs

Signature: _____ Date: _____

Adviser: Philipp Fluri, Visiting Professor, Department of International Affairs

Signature: _____ Date: _____

A Growing Cybersecurity Threat in Taiwan and the EU: A Content Analysis and Policy Assessment Towards Multi-Level Cooperation

Manuel Preda Herrera 王博, B.A.

Wenzao Ursuline University of Languages, 2022

Abstract

In the wake of the COVID-19 pandemic, cybercrime, and cyberattacks increased by nearly 600% worldwide. Both the public and private sectors in the European Union and Taiwan have been hacked and put under threat. As the nation becomes more connected and technological, attackers seek to exploit its vulnerabilities. A growing number of Taiwanese institutions and businesses are being targeted. A parallel case can also be pointed out by European Union governments and enterprises. Despite this, the majority of organizations remain at the beginning stages of their development, coordination, and response to cyber security threats. In order for Taiwanese and European economies to operate effectively, cyberspace has to be open, safe and aligned with deep cooperation, a task that this study addresses and identifies areas for improvement. In this study, I explore possible synergies between the European Union and Taiwan in cybersecurity as well as how to coordinate actions when it comes to Advanced Persistent Threats (APTs) and other digital dimensions, identifying vulnerabilities, challenges, and most importantly, finding feasible solutions. Furthermore, it provides recommendations for overcoming challenges they face in leveraging public-private partnerships and implementing experience-based cybersecurity practices by focusing on fields of potential collaboration and weaknesses that overlap.

Keywords: Cybersecurity, Cyber Space, Policy-making, Synergy, Private Sector, Public Sector, Cyberdefense, ENISA, MODA

台灣和歐盟日益增長的網絡安全威脅:多層次合作的內容分析和政策評估

Manuel Preda Herrera 王博, B.A.

Wenzao Ursuline University of Languages, 2022

Abstract

在 COVID-19 大流行之後，全球網絡犯罪和網絡攻擊增加了近 600%。歐盟和台灣的公共和私營部門都遭到黑客攻擊並受到威脅。隨著各國國變得更加互聯，攻擊者試圖利用其漏洞，並使越來越多的台灣機構和企業成為目標，歐盟政府和企業走過的經驗，可以提供台灣作為參考。面對網路攻擊，大多數台灣的組織仍處於發展、協調和應對網絡安全威脅的初始階段。為了讓台灣和歐洲經濟體有效運作，網絡空間必須是開放、安全的，並與深度合作、保持一致，這是本研究試圖討論的領域。在這項研究中，探討了歐盟和台灣在網絡安全方面的協同作用，以及在 APT 和其他數字維度方面如何協調行動，識別漏洞和挑戰，最重要的是找到可行的解決方案。此外，它通過關注潛在的合作領域和重疊的弱點，為克服他們在利用公私伙伴關係和實施基於經驗的網絡安全實踐方面的挑戰提供了建議。

關鍵詞:網絡安全、網絡空間、政策制定、協同作用、私營部門、公共部門、網絡防禦、ENISA、MODA

ABBREVIATIONS

NIS: Network and Internet Security

NCPT: National Cyber Security Program (Taiwan)

GDPR: General Data Protection Regulation (European Union)

MODA: Ministry of Digital Affairs (Taiwan)

EU: European Union

ENISA: European Agency for Cybersecurity

iWin: Watch Internet Network

NICST: National Information and Communication Security Task Force (Taiwan)

IoT: Internet of Things

ICT: Information and Communication Technology

APTs: Advanced Persistent Threats

HITCON: Taiwan's Hacks in Taiwan Conference

FIRST: International Forum of Incident Response & Security Teams

R&D: Research and Development

EEAS: European External Action Service

DPP: Democratic Progressive Party (Taiwan)

CDI: Core Defense Industries

TABLE OF CONTENTS

LIST OF TABLES & FIGURES

INTRODUCTION

Background

Cyber security is becoming more integral in everyday life in the digital age, as well as the relevance of strengthening the capability to protect national security. A high level of specialization distinguishes the Taiwanese economy in producing components, especially technological devices. Security plays an increasingly critical role as hardware becomes increasingly intelligent. This, in conjunction with the increasing number of cyberattacks, has prompted the Taiwanese government to strengthen and support the Cybersecurity eco-system through regulatory reforms and economic incentives. Taking 2019 as an example of a year when nation-states were increasingly connected, we identified six major trends in cyber security attacks. The following trends are considered security threats to critical infrastructures: Advanced Persistent Threats (APT) targeted attacks to steal confidential data, hacking into cyber security suppliers to compromise supply chain security, the proliferation of critical infrastructure security risks, and the intensification of data leaks and digital certification attacks. Looking at the Taiwanese case, throughout 2016-2019, hackers invaded the web hosting industry by taking control of 500,000 webcams and launching Distributed Denial of Service (DDoS) attacks[1]. Hackers have turned to corporate networks for the foreseeable future to increase their bandwidth and facilitate DDoS attacks. As a whole, the number is expanding throughout the global economy, with countries highly involved in the technological supply chain potentially more vulnerable than those who are not.

[1] Information Security Office 資通安全處. "National Cyber Security Program of Taiwan (2021 to 2024)." 中文版(Open New Window), 2021. https://nicst.ey.gov.tw/en/FD815304EBFFE6FC/639d32e8-2a07-40da-b033-bc6c95d015ce.

Consequently, I turn my attention to two actors that are transversally different but interrelated: the European Union and Taiwan. The number and sophistication of cyberattacks and cybercrime are increasing throughout Europe. With 22.3 billion devices expected to be connected to the Internet of Things by 2024[2], this trend is expected to grow even further in the coming years. The European Union's General Data Protection Regulations (GDPR), which constitute the world's most stringent privacy and security laws, have gained worldwide renown as a model for regulating and increasing security against cyber attacks and vulnerability attacks.

Regarding Taiwan in particular, the Taiwanese National Cyber Security Program (NCPT) has emphasized the urgency of coordinating a national response to cybercrime from the public sector.Both policies show different approaches and procedures to counter a common general threat.

Regarding the first one, in spite of the fact that it was drafted by the European Union (EU), it imposes obligations on all organizations that collect or target data related to people in the EU. As of May 25, 2018, the regulation took effect. Those who violate the GDPR's privacy and security rules can face fines of up to tens of millions of euros. Consider the case of Frankfurt, Germany, which received a targeted Emotet malware attack in December 2018, which resulted in the suspension of internet service in several German cities. On the other hand, in Taiwan, cyber threats are also a real concern. Taiwan's financial sector has been targeted by a hacking group believed to be affiliated with the Chinese government, which exploited a vulnerability within a security software solution used by approximately 80%[3] of the country's financial institutions for months.

[2] Council, European. “Cybersecurity: How the EU Tackles Cyber Threats.” Consilium, April 29, 2022. https://www.consilium.europa.eu/en/policies/cybersecurity/.

[3] Wu, Jason, and Matthew Fulco. “Taiwan's Cybersecurity Dilemma.” Taiwan Business TOPICS, January 17, 2022. https://topics.amcham.com.tw/2021/05/taiwan-cybersecurity-dilemma/.

According to reports[4], the attacks began at the end of November 2021 and lasted until early February 2022. In spite of those incidents, the reality of cybersecurity policy-making is an essential part of ensuring the defense and security of nations that are highly interconnected with the Internet and other servers. Taiwan has been disappointingly unprepared for OT-related cyber threats in the past. Gwen Hsieh, security offerings manager at IBM Security, argues that plants with less sophisticated infrastructure are more vulnerable to cyberattacks, which makes them "low hanging fruit for hackers[5]". Taiwanese companies have always considered cybersecurity as " nice to have " until an actual attack forces them to adopt a more serious approach.

Contrary to the above situation, non-compliant companies in the EU are punished harshly by General Data Protection Regulation (GDPR) and local legislation. For instance, Germany requires operators of critical infrastructures, such as information technology and telecommunications, to report security breaches involving consumer and employee data. A company violating these regulations may be subject to fines as high as €10 million or 2% of its global revenue. However, in Taiwan, penalties imposed by the Executive Yuan for unreported security breaches are limited to only NT$5 million(158,664.39 €, taking the value of 1 EUR = 31.5131 TWD). For Taiwanese companies to be held accountable, stricter regulations will probably need to be enacted. The cybersecurity sector in the European Union and Taiwan each has its strengths and flaws. By combining those strengths and challenges to overcome and creating software and hardware integrations, there is a real opportunity to develop cross-national synergy, which will enforce and harden both

[4] Cimpanu, Catalin. "Chinese Hackers Linked to Months-Long Attack on Taiwanese Financial Sector." The Record by Recorded Future, February 23, 2022. https://therecord.media/chinese-hackers-linked-to-months-long-attack-on-taiwanese-financial-sector

[5] Wu, Jason, and Matthew Fulco. "Taiwan's Cybersecurity Dilemma." Taiwan Business TOPICS, January 17, 2022. https://topics.amcham.com.tw/2021/05/taiwan-cybersecurity-dilemma/.

private and public sector cybersecurity strategies.

Motivation

As a result of my desire to pursue an academic career after graduation, and my passion for Security, Defense, and Policy Strategies, cybersecurity became one of my primary research areas. An essential aspect of the study is the threat interconnected nations pose to national security, which will serve as a stepping stone to my future academic career. A deeper understanding of the economics and development of nation-states' ability to maintain security depends on understanding the processes underlying the defensive and offensive aspects of cybersecurity.

Research Purpose

As the EU and Taiwan have similar cybersecurity and national threats, both could pursue similar policies to engage the private sector, especially for the low-regulated Taiwanese market. Further, the EU and Taiwan are governed as democratic regimes on an international and domestic scale. As a result of this similar political approach, both regions are expected to seek similar outcomes from cybersecurity policies and the process of establishing such procedures. My research aims to compare both situations, challenges, incidents, policy-making, relevant actors, and actions taken by both sides to identify which strategies might foresee more consolidated cybersecurity and defense policy, as well as action-oriented recommendations.

Research Questions

1. In terms of cybersecurity threats, how does Taiwan differ?

2. Are Taiwanese-European cooperations capable of improving the current cyber security situation of both parties?

3. What specific areas of cooperation between the two sides should be opened up and strengthened?

Contribution

Specifically, this research aims to develop a comprehensive international cybersecurity policy, identify Taiwan's cybersecurity efforts, analyze Taiwan's cybersecurity dilemma, and argue for the relevance of the European Union's Cyber Security policy for a Taiwanese response policy and further collaboration. Recognizing the critical cybersecurity players operating in Taiwan and Europe and developing a comprehensive database is also integral to my contribution, enhancing and showing the flaws of both systems and recommendations to overcome them.

Limits

Taiwan's Cybersecurity policy and discourse is a relatively new initiative undertaken by the government. As a result, fewer data are available than the one from the EU side. Additionally, the information about sensitive and critical cyberattacks cannot be accessed for research rather than reports and articles posted after the mentioned attack occurred. Consequently, we can only analyze challenges and real threats based on the narratives and facts that Taiwan and the EU are willing to share. It would have been an ideal scenario for my research to conduct final

interviews to corroborate some recommendations and collect primary data from the person who currently manages and create cyber defense policies, but this was not possible since

a. Lack of connection with the research agencies and institutions
b. Time-consuming on the individual arrangement of specific interviews with a low probability of response
c. Personal and professional inferences subtract big quantities of time from the research design and process.

Nevertheless, these limitations haven't stopped a meticulous and extensive analysis of the current background, points of cooperation and conflict, as well as the expected outcomes of this research paper.

Delimits

The scope of my research will be limited to the challenges, threats, and policy discourses related to Taiwanese and European Union national interests, ignoring other vulnerable states such as the United States or Japan. Policy analysis will mainly focus on the government mentioned above policies toward cybersecurity, whereas other related policies or minor regulations will broaden the scope of my research but not be included in the primary analysis process.

LITERATURE REVIEW

The Role of the Private Sector in Cybersecurity

Even though the new digital era brings enormous economic and social benefits, it also transforms the nature and scale of cyber risks. It creates new vulnerabilities that attackers seek to exploit. A growing number of European governments and businesses, as well as Taiwanese, are being targeted. The majority of organizations, however, remain unaware of or seem to underestimate and even disregard the security vulnerabilities they face through and in cyberspace. It is essential for the reliable functioning of both European and Taiwanese economies that cyberspace is open, safe, and secure. This shows the importance of corporate cybersecurity for the economic well-being of the places under my study. A broad variety of agencies and private sector institutions aim to provide recommendations on how companies can overcome the challenges they face in implementing good cybersecurity practices. Nevertheless, these practices are not limited to European or Taiwanese governments; it is essential to remember that the more connected a nation is, the more vulnerable it becomes. Giving a more clear example of this, linked to having a broader understanding of the cyber threat we are experiencing, The United States of America, as a global provider of data and the internet, is, without doubt, the most connected nation on earth when examining its connectivity as a whole[6].

As a result, the United States private sector cybersecurity policy may serve as a reference for understanding how the direction of regulations and actions can be anticipated, and regarding the specific side of the Taiwanese private sector, after extensive revision of related documents, we can witness the high level of reference

[6] Cybersecurity & Infrastructure Security Agency. “Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization.” CISA, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-277a.

that Taiwanese corporations take from the American counterpart, even in some cases, cooperation directly

Businesses manage a significant share of online activity related to national security, so they must ensure the system's overall integrity more effectively. The United States relies heavily on the private sector to ensure federal security[7]. Protecting the private sector is increasingly important since the United States relies heavily on private corporations to provide national security, more than most, if not all, other nations. Corporations manufacture the majority of the nation's arms. Corporations primarily produce software and hardware for government computers. Companies under contract with the government carry out many critical security functions, including collecting and processing intelligence and conducting covert operations.

As a result of the Bush administration's contracting out of significant parts of previous in-house missions, the government heavily relied on the private sector for security, including cybersecurity. During the administration of President Obama, this trend has only slightly slowed down. As long as safety is provided only to the computers and Internet used by the public sector, the United States cannot be considered secure.

The private sector may appear at first glance to be strongly supportive of new cybersecurity measures. The costs associated with cybercrime, such as electronic money theft, are significant for private companies. The same is true of industrial espionage, mainly perpetrated by other countries, depriving American corporations of the fruits of their long-term investments in research and development(R&D) and giving unfair competitors a significant advantage. Furthermore, if cyber warfare were

[7] Wheeler, Tom. “Protecting the Cybersecurity of America's Networks.” Brookings. Brookings, March 9, 2022.
https://www.brookings.edu/blog/techtank/2021/02/11/protecting-the-cybersecurity-of-americas-networks/.

to break out, many of the assets that would be damaged are likely to belong to private corporations. Furthermore, businesses are owned and operated by individuals with a vested interest in the country's safety.

Simply put, businesses have not shown a solid commitment to cybersecurity. Philosophical reasons are one of the reasons. Many corporate leaders and think tanks in the corporate world adhere to the libertarian or conservative laissez-faire approach, believing they should be left alone, not regulated, and free to pursue their interests. Further, they assert their primary duty is to their shareholders, who own the corporations, rather than the common good.

In addition to such philosophical arguments, several more practical obstacles have limited and continue to define efforts to improve security in the private sector.

According to some security experts, current incentives for corporations to improve the security of their computer systems are not aligned in a manner that encourages voluntary action. It is common for companies to conclude that the cost of implementing security measures is greater than the loss associated with cybercrime. According to Fred H. Cate[8], director of the Center for Applied Cybersecurity Research at Indiana University, government intervention in the cybersecurity market is necessary.

Having examined the American case regarding private sector cybersecurity, it is relevant for the study to examine how the European Union views the private sector regarding its cybersecurity efforts. In addition to offering many economic and social benefits, this new era of digitization also poses several challenges and new vulnerabilities that cyber attackers seek to exploit. The frequency with which European countries and businesses are targeted is increasing. By the 2017 State of

[8] Cate, Fred H. and Dempsey, James X., "Bulk Collection: Systematic Government Access to Private-Sector Data" (2017). *Books & Book Chapters by Maurer Faculty*. 173.
https://www.repository.law.indiana.edu/facbooks/173

Information Security Survey in Europe[9], at least 80% of companies have been affected by an information security incident within the last year, with the number of security incidents increasing across the industry. According to some, the total number of security incidents worldwide increased by 38% in 2015[10], compared to the preceding year. Even though ransomware is not a new phenomenon, (non)Petya and WannaCry have become well-known for crippling businesses in Europe and highlighting the importance of cybersecurity awareness.

The potential impact on businesses is, however, unknown or underestimated by many companies. According to a survey conducted by Marsh[11], 69% of European companies do not fully understand their exposure to cyber risks or have a basic understanding. In addition to improving their commercial performance, a more cyber-secure and cyber-aware environment will also benefit the European economy. Furthermore, companies must keep up with the drastically changing regulatory environment and the rapidly evolving cyber threat landscape. Upon implementing the General Data Protection Regulation (GDPR), companies must notify national data protection authorities and affected individuals when a data breach occurs. To avoid staggering fines, organizations should prepare to comply with all aspects of GDPR, as failure could result in staggering penalties. Symantec's State of European Data Privacy Survey indicates that many companies are unaware and unprepared for the new regulation and its implications.

For this major and general threat posted for the European Union

[9] PricewaterhouseCoopers, PWC. "Cybersecurity, Risk & Regulatory." PwC, 2022. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory.html.
[10] ENISA, European Agency. "ENISA Surveys Evolving Threat Landscape." *Computer Fraud & Security* 2013, no. 1 (2021): 1–3. https://doi.org/10.1016/s1361-3723(13)70001-0.
[11] Marsh &, McLennan Companies. "MMC Cyber Handbook 2020 - Marsh Mclennan." MMC Cyber Handbook 2019 Perspectives on Cyber Risk in the Digital Era, 2020. https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2019/oct/MMC_cyber_handbook_2020_final_digital.pdf.

Cybersecurity vulnerability, the European agency for specific Cybersecurity challenges was created. It is the responsibility of the European Union Agency for Cybersecurity (ENISA) to achieve a high standard of cybersecurity across the European Union.

With the help of cybersecurity certification schemes, ENISA contributes to developing EU cyber policy, enhances the trustworthiness of Information and Communication Technology (ICT) products, services, and processes, collaborates with the Member States, and prepares the EU to face tomorrow's cyber challenges. Further exploration of this regard will be given in the section " Role of Public Sector in Cybersecurity".

Last but not least, it is now time to summarize and examine the relationship between the Taiwanese private sector and the national cybersecurity threat level.

It has been reported that the Taiwanese tech hardware giant Acer has been the victim of a ransomware attack - a form of cyber attack in which money is demanded in exchange for access to hacked sensitive data. A hacker group known as Revil (also known as Sodinokibi), believed to be located in Russia, was responsible for the attack. Its dark web-based data leaks blog posted screenshots of hacked financial documents and confidential files. It demanded Acer pay $50 million - the highest amount ever asked in such an attack. In a reported negotiation, Acer offered a lower sum to REvil, which the hackers rejected[12].

Around a month later, Quanta, Apple's leading Taiwanese supplier of

[12] Abrams, Lawrence. "Computer Giant Acer Hit by $50 Million Ransomware Attack." BleepingComputer. BleepingComputer, March 20, 2021. https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/.

MacBooks, was attacked by REvil's second Taiwanese ransomware attack[13]. The group posted 21 screenshots of what it claimed were stolen MacBook schematics on its blog. Like the Acer attack, REvil is believed to have demanded US$50 million from Quanta to retrieve the files. However, the tech news website Bleeping Computer reported that neither Quanta nor Apple paid the ransom by the date REvil specified.

The group began publishing the files shortly after that.

Similar cyberattacks have been reported against Taiwanese electronics company Compal and the state-owned Chinese Petroleum Corporation in recent months, indicating a growing trend.

The sophistication and frequency of such attacks have increased over the years, with hackers often demanding payment in cryptocurrency, which has become increasingly popular for its convenience and anonymity. The IBM X-Force Threat Intelligence Report estimates that 23% of all cyberattacks in 2020 were caused by ransomware[14].

Many Taiwanese semiconductor manufacturers are integrating cybersecurity into their business models. One of the significant factors in Taiwan's semiconductor industry's success is the trust it has built with its customers by safeguarding their personal information.

As important as it is for customer relations to ensure sensitive information will be protected, the Taiwanese national cybersecurity horizon provides a broader perspective on the industry's reputation in this regard. Considering the importance of Taiwanese chip manufacturers to the global technology supply chain, cybersecurity is

[13] Murphy, Hannah. "Apple Supplier Quanta Hit by Cyber Attack." Subscribe to read | Financial Times. Financial Times, April 21, 2021. https://www.ft.com/content/0ec11549-9d68-4ca2-bbac-34684c86abab.

[14] IBM, Enterprises. "IBM Security X-Force Threat Intelligence Index." IBM, February 23, 2022. https://www.ibm.com/reports/threat-intelligence/.

no longer just an issue of concern at the company level. Still, it is also a matter of national security. Keeping in mind the importance of integrating personal data privacy and innovation into digital defense systems, Taiwan and the entire global economy is at risk if the private sector does not take responsibility.

Rather than targeting enterprises with well-developed cyber defenses, such as Taiwan Semiconductor Manufacturing Co. (TSMC), attackers focus on weaker upstream and downstream parts of the supply chain[15]. Manufacturers of equipment, suppliers of materials, and even public utilities such as water and electricity are among the weaker targets. Cyber-attacks are more likely to occur in plants with less sophisticated infrastructure.

Additionally, fabless companies, such as Broadcom and Qualcomm, exchange large amounts of data and sensitive information with their supply chain partners, making it increasingly difficult to prevent phishing emails, credentials theft, and ransomware attacks.

It should be a given that Taiwan has a robust cybersecurity infrastructure given its irreplaceable role in the global high-tech supply chain. Despite this, Taiwan has been disappointingly underprepared for cyber threats related to the OT. Despite a 2000% increase in OT-related security incidents in 2019, around 81% of companies that were attacked did not have OT-specific incident response plans[16]. In addition, many Taiwanese manufacturers still use outdated operating systems or, in some cases, second-hand computers.

Cybersecurity has always been merely a "nice thing to have" for Taiwanese companies until an actual attack compels them to take an active role in cybersecurity.

[15] TSMC, English Company Press. “TSMC Details Impact of Computer Virus Incident.” TSMC Details Impact of Computer Virus Incident, 2018. https://pr.tsmc.com/english/news/1969.

[16] Ibm, Enterprises. “IBM Security X-Force Threat Intelligence Index.” IBM, February 23, 2022. https://www.ibm.com/reports/threat-intelligence/.

Currently, investing in cybersecurity is not viewed as a profitable investment by companies since they mistakenly believe that undergoing an attack costs less than investing in cybersecurity. However, this trend during the pandemic seems to have changed in direction.

Let's look at the general overview of what has been revealed in this literature review.

Attackers are exploiting new vulnerabilities as the new digital era brings enormous economic and social benefits. Organizations and private institutions provide recommendations on how companies can implement good cybersecurity practices. Increasing connectivity makes a nation more vulnerable to cyber threats. In addition to contracting out significant parts of previous in-house missions, the Bush administration heavily relies on the private sector to ensure federal security. Obama's administration hasn't slowed down this trend. It appears that many corporate leaders and think tanks support new cybersecurity measures but support a libertarian or conservative laissez-faire approach that emphasizes shareholders over society.

Private sector security efforts have been limited by philosophical arguments and costs associated with security implementation. According to this, the private sector cybersecurity perceptions in the United States and the European Union were examined above. Targeting European businesses and countries is on the rise. Due to underestimating cyber risks, European economies benefit from a more cyber-secure and cyber-aware environment.

Regarding the General Data Protection Regulation (GDPR) and the action of the ENISA agency, these two elements are essential to understanding the current trend of development of the European cybersecurity horizon. According to Symantec's State of European Data Privacy Survey, data privacy regulations are unfamiliar to many

companies. ENISA was created to ensure high cybersecurity standards across the EU.

I examined how hackers associated with the Russian hacker group Revil attacked Taiwanese hardware giant Acer on the Taiwanese side. Apple and Quanta were told to pay $50 million to REvil by a specified date, but neither did.

An example of rising cybersecurity threats to the Taiwanese private sector is the state-owned Chinese Petroleum Corporation and Taiwanese electronics company Compal have both been attacked recently.

In order to ensure customer trust, Taiwanese semiconductor manufacturers integrate cybersecurity. Cybersecurity is a matter of national security for Taiwanese semiconductor manufacturers. Rather than targeting enterprises with well-developed cyber defenses, attackers target weaker parts of the supply chain, such as equipment manufacturers, materials suppliers, and even public utilities.

In Taiwan, outdated operating systems and second-hand computers make it prone to cyber-attacks. Taiwanese companies seem to be increasing their investments in cybersecurity actions due to the cyber threats pandemic timed related attacks.

The Role of the Public Sector in Cybersecurity

This literature review focuses exclusively on institutions related to cybersecurity and data protection to advance the understanding of European and Taiwanese public sector policies and actions regarding cybersecurity. As a result, the European Cybersecurity Agency (ENISA) and the General Data Protection Regulation (GDPR) on the European side, the Taiwanese National Cybersecurity Plan, and the Ministry of Digital Affairs (MODA) on the Taiwanese side serve as the section's cornerstones.

Protecting the open internet and promoting freedom and opportunity online

through the EU Cybersecurity Plan.

In conjunction with the High Representative of the Union for Foreign Affairs and Security Policy, the European Commission has published a cybersecurity strategy and a proposed directive on Network and Information Security (NIS).

As outlined in the EU's cybersecurity strategy, "An Open, Safe and Secure Cyberspace," this document represents the EU's comprehensive approach to preventing and responding to cyber disruptions and attacks. As a result, the digital economy can grow safely and by European values of freedom and democracy. Cyber resilience is being enhanced, cybercrime is being reduced, and European cyber security policies are being strengthened.

By the Common Security and Defence Policy (CSDP), the development of cyber defense capabilities is necessary. The story of industrial and technological resources is essential to promote cyber security. By developing a coherent European cyberspace policy, core European values can be promoted

Towards international cooperation; the EU international cyberspace policy promotes respect for EU core values, defines norms for responsible behavior, and applies existing international law in cyberspace. It also assists countries outside of the EU in building cybersecurity capabilities.

As a result of the EU's commitment to protecting citizens from online crime, a European Cybercrime Center has been established (IP/13/13), legislation on attacks on information systems has been introduced (IP/10/1239), and a Global Alliance for combatting child sexual abuse online has been established (IP/12/138). This Strategy also includes developing and funding a network of National Cybercrime Centers of Excellence to facilitate training and capacity building[17].

[17] Commission , European. “Cybersecurity Policies.” Shaping Europe's digital future, 2020. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

Providing a framework for ensuring a secure and trustworthy digital environment throughout the EU is the goal of the proposed NIS Directive, which is consistent with the overall Strategy. Under the Directive, all Member States, Internet enablers, and operators in the energy, transport, banking, and healthcare sectors are required to ensure that the digital environment is secure and trustworthy.

An appropriate national NIS strategy that each Member State must adopt, as well as the designation of a competent authority for the NIS responsible for preventing, handling, and responding to NIS risks and incidents at the national level;

In addition, the Member States and the Commission should establish a mechanism for sharing early warnings of risks and incidents through a secure infrastructure, cooperating, and undertaking regular peer reviews;

A critical infrastructure operator (financial services, transportation, energy, health), an enabler of information society services, and a public administration must adopt risk management policies and report significant security incidents affecting their core services.Neelie Kroes, Vice-President of the Digital Agenda at the European Commission, said[18]:

"We need to take coordinated action - the cost of not taking action is much higher than the cost of acting." Internet security is increasingly important as people become more dependent on it. A secure internet protects our freedoms, rights, and ability to conduct business. It's time to take coordinated action." For this reason, as long as the EU aims to maintain free and open cyberspace, it must adhere to the same values, norms, and principles it holds dear in the offline world. Protecting the rule of law, democracy, and fundamental rights in cyberspace is imperative. As outlined in the Strategy, the EU is taking concrete actions to reduce cybercrime drastically, but

[18] Commission, European. “The Cybersecurity Strategy.” Shaping Europe's digital future, 2020. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

many EU countries lack the tools to track down and combat online organized crime.

Taiwan has effectively increased its cyber security preparedness since 2001 due to six major cyber security plans or programs developed by the National Information and Communication Security Taskforce, Executive Yuan (NICST). The following highlights are provided for each project or program:

a.Plan for Phase One of the Mechanism (2001-2004)

The development of a cyber security defense system and completing the classification mechanism for government agencies. The Executive Yuan announced on January 17, 2001, the "Building Taiwan's Communication and Information Infrastructure Security Mechanism Plan" (Phase One Mechanism Plan), which aims to create a safe, reliable information and communication environment for Taiwan. As a result of this phase, a cyber security defense system has been developed, including

As a result of the establishment of the NICST in conjunction with the technical staff unit, the National Center for Cyber Security Technology, Taiwan will now have a competent authority responsible for its cyber security policies and infrastructure.

(1) The promotion of cyber security management systems for key government agencies whose work is directly related to the public's day-to-day lives, the provision of relevant cyber security support, and the designation of government agency requirements at different levels through the establishment of mechanisms and categories for reporting and notifying cyber security incidents by agencies, as well as conducting cyber security audits on specific agencies.

A third priority is to promote cyber security education and training among information personnel, reinforce cybersecurity workforce training and awareness, and raise public awareness of cyber security.

Cyber security laws and regulations should be revised and amended, technical standards and regulations should be developed, and mechanisms should be established for inspecting and ensuring building products are secure.

The planning, promotion, and implementation of Information Security Management Systems (ISMS) for key operating systems of critical infrastructures and cyber security management programs, including alert and reporting mechanisms for the cyber security center and training for personnel.

b. Mechanism Plan for Phase Two (2005-2008)

Establishing the national security operation center and completing cyber security defense capabilities. In order to strengthen Taiwan's overall cyber security defense foundation, the Executive Yuan has approved the "Building Taiwan's Communication and Information Infrastructure Security Mechanism Plan (2005-2008 Phase Two Mechanism Plan)" as an extension of the Phase One Mechanism Plan. This has led to the following key outcomes:

1. *Establishing a National Security Operation Center* (N-SOC) that will provide 24-hour security for key government agencies, including monitoring and alerting services.

2) *Establishing a mechanism for appointing chief information security officers* (CISOs) at government agencies responsible for promoting and implementing information security plans within departments.

The cyber security responsibility level classification of government agencies is expanding. This increases the number of significant government agencies included in the cyber security defense system and extends the scope of that system to have an education. Assisting regional education network centers in establishing ISMS by promoting the introduction of ISMS into the education system.

(3) *Enhancing work performance through auditing*, introducing internal auditing systems to government agencies to ensure the promotion of cybersecurity-related activities, and conducting external cybersecurity audits of public and private entities to provide audit recommendations.

The cyber security plan defense range will be extended to enhance online transactions and protect personal information. This will lead to the development of cyber security reinforcement plans.

c. (2009-2012) Phase Three Development Program

Strengthening the overall capability of responding to cyber security incidents and improving the mechanism for reporting and responding.

"National Cyber Security Development Program (2009-2012)" (Phase Three Development Plan) was announced by the Executive Yuan in January 2009[19]. Aiming to develop a "secure, trustworthy Taiwan" and sound, quality digital life," the program shared the government's experience promoting cyber security with society, gradually reinforcing cyber security defense mechanisms within the private sector. Among the significant findings are the following:

Establishing a cyber security incident response procedure from detection, recognition, and analysis to response is essential, enhancing reporting efficiency and continuously strengthening emergency reporting, response, and recovery capabilities.

A- and B-level government agencies must implement cyber security governance and performance evaluation. They must assign cyber security personnel, categorize and classify information systems, and develop basic cyber security mechanisms consistent with their classifications and categories.

[19] Digital Affairs (R.O.C.) , Minister of. “Cyber Security Policies and Regulations-Operations | Administration for Cyber Security, Moda.” Ministry of Digital Affairs(open in new window), 2022. https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648.

Taiwan's government agencies and businesses should implement the Plan-Do-Check-Act (PDCA) model and promote international cyber security standard certifications (such as ISO 27001) to reduce relevant risks.

(4) *Enhancing the reliability and security of e-commerce*, strengthening identity verification mechanisms, and promoting PKI certification services to facilitate secure online transactions.

(5) *Encouraging businesses and organizations to conduct third-party evaluations*, enforcing legally authorized cyber security inspections on all businesses to ensure enhanced personal information protection, building cyber security management systems, conducting internal audits, and enlisting third parties to complete cyber security audits.

(6) *Strengthening cyber security research capacities*, encouraging higher education institutions to offer cyber security courses, cultivating professional cyber security research talents, developing key cyber security technologies, and transferring them to industries for added-value applications.

They are promoting cyber security awareness, conducting cyber security awareness events at various school levels, encouraging businesses to review the security of their information assets, and organizing cyber security checks and competitions for citizens to increase their awareness level.

d. Program for Phase Four Development (2013-2016)

Sharing cyber security intelligence, strengthening cyber security defense management, and establishing joint monitoring mechanisms. The Executive Yuan approved a National Strategy for Cybersecurity Development Program (2013-2016) in 2013. Using the vision of "building a safe cyber security environment and moving towards a high-quality network society," the program emphasized the government's

ability to defend against cyber-attacks. It promoted the following four significant objectives[20]:

Establishing a national policy and environment: continuously updating and modifying cyber security policies, regulations, guidance, standards, and handbooks; reviewing Taiwan's cyber security regulations and discussing the creation of dedicated laws related to cyber security; implementing a mechanism to ensure appropriate cyber security personnel and budgets for government agencies and conducting annual assessments of cyber security service providers. To promote public corporatization, prepare to establish and operate the National Center for Cyber Security Technology. Conducting inspections and verifications of cyber security equipment, interacting with international certification and verification organizations, and regularly reviewing inspection items.

Developing a structure for government cyber security governance, evaluating cyber security maturity levels at A-, B-, and C-level government agencies, and establishing the Institute of Watch Internet Network (iWIN) as a means of improving internet content security management mechanisms; conducting cyber security offense and defense drills, preparing cyber security scenarios and hands-on exercises.

Industrial development and technological upgrades are needed to enhance technological competitiveness and innovative cyber security autonomy. We are strengthening collaborations with businesses and academic institutes to develop cybersecurity technology and utilize innovative cybersecurity technology in practical applications. Talent cultivation and international exchanges: developing professional

[20] Pryor, Crystal D., Tania Garcia-Millan, Jeffrey Gelman, Tanvi Madan, Scott Moore, Crystal Pryor, Lisa Reijula, et al. "Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership." Edited by Bonnie S. Glaser and Matthew P. Funaiole. *Perspectives on Taiwan: Insights from the 2018 Taiwan-U.S. Policy Program*. Center for Strategic and International Studies (CSIS), 2019. http://www.jstor.org/stable/resrep22549.5.

cyber security training and certification mechanisms; establishing professional cyber security personnel registration and certification mechanisms; and establishing a system for evaluating cyber security competence, which requires personnel across all departments to complete cyber security competence training courses and pass tests regularly.

e. Development Program Phase Five (2017-2020)

We are encouraging the passage of the Cyber Security Management Act, which strengthens Taiwan's joint cyber security defense system.

As part of Phase Five of the National Cyber Security Program (2017-2020), the Executive Yuan approved the "National Cyber Security Program (2017-2020).While promoting the country's digital transformation and the development of an innovative economy, the government is facing cyber security threats and challenges. security defense measures in response to complex and ever-changing cyber security threats.

Based on the vision of "building a secure, trustworthy digital nation," Phase Five integrates the three primary policy goals of improving national cyber security defense mechanisms, enhancing cyber security industry autonomy, and cultivating high-quality cybersecurity talent, designating 11 specific measures to gradually launch Taiwan's cyber security defense in depth and joint defense system and stabilize Taiwan's cyber security frontline[21].

f. In Phase Six of the Development Program (2021-2024),

This Cybersecurity program plays an increasingly significant role in Taiwan's

[21] Pryor, Crystal D., Tania Garcia-Millan, Jeffrey Gelman, Tanvi Madan, Scott Moore, Crystal Pryor, Lisa Reijula, et al. “Taiwan’s Cybersecurity Landscape and Opportunities for Regional Partnership.” Edited by Bonnie S. Glaser and Matthew P. Funaiole. *Perspectives on Taiwan: Insights from the 2018 Taiwan-U.S. Policy Program*. Center for Strategic and International Studies (CSIS), 2019. http://www.jstor.org/stable/resrep22549.5.

national security. A national information and communication security taskforce of the Executive Yuan will continue implementing Phase Five of the National Cyber Security Program (2017-2020) to respond to international trends and new forms of cyberattacks and threats as well as to strengthen Taiwan's cyber security capacity and advantage based on its existing defense foundations. To gradually increase Taiwan's cybersecurity cyber defense capacity and set goals for the government to promote cyber security defense strategies and plans, the National Cyber Security Program of Taiwan (2021-2024) (Phase Six Development Program) was announced on February 23, 2021. The Phase Six Development Program aims to cultivate excellent cybersecurity talent within the country, improve cybersecurity defense measures for critical infrastructure, and employ innovative technology to prevent and eliminate threats at their source in a proactive manner. The Phase Six Development Program aims to create a resilient, secure, innovative country by promoting businesses' cyber security awareness and capacities.

As part of the program, three primary policy goals are incorporated, including "establishing an active defense base network establishing a hub for cyber security research and training in Asia-Pacific,and establishing a safe network environment by collaborating with public and private sectors"[22] as well as the four major strategies of recruiting global top talent, cultivating autonomous development capacities. Public and private governance must be promoted, critical infrastructures should be strengthened, intelligent, innovative technology should be utilized to defend against potential threats actively, and general defense capacity should be enhanced by

[22] Pryor, Crystal D., Tania Garcia-Millan, Jeffrey Gelman, Tanvi Madan, Scott Moore, Crystal Pryor, Lisa Reijula, et al. "Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership." Edited by Bonnie S. Glaser and Matthew P. Funaiole. *Perspectives on Taiwan: Insights from the 2018 Taiwan-U.S. Policy Program*. Center for Strategic and International Studies (CSIS), 2019. http://www.jstor.org/stable/resrep22549.5.

establishing a secure and intelligent network.

The government hopes to develop a safe and resilient innovative country by integrating outstanding cyber security industry development programs for the six core strategic sectors as cyber security industry development continues.

METHODOLOGY

Research Process

In selecting and analyzing the content to discuss, this study applied the Critical Incident Technique (CIT) to determine the significance of the cybersecurity threat to Taiwan's national security and to verify the urgency of coordinating Taiwan's responses. The following section will examine Taiwanese-managed detection and response efforts undertaken by the private sector and the government. Parallel to this, this study explores in terms of qualitative content analysis the real challenges and threats the European Union has faced, how its response has already culminated in a coordinated policy enforcing strategy, and how ENISA and Taiwan’s Cybersecurity Section are laying the groundwork for the defense about these cybersecurity threats from abroad, acting as an international reference, and for the objective of this study, finding synergies and differences with its Taiwanese counterpart. Based on the National Cyber Security Program of Taiwan (2021-2024) as an example of Taiwanese response to the real threats to the country, and the recently inaugurated Ministry of Digital Affairs, this study intends to examine Taiwan's cybersecurity response at the national level. Further, I intend to analyze recent cybersecurity attacks against Taiwan and the European Union, using the International Forum of Incident Response & Security Teams (FIRST) to verify sources of information and database acknowledgment.

To create recommendations for the Taiwanese counterpart, as well as further knowledge for the European side, this study examines and analyzes ENISA's actions and how it prevents and anticipates security threats, evaluating which variables are similar and applicable in both countries

DATA ANALYSIS

European Union's Policy-Making in Cybersecurity

Even though the European Union (EU) has long been involved in the field of computer security and electronic communications (European Commission, 1993; Council of the European Union, 1997), it was within the last decade that it took deliberate steps to establish a comprehensive approach to cyber security. Cyber-attacks on individuals, companies, and critical infrastructure are on the rise. The European discourse has gradually begun to reflect that society's reliance on technology constitutes a rapidly growing security risk that requires appropriate mitigation (European Commission, 2001). Consequently, the European Union attempted to assume a cooperative support role in cyber security.

As cyberspace and cybercriminals are not subject to national borders, the European Union presented itself as the most logical and efficient approach to addressing the Member States' challenges in addressing cyber security threats (Council of the European Union, 2005). In response to attacks against information systems, the Council adopted an Action Plan on Attacks against Information Systems in 2005[23], and Europol set up the European Cybercrime Centre (EC3) in 2013.

For the EU's cyber security policy, coherence has become particularly crucial

[23] Commission , European. "Digital Inclusion." Shaping Europe's digital future, June 2022. https://digital-strategy.ec.europa.eu/en/policies/digital-inclusion.

because, for long periods, its governance was highly fragmented, with relevant actors working independently in distinct areas such as law enforcement, critical infrastructure protection, and defense. Due to the pursuit of policy coherence and the constant increase in cyber security attacks on essential infrastructures of information as well as on personal and commercial data, the European Commission and the Human Rights Council of the EU published their first cyber security strategy in 2013 (European Commission and HREU, 2013). The plan aims at improving member states and the private sector's resilience to cyber threats by fostering more coordination between all stakeholders, promoting more significant investments in national and private sector capabilities to respond to attacks, further developing cyber defense capabilities, and engaging with international partners.

During the European Council of October 2017, the EU announced its commitment to increase the implementation of its Cyber Security Strategy and ensure the coherence of its Cyber Security Policy (European Council, 2017). Following this decision, the EU will acquire a more significant role in this area and streamline the application of a common approach across all member states. In particular, the EU plans to upgrade the mandate of the European Agency for cyber security (ENISA), making it into the core of action-planning and response for the Union, and create a scheme for cyber security certifications. The Council of the European Union had approved the Cyber Diplomacy Toolbox a few months earlier, in June 2017 (Council of the European Union, 2017). This toolbox aims to strengthen the EU's activities in this area and enhance a coordinated response in case of cyber-attack on European targets.

Despite these efforts, after my study regarding the current response linked to its background, several external problems remain: externally, there is a lack of public

awareness of cyber security risks; the private sector has a limited capacity to respond to incidents; a rapid expansion of the tools available for cybercriminals; and attribution remains a challenge. On the internal front, insufficient progress has been made concerning countering institutional fragmentation, defining what resilience is, how it is achieved, advancing toward binding legal regimes, and ensuring adequate funding levels.

Regarding the specifics of ENISA, its primary function and work are actively supporting the Member States, Union institutions, bodies, offices, and agencies in improving cybersecurity; ENISA aims to achieve a high standard level of cybersecurity across the Union. The work they do involves developing and implementing policies, building capacity and readiness, facilitating operational cooperation at the Union level, enhancing the trustworthiness of ICT products, services, and processes by implementing cybersecurity certification schemes, promoting knowledge sharing, research, innovation, and awareness, and fostering cross-border communities.

In 2020, the European Commission and the High Representative presented a new EU Cybersecurity Strategy. In addition to hospitals, energy grids, and railways, the Strategy also covers the security of essential services. European homes, offices, and factories are becoming increasingly connected, which poses a security risk.

As part of the Cybersecurity Strategy, the EU will build collective capabilities to respond to major cyberattacks and work with partners around the world to ensure international security and stability in cyberspace. Using the EU and Member States' collective resources and expertise, a Joint Cyber Unit can respond effectively to cyber threats.

Cybersecurity threats are almost always cross-border, and a cyberattack on a

critical facility in one country can affect the entire EU. A strong government agency is necessary for EU countries to oversee cybersecurity and to share information with their counterparts in other member states. The importance of this is particularly evident in sectors that are critical to the well-being of our society.

By the NIS Directive, which all countries have now adopted, such government bodies will be created and will cooperate. At the end of 2020, this Directive was reviewed. Following the review process, the Commission presented a proposal on 16 December 2020 for a Directive on measures to ensure a high level of cybersecurity across the Union (NIS2 Directive).

As the last point, it is also essential to state its vision toward external cybercrime. Several measures are protecting cyber threats originating outside the EU's borders[24]. The European External Action Service and member states (the 'cyber diplomacy toolbox) develop a joint diplomatic response to malicious cyber activities. As part of this response, the EU has initiated diplomatic cooperation and dialogue, taken preventive measures against cyberattacks, and imposed sanctions against those responsible for cyberattacks that threaten the EU.

In the event of external cyber threats, the Commission assists in decision-making on how to respond. While cooperation and sharing of intel for cyber responses are at the core of such potential measures, different challenges and threats remain a threat to the entire Union. In order to increase the veracity of the real capabilities of the EU in terms of cyber cooperation and response, this section needs to be followed up on the current events within the EU for further validation and confirmation.

[24] Commission, European. "Online Privacy and Safety." Shaping Europe's digital future, 2022. https://digital-strategy.ec.europa.eu/en/policies/online-privacy.

Taiwan’s Potential Cybersecurity Vulnerability

In recent years, Taiwan has implemented a cybersecurity policy to create a hub of cybersecurity start-ups worldwide. The four effective strategies can be summarized as follows:

- Developing a cybersecurity training system based on demand
- Consolidating the niche market
- Establishing international partnerships
- Selecting test sites for new products

Taiwan occupies a unique position in the international arena in politics and economics. Taiwan's public and private sectors are exposed to the most significant cybersecurity risks posed by China. It has been reported that, according to the director of the American Institute in Taiwan, when the United States and Taiwan jointly conducted the Large-scale Cyber Defense Exercise in November 2019, China's cyberattacks on Taiwan's technology industry increased by seven times in 2018 and by twenty times in 2019. In addition, the Vice Premier of the Executive Yuan of Taiwan pointed out that China is responsible for 60% of the 30 million cyberattacks against Taiwan each month.

Ransomware and advanced persistent threats (APTs) have targeted Taiwan in recent years. In recent months, several data breaches have resulted in hundreds of thousands of personal data being stolen and improperly sold.

Despite the fact that it is impossible to defend against various cyberattack methodologies, Taiwan's government, medical institutions, and service providers have become increasingly aware of the need for cybersecurity protection. Despite the threat of significant losses of profits, government and private organizations have become

more concerned about cybersecurity protection. Cybersecurity has become an integral part of national policy; industries have also stepped up their investment in the field and increased recruitment of cybersecurity talent; additionally, all significant stakeholders have given greater attention to the cybersecurity sector and protection technologies.

A review of the major cyber attacks incidents over the years of 2018/2019 is shown in Table 1, along with how these incidents led private and public sectors to coordinate in solving, preventing, and forecasting future attacks.

Table 1 Major Cyber Security Incidents occurred in Taiwan (2018 -2019)

Date	Way of Attack	Major Incident
2019/08	Ransomware	Hosts in the Ministry of Health and Welfare, large hospitals, and medical clinics were hacked. Important data such as patient profiles, staff rosters, medical images, and medical records were locked by encryption viruses. More than 55 medical institutions were the victims of the incident.
2019/07	Taking control of the server by malware upload	The database of 1111 Job Bank was hacked, resulting in the leak of 200,000 job seekers' personal data such as ID number, name, birthday, e-mail, phone number, address, and company.
2019/06	Taking control of the server by malware upload	590,000 personal data such as ID number, name, agency, job number, and job title were leaked from the Ministry of Civil Service and exposed on the foreign websites, affecting 243,376 people.
2019/04	APT	ASUS's automatic software update tool server was hacked, and the number of affected users worldwide may exceed 1 million.
2018/08	Malware	TSMC was attacked by the wannacry virus, which caused the production line to shut down and lost TWD 2.6 billion.
2018/08	Creating accounts with administrative rights after implanting backdoors	More than 2.98 million personal data of the citizens in Taipei were leaked and sold on a foreign forum.

Source[25]: Ministry of Digital Affairs (Taiwan)

[25] Digital Affairs, Ministry of. "Cyber Security Policies and Regulations-Operations | Administration for Cyber Security, Moda." Ministry of Digital Affairs(open in new window), 2022. https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648.

In an effort to promote the development of Taiwan's cybersecurity industry, Taiwan's Ministry of Economic Affairs has taken a series of measures that will hopefully enhance the growth of this sector. Accordingly, factors such as the perspective of talent, the market, technology, standards, and the environment are key elements for Taiwanese regulatory frameworks. In addition, a cybersecurity service team has been established to help small and medium enterprises diagnose and match their products with market demands. A study by Taiwan's National Cyber Security Centre[26] suggests that Taiwan's top three industries (manufacturing, banking, and health care) have basic capabilities to prevent cyberattacks but have no advanced capabilities and require cybersecurity awareness and training. NT$49.34 billion was the output value of Taiwan's cybersecurity industry in 2019[27], increasing 12.3% over 2018. Statistics indicate that there are eight subsectors in the cybersecurity industry: endpoint and mobile device security, network security, data, cloud application security, Internet of Things security, cybersecurity operations management services, cybersecurity testing, identification, and consulting services.

Concerning the specific regulation-making process and national response mechanism regarding the aforementioned threats, the National Security Council, under the President's instructions (Lee Teng-hui), the National Security Council announced the "Building Taiwan's Communication and Information Infrastructure Security Mechanism" proposal in May 2000 to coordinate and accelerate the building of Taiwan's cyber security infrastructure, strengthening cybersecurity capacities. On Aug. 30, 2000, the President approved the proposal and sent it to the Executive Yuan

[26] Wu, Benson. "Taiwan Sees Its Cyber Capabilities as the Hard Reality of Soft Power." The National Bureau of Asian Research (NBR), March 20, 2019. https://www.nbr.org/publication/taiwan-sees-its-cyber-capabilities-as-the-hard-reality-of-soft-power/.
[27] Commission of, the European Union. "GDPR Archives." GDPR.eu, May 25, 2018. https://gdpr.eu/tag/gdpr/.

for planning. To promote Taiwan's cyber security infrastructure building, the Executive Yuan gathered ministries and councils in September 2000 to discuss relevant plans over twelve meetings, passing the Phase One "Cyber Security Mechanism Plan" and establishing the "National Information and Communication Security Task Force" (NICST).

The digital economy has redefined global industrial structures in recent years as industries develop across generations, borders, fields, and realities. As the digital economy and the Internet of Things (IoT) emerge, a new national security development program phase must be based on digital national security and cyber security as the digital economy and the Internet of Things (IoT) emerge. It is necessary to create a comprehensive industry ecosystem to build an industry ecosystem, accelerate innovation, optimize industry structure, and comply with cyber and national security policies.

A NICST Executive Yuan initiative was proposed to build a secure and trustworthy digital nation based on its vision of the "National Cyber Security Program (2017-2020)", under the instructions of incumbent President Dr. Tsai Ing-wen. It aims to create a national cyber security joint defense system, improve security defense mechanisms overall, and strengthen cyber security autonomy[28].

Cyber security plays an essential role in Taiwan's national security and even various aspects of socio-economic activities due to the wide breadth of information and communication applications. By gradually enhancing and expanding Taiwan's cyber security defense capability and advantage based on the existing defense foundation in response to international trends and new forms of cyber-attacks and threats, the NICST continues to implement Phase Five of the National Cyber Security

[28] Policies, MODA. “Major Policies | Ministry of Digital Affairs.” Major Policies | Ministry of Digital Affairs, page 368, 2022. https://moda.gov.tw/en/majorpolicies/368.

Program (2017-2020). In addition to proposing a goal for the government to follow when promoting cyber security defense strategies and plans, the "National Cyber Security Program of Taiwan (2021-2024)" was also introduced.

As a final point, it is important to consider the cyber consequences of the events of summer 2022 on Taiwan's cybersecurity defense and strategy.

According to available data on cyber attacks[29] this study has found that Taiwan has been the most targeted nation for foreign disinformation for the past nine years. According to Taiwanese politicians and researchers, many of those attacks originate in China.

Prior to Nancy Pelosi visiting Taiwan in August, cyberattacks on the small island spiked as hacking attempts and misinformation spread through popular social media platforms, such as Facebook, YouTube, and LINE, a popular instant messaging app in Taiwan.

Cybersecurity responsibility for the presidential office and national defense ministry websites is at Level A. In addition, the government's Web sites will be inspected round-the-clock by Executive Yuan's cybersecurity department.

Government officials closely monitor the situation, as targets and means of cyberattacks change daily. In the past few months, government agencies have reported increasing cyberattacks. However, it has been said during regular information security drills, protocols were developed that prevented significant damage. In June and last, Taiwan Power Co reported 4.9 million cyberattacks .In response to several users reporting that the Web site of Taiwan Taoyuan International Airport took longer to open than usual yesterday, hackers are alleged to have attacked the area.

[29] & Infrastructure Security Agency, Cybersecurity. "Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization." CISA, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-277a.

A statement from Taoyuan International Airport Corp said the airport's official website's Internet connection has been unstable on August 5th 2022. Taiwan Railways Administration's Xinzuoying Station and some 7-Eleven convenience stores were also hacked before Pelosi arrived, displaying messages in simplified Chinese characters pleading for her departure.

As Taiwan's cyber defense and response capability appears to be significantly more vulnerable as a result of the current situation over the past few months and throughout 2022. The entire Taiwanese cyber infrastructure must take stronger and cooperative action, and the timing is critical.

Specifics of Taiwanese Cybersecurity Challenges

A comprehensive analysis of a wide range of data related to incidents that occurred in Taiwan's cybersecurity field has revealed several weaknesses that must be addressed and resolved to strengthen the nation's cybersecurity capability intertwined with its industrial sector.

a. There is a small scale and output value:

A good cybersecurity ecosystem is required. The scale and output value of Taiwan’s cybersecurity industry are still small. Small and medium businesses constitute the majority of cybersecurity companies with the capacity for R&D. Financial institutions, high-tech companies, and large organizations import cybersecurity products due to difficulty competing with major international corporations. Consequently, Taiwan's cybersecurity industry has difficulty developing on a long-term basis. A sound environment for developing Taiwan's cybersecurity industry requires *government support in terms of market, technology, and talent.*

b. Businesses lack cybersecurity awareness:

As Taiwan's ICT industry develops products and services, it considers costs and the lack of "Security Inside," which hinders the overseas sale of Taiwanese ICT products since privacy concerns are involved. According to the Federal Trade Commission, HTC, Asus30, and D-Link do not offer adequate privacy protection and cybersecurity protection for their products[30]; in addition, enterprises do not receive adequate cybersecurity training and have no incentive to develop cybersecurity products. Most Taiwanese enterprises still view cybersecurity products as "nice to have.", as mentioned in the Background section. Companies that provide cybersecurity products need to make *significant efforts to promote cybersecurity products* and raise cybersecurity awareness within the company.

c. Small and medium enterprises dominate Taiwan's cyber security industry:

These types of companies have limited international marketing resources. Taiwan has a large number of small and medium-sized companies involved in cyber security. Nearly 60% of Taiwan's cyber security companies had annual revenues below NT$100 million and lacked international marketing resources as of 2016[31]. Approximately 35% of the companies export their products to China, Malaysia, the United States, Japan, and Singapore. Start-ups drive Taiwan's cybersecurity industry. However, the venture capital market pays little attention to these start-ups, and these companies cannot expand their customer base and generate revenues. In general, *Taiwan's cybersecurity industry does not have sufficient marketing resources.* A key

[30] Information, Security Management. “Asus Corporate Social Responsibility.” ASUS Corporate Social Responsibility, 2022. https://csr.asus.com/english/article.aspx?id=1741.
[31] Ocean, Report. “Cyber Security Market Growth Analysis by Revenue, Size, Share, Scenario on Latest Trends, Types and Applications: Taiwan News: 2022-02-18 05:49:33.” Taiwan News. Taiwan News, February 17, 2022. https://www.taiwannews.com.tw/en/news/4447491.

issue for Taiwan's cybersecurity industry is assistance with developing export strategies and strengthening connections with international markets.

d. The cybersecurity ecosystem lacks standards and sites:

Consequently, Taiwanese cybersecurity products lack adequate capability and maturity as a result of a lack of domestic large-scale cyber attack defense test sites, which prevents practical evaluation of the level of cybersecurity and competitiveness with international competitors; also, *Taiwanese cybersecurity products are vulnerable to privacy breaches and foreign penalties* due to a lack of standards, test specifications, and comprehensive cybersecurity inspection and certification systems.

e. There is a shortage of critical technologies and professionals:

R&D of crucial cybersecurity technologies requires a considerable amount of human resources and time[32]; domestic cybersecurity companies are currently small and lack sufficient resources, making it challenging to fund the R&D of key cybersecurity technologies. In addition, cybersecurity protection systems are still in their infancy stages of development; Internet of Things security and critical infrastructure security are still in their infancy stages. *It is necessary to conduct testing at testing sites in order to achieve their results.*

[32] Hsin-fang, Lee. "Information Security: At Least 900 Cybersecurity Jobs Need to Be Filled to Combat Chinese Espionage." Taipei Times, April 5, 2021. https://www.taipeitimes.com/News/taiwan/archives/2021/04/06/2003755174.

National Cybersecurity Program of Taiwan and MODA

The Legislative Yuan of Taiwan passed the Cybersecurity Management Law on May 11, 2018. As part of its commitment to cybersecurity under the policy "Cyber Security is National Security[33]" This law mandates cybersecurity requirements for Taiwan's government agencies and operators of critical infrastructures. As part of this push, the administration is also working to develop Taiwan's indigenous cybersecurity industry through a policy of cyber autonomy.

An "autonomous" domestic cybersecurity industry is one impetus for building up an "autonomous" domestic defense industry in response to an uncertain international cyber technology transfer environment and the apparent threat from China. DPP think tank New Frontier Foundation identified cyber security as one of Taiwan's "Core Defense Industries" or CDI, along with aerospace and shipbuilding.

To assist Taiwan's cybersecurity industry and create a local market for cyber products, Taiwan's Ministry of Defense opened its cybersecurity contracts to small and medium-sized companies.

Taiwanese President Dr. Tsai Ing-wen herself enlisted the private sector as early as 2016 to support Taiwan's national defense. Speaking at Taiwan's Hacks in Taiwan Conference (HITCON), a gathering of Taiwan's hacker community, she discussed how "hacker spirit" can support her government's goal of elevating cybersecurity to a national priority.

In response to the Tsai administration's commitment to cyber autonomy and its promise for additional funding, the Ministry of Foreign Affairs (MODA) has

[33] Digital Affairs (R.O.C.) , Minister of. “Cyber Security Policies and Regulations-Operations | Administration for Cyber Security, Moda.” Ministry of Digital Affairs(open in new window), 2022. https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648.

established a practical and legal Department for National Cyberdefense. In terms of these efforts, the Executive Yuan, MODA, has led several tracks to some success. It will be necessary for MODA to take a whole-market approach and a targeted industry approach to simultaneously help Taiwan's cyber firms become globally competitive and defend against Chinese and other cyber threats.

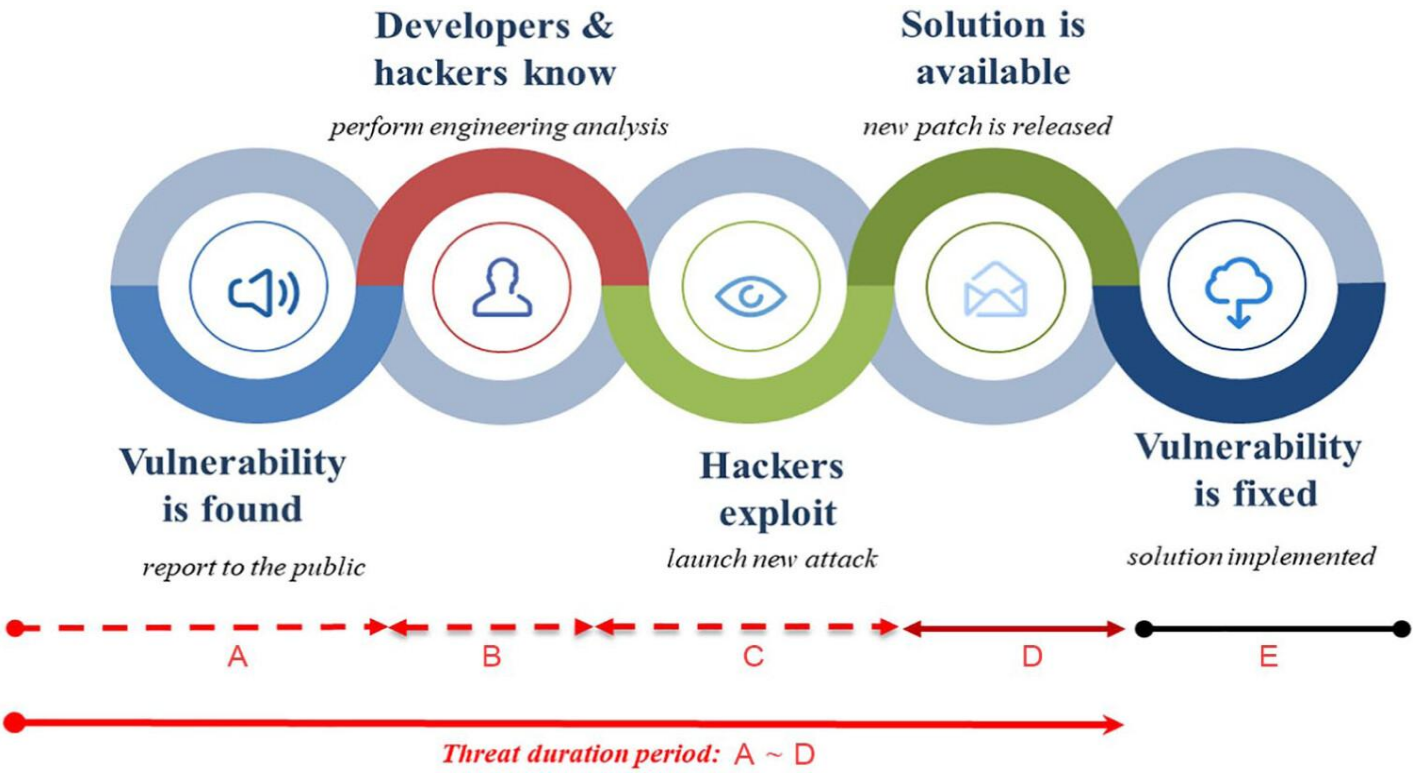
It may be possible for Taiwan's cybersecurity industry to develop a local market through cyber autonomy. However, MODA's cyber funding may be limited in the market, and Taiwan's cyber firms still face tough competition internationally. According to both Taiwan's public and private sectors, Taiwan's unique threat environment contributes to developing an autonomous, competitive industry through acquiring expertise in a wide range of cyber tactics, techniques, and procedures. However, it is unclear if this environment will apply to the needs of the rest of the world, and for the extension of this study, to the European Union.

To counter China's concerted cyber attack, a coordinated and determined interagency response is necessary, and MODA policy-making and actions are still in their infancy. To protect Taiwan's "digital territory[34]" Taiwan's private cybersecurity sector must be mobilized to protect government agencies, private companies, the military, and other sectors. *This study foresees that its forward Master's Degree Thesis will follow up on the issue over the course of the national response.*

The following Figure 1 shows the time span of threat and detection for both Taiwanese and EU's vulnerability detection and response.

[34] Taiwan , Country Commercial Guide. "Taiwan - Information and Telecommunications Technology." International Trade Administration | Trade.gov, 2022. https://www.trade.gov/country-commercial-guides/taiwan-information-and-telecommunications-technology.

Figure 1 Zero-day threats lifespan: (A) Few know, (B) Many know, (C) Window period, self-defense period, (D) Update is available, and (E) Update is implemented.



Source[35]*: SAGE Journal*

In response to ongoing cyber threats, Taiwan should adjusts its long-term strategy every four years. This will ensure that the state's cyber security policy moves steadily toward a better future by setting appropriate cyber security policies and horizontal goals. However, Taiwan's strategy needs to be sufficiently general to allow the structures and legal regulations to function well. According to a detailed analysis of the government's cyber defense actions, the capability of responding to APTs has been significantly increased, NICST prevention-oriented response has increased, and

[35] Huang, K.-J., & Chiang, K.-H. (2021). Toward a Self-Adaptive Cyberdefense Framework in Organization. SAGE Open, 11(1). https://doi-org.wenzao.idm.oclc.org/10.1177/2158244020988855

a digital and logistic infrastructure, coordinated by MODA and the Ministry of Defense, is being developed. Through the course of this study, good signals of positive development have been encountered and followed.

SPECIFICS OF EU CYBERSECURITY DETECTED FLAWS

New products and services have been introduced into our daily lives due to the advent of technology. As a result, cybercrime and cyberattacks are increasing, having an increasing economic and societal impact. Since 2017, the EU has been accelerating efforts to strengthen cybersecurity and digital autonomy at a critical time.

As part of my study, I examine EU cybersecurity policy, cybercrime and cyber defense, as well as efforts to combat disinformation. This study has identified 3 major challenges that threaten the EU cyber defense strategy: digital single market, strengthening a network and information security, and fighting cybercrime.

Table 2 shows the examples and challenges found for the current EU cybersecurity policy.

Table 2 Detected Flaws in EU Cybersecurity Policy

POLICY AREAS	EXAMPLES
Digital Single Market	• It is difficult to enforce legal remedies in EU Member States since duties of care are governed by diverse legal frameworks, which causes legal uncertainty and difficulty enforcing legal remedies. • In the EU, there is no overarching legal framework for software vulnerability disclosures, which would enable a coordinated approach.

Strengthening a network and information security	• There is no restriction on member states, including sectors not covered by the NIS Directive. Other crimes, such as human trafficking and illegal immigration, can be committed through the accommodation industry, which is not covered.
Fighting cybercrime	• The national legislation of many Member States does not define e-evidence. • In addition to avoiding non-cash payment fraud, the current framework decision excludes virtual currencies, e-money, mobile money, phishing, skimming, and the possession and sharing of payer information.

Source[36]: European Union, Data Protection Office.

It is important to note that as a result of these outlined challenges and potential corrections to correct operability in cybersecurity defense, we should focus on the external sharing of information and the increased international cooperation that will help to establish a global framework where the capability of improving in this regard lies. A key factor that plays into the success of the cooperative effort between the EU and the Taiwanese counterpart is the importance of timing and the urgency of setting a unified legislative framework.

[36] Ho, Kah-Kin. "Cybersecurity: The Strategic View." Edited by Damien D. Cheong. *Cybersecurity: Some Critical Insights and Perspectives*. S. Rajaratnam School of International Studies, 2014. http://www.jstor.org/stable/resrep05892.4.

Taiwan & EU Potential Capability for Cooperation

Taiwan and the EU are focused on expanding their markets, collaborating on technology, and exchanging policies. The partnership has recently increased in innovative areas such as circular economy, smart cities, offshore wind, photonics, cybersecurity, startups, and semiconductors.

Cybersecurity cooperation between Taiwan and the EU is still developing, and both parties are exploring suitable cooperation models. The currently active communication between cybersecurity companies in Taiwan and the EU about possible cooperation has started to materialize into the signing by Taiwan of the Joint Declaration on Privacy and the Protection of Personal Data on October 8th, 2022. Regarding legislation concerning economy, trade, and business cooperation, the Taiwanese government is optimistic and open to international collaboration and connection, and it has supported local industries through legislation. However, it is essential to note that Eastern and Western cultures differ; Taiwan remains a particular political entity for international organizations. These factors will affect Taiwan and the EU's bilateral cooperation to varying degrees.

Eastern and Western countries may have different business habits, especially in establishing cooperation models. Traditionally, business people placed great importance on interpersonal relationships and trusted each other. Verbal agreements were more common than written agreements in those days. Communication and confirmation costs will likely increase as Western companies struggle to adapt and accept this. Due to globalization, Taiwanese companies have tended to adopt or follow Western business culture, including contract formulation and signing.

Since Taiwan is not a member of the United Nations, it faces potential

diplomatic obstacles. Establishing diplomatic relations has been relatively complex for a long time, and China has repeatedly pressured countries worldwide, including Taiwan, to intensify restrictions on Taiwan's prudent development. Applicants are even rejected from international non-profit organizations that are not politically or economically related. It is also challenging to achieve a country's ideal goals when dealing with issues of cooperation with Taiwan due to very conservative and cautious attitudes. Currently, informal contact and communication are taking place.

The Taiwanese government maintains a positive and open attitude toward developing cyber security. It is optimistic that Taiwanese cyber security companies will be able to take advantage of any domestic or foreign cooperation opportunities, whether joint R&D of technology and products or joint market expansion. However, Taiwan and the EU still need help in their bilateral cyber security cooperation. As both parties' domestic markets are pretty limited, it would be inappropriate to see occupying each other's market as the ultimate goal of collaboration so as not to fall into the zero-sum trap. Risk factors associated with R&D cooperation include personal protection, homogeneous competition, trust, patents, and ownership of achievements. Collaborative opportunities will be hard to find if the perspectives are not complementary. Following intensive analysis of synergy and coincident points of collaboration and scenarios between the two parties, the following points have been decoupled from their current collaboration and those that might occur in the future.

1. **Expansion of markets:**
    a. Taiwan and the EU can expand their domestic markets bilaterally to supplement regional marketing. Both parties are Global EPIC members, allowing them to discuss and work together to develop profitable products and services and

explore potential opportunities in the EU market. Moreover, by introducing each other's products, Taiwan and the EU can offer more choices based on bilateral market demand gaps.

2. **Collaboration in technology:**
    a. The EU has one of the most advanced cybersecurity technologies in the world. By comparing their respective cybersecurity technologies, Taiwan and the EU could develop total solutions that complement each other.
3. **Exchange of policies:**
    a. Security issues such as IoT security, 5G security, and supply chain security are shared by Taiwan and the EU, as well as common security standards for products and technologies. After entering a partnership, both parties may share details about their standardization processes, policies, and leading pilots.
4. **Contactless economy:**
    a. World health has been adversely affected by the COVID-19 epidemic. People are seeking to suppress the spread of the epidemic by adopting the "contactless economy.". People want to work from home, attend online meetings, take courses online, receive digital health care, and make payments digitally. Automated warehousing, smart manufacturing, and service robots are other areas that have growth potential. Companies from foreign countries may invest in Taiwan or work with

Taiwanese companies to explore "contactless economy[37]" business opportunities. Innovative IoT applications are developed using Taiwan's ICT, machinery, and medical equipment industries.

5. **Taiwanese IoT successful system working as a reference for cooperation:**

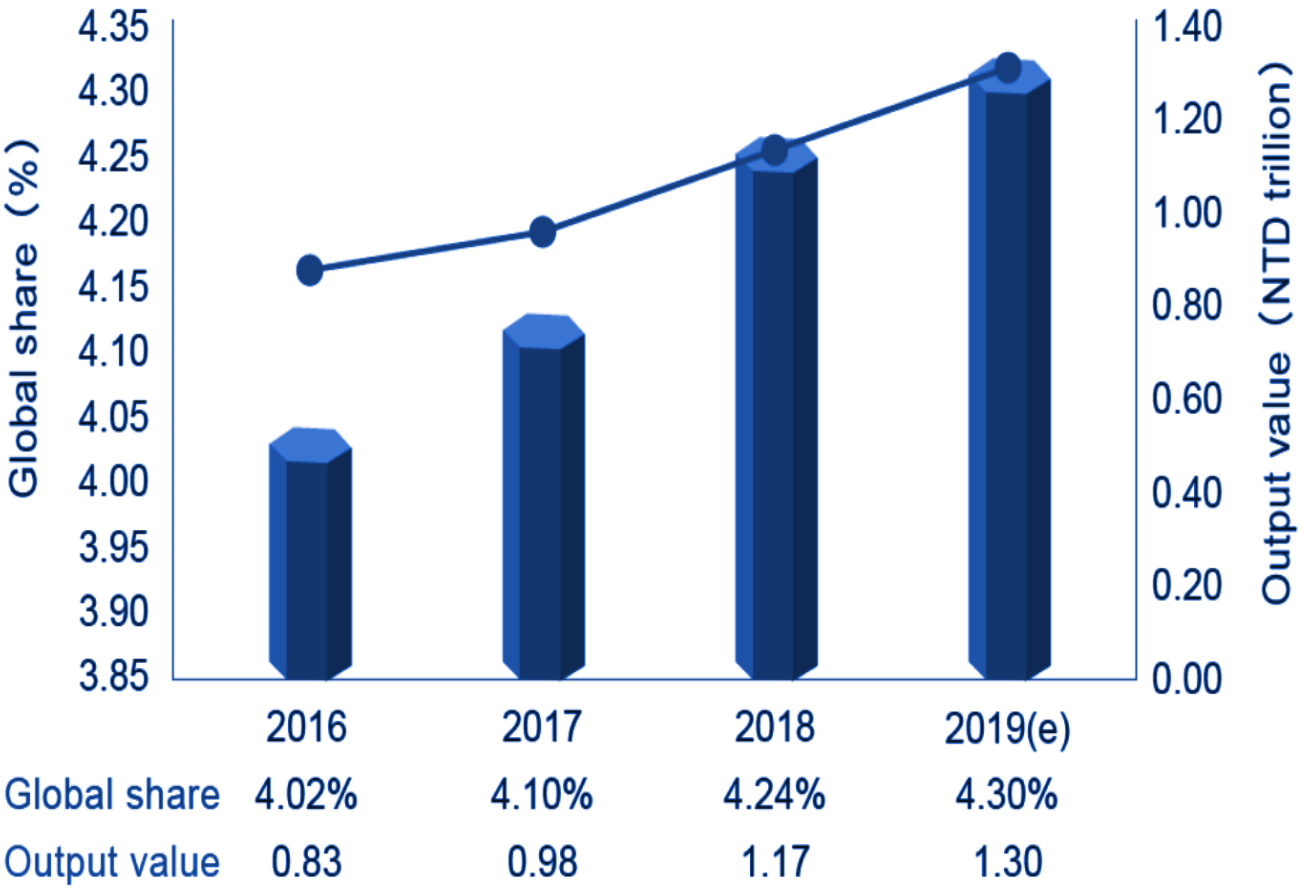
   a. To promote cross-disciplinary cooperation and create industry standards, the Taiwan government established the "Major League IoT, ASVDP" in 2016. Several Special Interest Groups (SIGs) have been formed within the League, including one for smart transportation, another for smart logistics, one for smart manufacturing, one for smart energy efficiency and environmental monitoring, one for smart commerce, one for smart homes, one for smart farming, one for smart healthcare, and one for the security of IoT data. In 2018, Taiwan's IoT industry generated $1.1 billion, surpassing the NT$1 trillion mark for the first time and accounting for 4.24% of global output value, up from $0.83 trillion in 2016[38]. Additionally, Taiwan is close to emerging markets in Asia, has a complete semiconductor supply chain, and has abundant engineering talent. The semiconductor and ICT industries in Taiwan can be strengthened by foreign investment.

[37] Mehrotra, Mohit. "Contactless Economy: Deloitte Sea: Consulting." Deloitte, September 11, 2020. https://www2.deloitte.com/gu/en/pages/strategy/articles/contactless-economy.html.

[38] MOEA, Industrial Development Bureau. "Contact Taiwan." Contact TAIWAN-Key Industries--The Internet of Things, October 7, 2022. https://contacttaiwan.tw/main/docdetail.aspx?uid=1078&pid=727&docid=11158.

As shown in Figure 1, Taiwan has global solid relevance in the IoT industry, a potential pillar for EU-Taiwan cooperation.

Figure 2 Global output value of Taiwanese IoT industry (2016-2019)



Source[39]*: Industrial Development Bureau, MOEA*

In terms of policy-action and government cooperation, Taiwan recently adopted the Joint Declaration on Privacy on October 8th, 2022, and the EU released central cyber policy and data protection regulations, resulting in a stronger

[39] Wang, Vincent Wei-cheng. "Developing the Information Industry in Taiwan: Entrepreneurial State, Guerrilla Capitalists, and Accommodative Technologists." *Pacific Affairs* 68, no. 4 (1995): 551–76. https://doi.org/10.2307/2761276.

relationship between the two countries. It commits signatories to support and advance international policy discussions and cooperation across the Indo-Pacific region, Europe, and beyond regarding cross-border data flows. The European External Action Service (EEAS) plans to promote lawfulness, fairness, transparency, and the rights of individuals in the public and private sectors through comprehensive legal frameworks and policies.

Taiwan joins the declaration to promote a safe and secure environment for exchanging personal data with international partners. At the same time, it fosters a mutual exchange of information and support regarding digital affairs, coordinated by ENISA for the EU side and MODA for the Taiwanese side.

CONCLUSION

The EU and Taiwan are significant economic and trade gateways in their respective regions. Startups in the cybersecurity industry can collaborate to enter surrounding markets by assisting each other in landing in their separate areas.

Among the Asia-Pacific region's cybersecurity hubs, Taiwan occupies a prominent position. EU cybersecurity companies that land in Taiwan will have the opportunity to expand their Asia-Pacific market; similarly, Taiwanese technology companies will have the chance to gain access to the European market through the adhesion to stronger cyber cooperation.

In contrast to their Chinese or American counterparts, Taiwanese cybersecurity companies can use their cooperation experience to advance into the European market and consolidate a stronger position, demonstrating relevant differences in Taiwanese cyber threats and cyber responses throughout the analysis.

Taiwan's and the EU's cybersecurity industries are similar in that domestic

demand is relatively small, and most cybersecurity companies are small and medium-sized; both are also at the intersection of regional cyberattacks, which is surprising given the size of both sides' manufacturing and technology capabilities.

Cybersecurity start-ups thrive in an environment with well-established ICT infrastructure. Regarding cybersecurity products and technologies, Taiwan and the EU have a strong potential for cooperation, already started by Taiwan joining the Joint Declaration on Privacy on October 8th, 2022. Taiwanese companies have the advantage of hardware cyber security platforms and threat intelligence. In contrast, European companies benefit from cybersecurity intelligence, infrastructure management, and monitoring, as well as a long track record in coordinated cyber response compared to their Taiwanese counterparts.

Cybersecurity companies from Taiwan and the EU can enter adjacent markets by sharing threat intelligence. For example, there are sometimes differences in cybersecurity threats across different regions. As a result of bilateral cooperation between Taiwan and the EU, Taiwan can fully share intelligence and control cyberattack patterns to achieve real-time protection. Furthermore, there is also the possibility of combining Taiwanese network hardware with EU software applications to accomplish this.

Despite its lack of sound IoT security regulations, Taiwan is very successful at promoting individual IoT products, such as video surveillance security standards and certifications. The "IoT Security Industry Standards[40]" were promulgated to promote international exchange in English. Consequently, to lead an effective cyber response, a high level of cooperation and information sharing between public and

[40] Information Security Office 資通安全處. “National Cyber Security Program of Taiwan (2021 to 2024).” 中文版(Open New Window), 2021. https://nicst.ey.gov.tw/en/FD815304EBFFE6FC/639d32e8-2a07-40da-b033-bc6c95d015ce.

private entities is needed, a problem that has just been well addressed.

In conclusion, this study affirmatively and strongly finds POSITIVE deeper cooperation between Taiwan and the EU concerning cyber security threats as a result of this extensive analysis, which serves as the first step towards a further and deeper research project programmed for a Master's thesis. In the section on recommendations, specific areas for further cooperation are described.

RECOMMENDATIONS

A series of strategies and models for Taiwan-EU cooperation are presented in Table 3 on the basis of government cooperation, information sharing, and matching of businesses.

Table 3 Proposed Strategies for EU - Taiwan Cyber Cooperation

Aspect of Cooperation	Area of Integration	Proposed Strategies
Public Sector	Industrial Development, Security Standards and Certifications	• Taiwan's IoT standard as a model[41]. • Taiwan successfully promotes cybersecurity standards for video surveillance systems. • IoT Security Industry Standards.
Public Sector	Testing and Conferences Promotion	• Taiwan's Cybersec 2022

[41] MOEA, Industrial Development Bureau. "Contact Taiwan." Contact TAIWAN-Key Industries--The Internet of Things, October 7, 2022. https://contacttaiwan.tw/main/docdetail.aspx?uid=1078&pid=727&docid=11158.

		Successful Conference ● Netherland's Hack the Hague successful conference ● Private and public cybersecurity solutions should be tested in Taiwan and the EU.
Private Mutual Coordination	Cyber Resilience	● Establishment of a Cyber Resilience Centre between ENISA and Taiwan ● Follow the model of Cyber Resilience Center at High Tech Campus Eindhoven[42]
Private Mutual Coordination	Global Market Integration	● Synergy of tech niche by both markets ● Short-term solutions to current private sector threats

Source: Cited Sources Below

Specifically, the short-term plan involves finding suitable partners (such as system integrators in the same application field or cooperative cybersecurity companies) to conduct proofs of concept for specific application areas; the

[42] Bart , Brouwers. "Cyber Resilience Centre in Brainport Eindhoven." Innovation Origins, June 3, 2018. https://innovationorigins.com/en/cyber-resilience-centre-brainport-eindhoven/.

medium-term plan is to promote sales in related fields, and the long-term goal is to expand markets based on Taiwan and the EU in the surrounding areas.

As the study has concluded, the background research and data collection, as well as an analysis of the potential for improvement, threats, and responses on both the Taiwanese and European sides, have been linked and have enabled the development of single recommendations for the integration of the private and public sectors. An affirmative contrast and verification of the research process requires regular revision of the findings.

BIBLIOGRAPHY

Abrams, Lawrence. “Computer Giant Acer Hit by $50 Million Ransomware Attack.” BleepingComputer. BleepingComputer, March 20, 2021. https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/.

Bart, Brouwers. “Cyber Resilience Centre in Brainport Eindhoven.” Innovation Origins, June 3, 2018. https://innovationorigins.com/en/cyber-resilience-centre-brainport-eindhoven/.

Braden, R. “RFC 1122 - Requirements for Internet Hosts - Communication Layers.” Document search and retrieval page, 1989. https://datatracker.ietf.org/doc/html/rfc1122#page-18.

Cate, Fred H., and Dempsey, James X., "Bulk Collection: Systematic Government Access to Private-Sector Data" (2017). Books & Book Chapters by Maurer Faculty. 173. https://www.repository.law.indiana.edu/facbooks/173

Cimpanu, Catalin. “Chinese Hackers Linked to Months-Long Attack on Taiwanese Financial Sector.” The Record by Recorded Future, February 23, 2022. https://therecord.media/chinese-hackers-linked-to-months-long-attack-on-taiwanese-financial-sector/.

Cimpanu, Catalin. “Frankfurt Shuts down It Network Following Emotet Infection.” ZDNet. ZDNet, December 19, 2019. https://www.zdnet.com/article/frankfurt-shuts-down-it-network-following-emotet-infection/.

Commission of the European Union. “GDPR Archives.” GDPR.eu, May 25, 2018. https://gdpr.eu/tag/gdpr/.

Commission, European. “Cybersecurity Policies.” Shaping Europe's digital future, 2020. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

Commission, European. “Digital Inclusion.” Shaping Europe's digital future, June 2022. https://digital-strategy.ec.europa.eu/en/policies/digital-inclusion.

Commission, European. “The Cybersecurity Strategy.” Shaping Europe's digital future, 2020. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

Council, European. “Cybersecurity: How the EU Tackles Cyber Threats.” Consilium, April 29, 2022. https://www.consilium.europa.eu/en/policies/cybersecurity/.

Country Commercial Guide, Taiwan. “Taiwan - Information and Telecommunications Technology.” International Trade Administration | Trade.gov, 2022. https://www.trade.gov/country-commercial-guides/taiwan-information-and-telecommunications-technology

Cybersecurity & Infrastructure Security Agency. “Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization.” CISA, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-277a.

Digital Affairs, Ministry of. “Cyber Security Policies and Regulations-Operations｜Administration for Cyber Security, Moda.” Ministry of Digital Affairs(open in new window), 2022. https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648.

Digital Affairs (R.O.C.), Minister of. “Cyber Security Policies and Regulations-Operations｜Administration for Cyber Security, Moda.” Ministry of Digital Affairs(open in new window), 2022. https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648.

ENISA, European Agency. “ENISA Surveys Evolving Threat Landscape.” Computer Fraud & Security 2013, no. 1 (2021): 1–3. https://doi.org/10.1016/s1361-3723(13)70001-0.

European Union, Data Protection Officer. “Data Protection.” European Data Protection Supervisor, March 16, 2022. https://edps.europa.eu/data-protection_en.

Ho, Kah-Kin. “Cybersecurity: The Strategic View.” Edited by Damien D. Cheong. Cybersecurity: Some Critical Insights and Perspectives. S. Rajaratnam School of International Studies, 2014. http://www.jstor.org/stable/resrep05892.4.

Hsin-fang, Lee. “Information Security: At Least 900 Cybersecurity Jobs Need to Be Filled to Combat Chinese Espionage.” Taipei Times, April 5, 2021. https://www.taipeitimes.com/News/taiwan/archives/2021/04/06/2003755174.

Huang, K.-J., & Chiang, K.-H. (2021). Toward a Self-Adaptive Cyberdefense Framework in Organization. SAGE Open, 11(1). https://doi-org.wenzao.idm.oclc.org/10.1177/2158244020988855

Information, Security Management. “Asus Corporate Social Responsibility.” ASUS Corporate Social Responsibility, 2022. https://csr.asus.com/english/article.aspx?id=1741.

IBM, Enterprises. “IBM Security X-Force Threat Intelligence Index.” IBM, February 23, 2022. https://www.ibm.com/reports/threat-intelligence/.

Information Security Office 資通安全處. “National Cyber Security Program of Taiwan (2021 to 2024).” 中文版(Open New Window), 2021. https://nicst.ey.gov.tw/en/FD815304EBFFE6FC/639d32e8-2a07-40da-b033-bc6c95d015ce.

Marsh & McLennan Companies. “MMC Cyber Handbook 2020 - Marsh Mclennan.” MMC Cyber Handbook 2019 Perspectives on Cyber Risk in the Digital Era, 2020. https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2019/oct/MMC_cyber_handbook_2020_final_digital.pdf.

McAfee Enterprise, Endpoint Detection. “What Is Managed Detection and Response (MDR)?” McAfee, 2021. https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-managed-detection-response.html.

Mehrotra, Mohit. “Contactless Economy: Deloitte Sea: Consulting.” Deloitte, September 11, 2020. https://www2.deloitte.com/gu/en/pages/strategy/articles/contactless-economy.html.

MOEA, Industrial Development Bureau. “Contact Taiwan.” Contact TAIWAN-Key Industries--The Internet of Things, October 7, 2022. https://contacttaiwan.tw/main/docdetail.aspx?uid=1078&pid=727&docid=11158

Murphy, Hannah. “Apple Supplier Quanta Hit by Cyber Attack.” Subscribe to read | Financial Times. Financial Times, April 21, 2021. https://www.ft.com/content/0ec11549-9d68-4ca2-bbac-34684c86abab

Ocean, Report. “Cyber Security Market Growth Analysis by Revenue, Size, Share, Scenario on Latest Trends, Types and Applications: Taiwan News: 2022-02-18 05:49:33.” Taiwan News. Taiwan News, February 17, 2022. https://www.taiwannews.com.tw/en/news/4447491.

Policies, MODA. “Major Policies｜Ministry of Digital Affairs.” Major Policies｜Ministry of Digital Affairs, page 368, 2022. https://moda.gov.tw/en/majorpolicies/368.

Pryor, Crystal D., Tania Garcia-Millan, Jeffrey Gelman, Tanvi Madan, Scott Moore, Crystal Pryor, Lisa Reijula, et al. “Taiwan’s Cybersecurity Landscape and Opportunities for Regional Partnership.” Edited by Bonnie S. Glaser and Matthew P. Funaiole. Perspectives on Taiwan: Insights from the 2018 Taiwan-U.S. Policy Program. Center for Strategic and International Studies (CSIS), 2019. http://www.jstor.org/stable/resrep22549.5.

TSMC, English Company Press. “TSMC Details Impact of Computer Virus Incident.” TSMC Details Impact of Computer Virus Incident, 2018. https://pr.tsmc.com/english/news/1969.

Valeriano, Brandon, and Ryan C. Maness. “International Relations Theory and Cyber Security.” The Oxford Handbook of International Political Theory, 2018, 258–72. https://doi.org/10.1093/oxfordhb/9780198746928.013.19.

Wang, Vincent Wei-cheng. “Developing the Information Industry in Taiwan: Entrepreneurial State, Guerrilla Capitalists, and Accommodative Technologists.” *Pacific Affairs* 68, no. 4 (1995): 551–76. https://doi.org/10.2307/2761276.

Wolford, Ben. “What Is GDPR, the EU's New Data Protection Law?” GDPR.eu, February 13, 2019. https://gdpr.eu/what-is-gdpr/?cn-reloaded=1.

Wu, Benson. “Taiwan Sees Its Cyber Capabilities as the Hard Reality of Soft Power.” The National Bureau of Asian Research (NBR), March 20, 2019. https://www.nbr.org/publication/taiwan-sees-its-cyber-capabilities-as-the-hard-reality-of-soft-power

Wu, Jason, and Matthew Fulco. “Taiwan's Cybersecurity Dilemma.” Taiwan Business TOPICS, January 17, 2022. https://topics.amcham.com.tw/2021/05/taiwan-cybersecurity-dilemma/.

BIOGRAPHY

Depending on how playful I am feeling I will sometimes introduce myself as an alchemist that uses social sciences for its own creations. In most cases, I only offer a trivial explanation for this remark. In my role as a political scientes, sociologist and researcher, I literally conjure up symbols from the aether and assemble them in an information hierarchy where they, in turn, control and manipulate equations and theories to understand the external world. While this formulation generally describes my work, my identification with alchemy also communicates other layers of meaning, suggesting metaphysical transformations and esoteric perspectives, as well as cultural and socioeconomic aspects intertwined in the equation of the ongoing work.

This narrative may simply be a fanciful way of expressing the idea that if you love what you do you will become a better person for it. I love what I do. I am passionate and enthusiastic and embrace life's challenges with delight. It is difficult for me to distinguish between my work, studies, and hobbies, as together they are becoming my life-work.

Education and learning have always been a primary focus of my social and intellectual pursuits. Both of my parents were deeply involved on my education since my early ages, carefully caring about the educators to my life, and my schooling instilled the value of education for its own sake. Having grown up in the southern Spanish city of Sevilla, moving to Barcelona at the age of seven, and completing my high school studies at the British School of Barcelona was a joyous and productive experience before college.

The passion my mother has shared with me regarding traveling extensively around the world has also been a major influence on my worldview over the years. A continuing source of accomplishment for me is the exploration and exchange of knowledge.

The academic training I have received has been analytical, and I have developed a strong commitment to first natural sciences. After a year of transition from my bachelor's degree in biochemistry at the University of Sevilla, I switched my focus to social sciences, where I started my journey at Buckingham University of London with a minor in economics, and I am currently under the completion of my studies at Wenzao University, located in Kaohsiung City, Taiwan.

This combination has translated well to the domain of a broad worldview perspective of social interpretations and perspectives, as well as world development, but my satisfaction in applying these talents is highly contingent upon the setting.

When my work is directed towards meaningful, constructive goals with humanistic outcomes, I thrive in the sense that my work truly fulfills me.