The Republic of China (Taiwan) National Cyber Security Strategy to develop a solid cyber diplomacy: How to build a route for Guatemala

Mónica Dalila Pozuelos Arriaza

MOFA Taiwan Fellow 2023

Visiting Scholar at the National Chengchi University

College of International Affairs, Department of Diplomacy

Table of Contents

Acknowledgment

I would like to express my deep gratitude to the Ministry of Foreign Affairs (MOFA) of the Republic of China (Taiwan), for granted the sponsorship during the research period, it has been an honor to be part of the "MOFA Taiwan Fellowship Program 2023". I'd like to thank to the National Central Library (NCL) for all the support and kindness of its personnel, and also to the National Chengchi University (NCCU) and its staff, for the warm welcome and help during my stay in Taiwan.

Introduction

The cyber security has become an important issue around the world, as important as protecting our borders and sovereignty, which is part of the national interest of any nation but, how can we defend our territory in the cyber space?

Also, regarding a cyber security program, how can we start to consolidate the best strategies according to our country needs. The Republic of China (Taiwan), has a complete cyber security program with a lot of positive guidelines to learn, as they have been working on these strategies for twenty-three years now, the results are a cyber security resilient program, and that is why it's imperative in this research to design this route for Guatemala.

This research it's been developed in four chapters as follows, on the first chapter it's described the argumentation, research questions, objectives and the methodology, in the second chapter the context including all the phases of the Cyber security program prior to the year 2021, follow by the third chapter with the theorical background which includes all the theorical terms in order to understand the cyber security, the cyber security strategy, the diplomacy and the cyber diplomacy; and the fourth chapter included the analysis of the interviews and the available data such as governmental websites, articles, books, the cyber security program 2021-2024 from Taiwan and Guatemala, and the last part included the conclusions with some recommendation.

The recommendations included some scenarios for Guatemala, and other elements found in the cyber security program of Taiwan.

I.- ***The importance of a resilient Cyber Security Program***:

The Republic of China (Taiwan) has been building a cyber security program for more than two decades, as this phenomenon of cyber-attacks start making the first appearance in 1999. It is important to mention that this program contains different strategies and phases where the cyber security program was consolidated, so it will be described during this research the challenges that Taiwan has been facing but also the goals they are reaching so far.

In fact, The Republic of China (Taiwan) has an unique cyber security culture and their cyber security strategy it is a great example of a cyber security resilient strategy, facing a lot of challenges but learning and creating a better strategy every day. According to Pryor (2018) Taiwan's government faces 20 to 40 million cyber-attacks every month. So, it is important to observe the cyber security program of Taiwan, with the strategies applied, as they are a good example of a resilient country in the cyber security matters.

In this research the results to be expected to find are the main elements of the cyber security program of Taiwan, in order for Guatemala to review and update the cyber security strategy, and make it strong enough to protect the information in the public and private sector, but most important in the public sector, specifically at the Ministry of Foreign Affairs of Guatemala.

In addition, Guatemala has as a cyber security strategy approved in 2018, a new born strategy, on which we can improve and apply the suggestions and example of Taiwan's Cyber Security Program. Furthermore, it's important to observe and describe the example and development of the cyber security program of Taiwan, in order for Guatemala to strength their cyber security strategy and analyze the elements around law, policies and regulations and update it based on this case; but to understand this phenomenon there are some questions as follows**:**

General Research Question:

- How The Republic of China (Taiwan) developed its national cyber-security strategy from 2021 to 2024?

Research Questions:

- What has The Republic of China (Taiwan) done to strengthen its cyber-diplomacy during 2021-2024?
- How is Guatemala handling the cyber security nowadays?

General Research Purpose:

- To describe how the Republic of China (Taiwan) is developing its national cyber security strategy from 2021 to 2024.

Research Purposes:

- To analyze the actions taken by the government of the Republic of China (Taiwan) in order to strength their cyber diplomacy during the 2021-2024.
- To define how is the government of Guatemala is handling the cyber security strategy nowadays.

Research Methodology: The Republic of China (Taiwan) developed in two decades a cyber security program which is very interesting to be analyzed. This program has been consolidated in different phases, but the main topic in this research it's to analyze the cyber security program including the strategies from 2021-2024, so we can design a route in order to strength our cyber security strategy of the Republic of Guatemala, created in 2018.

This research is based on an eleven-month period granted by the Ministry of Foreign Affairs MOFA of the Republic of China (Taiwan). The qualitive methodology was implemented, by working in some interview to experts of the cyber security and cyber diplomacy field, professors, and officials, also reviewing some sources such as governmental websites, articles, books, the cyber security program 2021-2024 and the previous programs from Taiwan and the cyber security strategy from the Republic of Guatemala created in 2018.

II - Context

Taiwan has a rather unique Cyber Security culture, which has been building in collaboration with the government and private sector, also with white-hat hackers (Burgers et al. 2021)

The Cyber Security Strategy of The Republic of China (Taiwan) prior to 2021: First of all, The Republic of China ROC (Taiwan) created a Cybersecurity strategy, strong enough to confront the challenges in the 21st century. One important thing to mention in this research is that Taiwan has an unique "***culture of Cybersecurity***"; but this strategy didn't start as a program it has been suffered changes in order to prevent the cyber-attacks.

According to Pryor (2018)

> Taiwan has faced serious cyber threats from China since at least 1999, which prompted the government to form the National Information and Communication Security Taskforce (NICST) in 2001 as an interagency body to promote government attention to information security. That year it also created the National Center for Cyber Security Technology (NCCST) to provide cyber security technical services, such as pre-incident protection, during-incident response and handling, and post-incident forensics and recovery, to government agencies (p. 3)

In fact, the creation of a cybersecurity strategy was a process on which we can find several steps and phases in order to protect the information and data in cyberspace. As a matter of fact, the cybersecurity plan has been developing since 2001, when the *Executive Yuan* announced the Building Taiwan's Communication and Information from Infrastructure Security Mechanism Plan". This one was built during the period of 2001-2004.

Phase One Mechanism Plan (2001-2004): The Executive Yuan was seeking to ensure that the Republic of China (Taiwan) were able to provided a secure communication and information environment and this was built during this period, also other facts are important to mention:

1. The establishment of the NICST in conjunction with the technical staff unit, the National Center for Cyber Security Technology, as the competent authority in charge of Taiwan's cyber security infrastructure and policies.
2. The promotion of cyber security management systems for key government agencies whose works relate to the public's daily life, providing relevant cyber security support and designating requirements for government agencies at different levels by building agency cyber security incident reporting and notification mechanisms and responsibility level categories and conducting cyber security audit on specified agencies.
3. The promotion of cyber security education and training among information personnel, reinforcing cyber security workforce training and awareness, and increasing public cyber security awareness.
4. The revision and amendment of laws and regulations relating to cyber security and the creation of cyber security technical standards and regulations, building product inspection and guarantee mechanisms.
5. The planning, promotion, and building of the Information Security Management System (ISMS) for key operating systems of critical infrastructures as well as cyber security management programs including cyber security center alert and reporting mechanisms and personnel training.[1]

So, during this phase, there are some elements to mention as the qualify staff to handle the National Center for Cyber Security Technology, and the promotion of the *cyber security education* in order to reinforce the workforce, was a big step for the next phases, also the (ISMS) represented the main key for critical infrastructure. In addition, the regulations and laws for the cyber security systems were reviewed and amendment, and for this research it is important to learn the lessons of this modifications and how this step helped to consolidate the program.

Phase Two Mechanism Plan (2005-2008): The remarkable elements to describe during this phase are the establishment of the National Security Operation Center (N-SOC) with a 24/7 defense,

[1] Ministry of Digital Affairs (August 3, 2023) Cybersecurity Policy and Regulations https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648

including alert and monitoring services; also, the expansion of the government agency cyber security responsibility level classification scope, greatly increasing the number of important government agencies includes the cyber security defense system and extending the scope to include education system[2].

Phase Three Development Program (2009-2012):

During this period, the Executive Yuan based on the vision of a “secure trustworthy smart Taiwan and sound quality digital life” [3] shared the government’s experience expanding the cyber security with the general population. In fact, the Taiwan´s national cyber security strategy start been handling by the National Information and Communication Security Taskforce (NICST). According to Burgers, et al. (2021) “This agency, is part of the executive branch of the Taiwanese government – the Executive Yuan – formulated the first national cyber security strategy in 2009: The National Strategy for Cyber Security Development program (NCSP)” (p.276). The main components included in this phase, were the evaluation level A – and B, also the implementation of the Plan – Do- Check- Act (PDCA) model to lower relevant risk.

In addition, encouraging all the business to do a third-party evaluation reinforcing the cyber security inspections to ensure the protection of the information and data for the users and customers. The strengthening of cyber security research capacities, encouraging higher education institutions to offer cyber security courses, and the promotion of cyber security awareness preparing events at schools and business in order to review their own information asset’s security[4].

Phase Four Development Program (2013-2016): It is important to mention that during this phase the Executive Yuan approved the” National Strategy for Cyber Security Development Program 2013-2016” and in this program the talent cultivation and international exchanges were promoted in order to have more qualify personnel and to establish personnel registration and certification mechanism. Cyber security defense and intelligence sharing: building a structure for

[2] Ibid
[3] Ibid
[4] Ibid

government cyber security governance, evaluating cyber security governance maturity levels at A-B-, and C-level government agencies; establishing the Institute of Watch Internet Network (iWIN) to enhance internet content security management mechanisms, conducting cyber security offense and defense drills, planning cyber security scenario and hands-on drills; implementing the government cyber security management system to improve government agencies' cyber security management works; promoting cyber security base environment security settings and continuing to plan various government configuration baseline (GCBs) settings; increasing cyber security threat intelligence collection capacity and enhancing data analysis and sharing mechanisms[5].

Phase Five Development Program (2017-2020): In the fifth phase it was incorporated three major policy goals creating a national cyber security joint defense system," "improving the overall cyber security defense mechanism," "reinforcing cyber security autonomy industry development," and the four major strategies of "enhancing the base environment for cyber security," "creating a national cyber security joint defense system," "increasing the autonomy of cyber security industry," and "cultivating high-quality cyber security talent," designating 11 (eleven) specific measures to gradually launch Taiwan's cyber security defense in depth and joint defense system and stabilize the cyber security frontline of Taiwan's digital territory[6].

So, in conclusion it's important to mention that The National Information and Communication Security Taskforce (NICT)[7] have developed imperative programs that helped to build the cyber security strategy nowadays, as follows:

- ✓ National Strategy for Cyber security Development Program (2013-2016)
- ✓ National Cyber Security Program of Taiwan (2017-2020)
- ✓ National Cyber Security Program of Taiwan (2021-2024)

With these programs, Taiwan has been demonstrating its capability to handle the risk and the security issues in the cyberspace arena, and also the resilience they handle in any situations. It is

[5] Ibid.

[6] Ibid

[7] The National Information and Communications security Taskforce (NICT) was established by the Executive Yuan in order to national security policies, accelerate the construction of a safe national cyber security environment.

one of the main reasons why it is necessary to identify the process of implementation of the cyber security program, which includes different strategies, which can help to strength Guatemala’s Cyber security Strategy, created in 2018. Guatemala has a lot of knowledge to get from Taiwan in the cyber security field, that is why it’s important to describe a law and regulations route for Guatemala to follow in order to have a reliable cyber security strategy, so we can be capable of protecting the most valuable information that is the Guatemalans data, and that can lead to the management of secure cyber diplomacy without the risk of cyber-attacks.

III. Theorical Background

> *The problems of Cyber security are not technical issues about how to prevent cyber penetrations, but political and geopolitical questions about the motivations of those responsible for the penetrations and about how we can limit what they do. (Riordan,2019)*

Cyber Security:

First of all, when we mentioned the word “**Cyber security**”, it comes to our minds a cybernetic term, that is referred to “the field of control and communication theory, whether in machine or in the animal” (Wiener, 1948). In addition, the cyberspace term “is not static it is a dynamic, evolving, multilevel ecosystem of physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by an expanding population of contributors”[8]. In fact, the cyber space it’s constantly changing and in evolution. In addition, the cyber security it’s interdisciplinary, because it can be analyzed in communications, computers (hardware and software) in social, economy and political field among others. When the countries are prepared and have a strong cyber security strategy, they can avoid cyber-attacks or reduce the risk. As a matter of fact, we can identify main ideas of the cyber security concept, such as communication, software, relations, ideas, interaction and people, so obviously the spread of internet in all levels (individual, government and collective) has become an important issue for the countries, regions and all over the world, due to the interactions of it and the vulnerabilities that can come with its use. But in this research, we would like to mention at least six (6) important terms about the “***cyber security***” as follows:

[8] Deibert & Rohoziinski, 2010 p.14

I. Cyber security consists largely of defensive methods used to detect and thwart would-be intruders.

II. Cyber security is the collections of tools, policies, security concepts security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user´s assets.

III. The ability to protect or defend the use of cyber-space from cyber-attacks.

IV. The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

V. The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modifications, or exploitation. (DHS, 2014) **(**Cited Craigen et al.2014 p. 14-15).

This means that the cyber security protects the data and the information in the cyber space, but what kind of threatens can occur if there is no security in the computer systems, in fact, what is a cyber-attack for instance? or how it can be recognized inside the computer system or the cyber space?

Cyber-attack: As we know the world its dominated by technology, and it's a new space where the societies need to adapt and understand how to handle it, due to the fact, that the information can be manipulated and stolen; but how the information can be disrupted? We need to understand the meaning of the threaten and how to control it. Actually, we need to understand the sense of a cyber-attack the classifications and how to avoid any disruption of information.

In fact, the cyber-attack it's the contamination of the data or information in the cyberspace and this could be through the process of hacking. So, the hacker infects the system which contains poor cyber security and looking for systems which are mis-configured.

In addition, once the access it's granted, he/she had access to the network and can remotely operate the systems and Commands can be sent to make the system to act as spy for the attackers and it will also be used to disrupt the other systems. The hacker will expect the infected system to have some flaws such as bugs in software, deficient in anti-virus, flawed system configuration so that other systems can be infected through this system.[9] A cyber-attack can be done for individual or collective proposes to steal information from any governmental organization or from the private sector. So, in order to classify the threatens faced by both sectors (public and private) it is necessary to have a list or a description of the type of cyber-attacks, so we will be able to understand how to fight back against these cyber-attacks.

These cyber-attacks regularly it's part of a strategy to inflict a retardation in the decision-making process, by playing a role crippling some areas, like emergency services and military which causes a delay in the tactical deployment, activation of life support, causing death or military defeats. [10]

The hackers can change the authorization access of the users, by authorizing new users, to access to any information from the organization or public institution, so the attacks can disrupt in domains in basic service as the transportation as railways, banking services, or another type of services as airline or stock markets.

In effect, the classification of the cyber-attacks can be categorized as follows:

- Based on Purpose
- Legal Classification
- Based on severity of Involvement
- Based on Scope
- Based on Network Types [11]

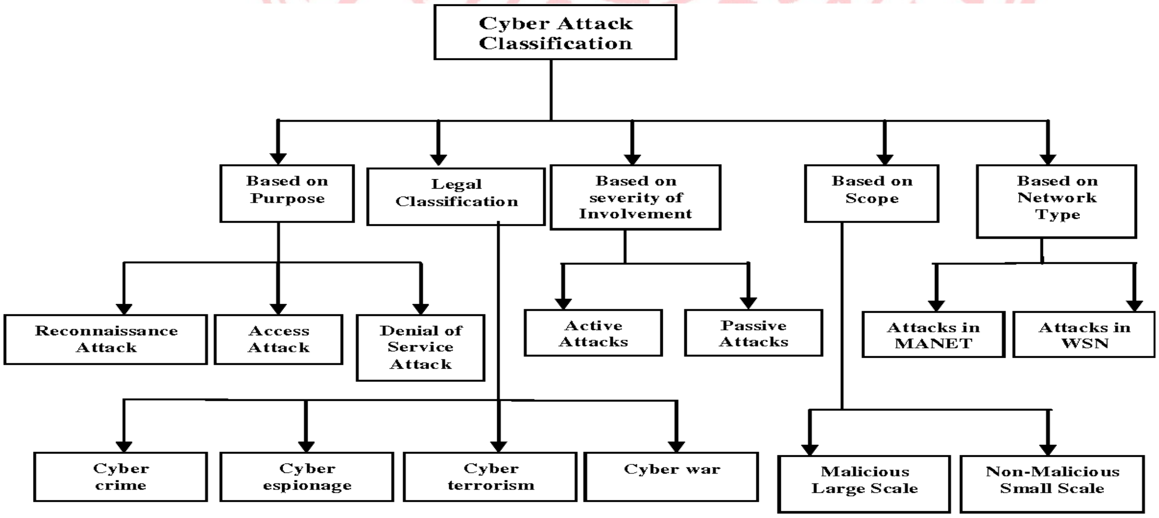


Diagram from Uma & Padmavathi, 2013

[9] Uma & Padmavathi, 2013, p.390
[10] Ibid, p.391
[11] Ibid. 392

In this diagram we observe the legal classification including the cyber terrorism, cyber-crime, cyber espionage and the cyber war, as a result, which are sensitive phenomenon to research, but it's necessary to study in order to be prepared and create a resilient culture. For research proposes, we will focus on the base of purpose and the legal classification in order to describe this phenomenon and build a proposal.

Cyber-attacks based on purpose: This kind of cyber-attacks are classified as reconnaissance attack, access attack denial of service attack. For Reconnaissance attack it's an unauthorized detection, system mapping and services.[12]
As an example, this is like leave a home alone, without windows and door, so the thief can enter without any problem.[13]

Cyber-attack based on legal classification: The motivations for the cyber-attacks, are several but to mention some of them, it is to obtain governmental and financial information from websites, online discussion forums, news and military/defense data, in order to obstruct the information so the hackers can block the access to important data. This can be done by selecting which user is authorized to have access to certain data. In this classification we can find: Cyber Crime, cyber war, cyber espionage, cyber terrorism.

Cyber Crime: The definition is "a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence." [14] This could be any kind of crime as long as they are using a computer as the object, in order to commit a crime against another user.

[12] Ibid. p. 392.

[13] In cyber-attacks based on purpose it can be found more attacks, as scanning the port which consist in receiving a lot of messages from the attacker attempting to break into the computer system in order to confirm the port number for each computer. In addition, we can find the social engineering attack which are websites infected by a malicious code SQL injection so that any user entered can be infected. Also, the phishing that is when the hackers send a fake e-mail using the legitime logo of a company to fool users to enter sensitive information in these web pages, this information can be the name, social security number, credit/debit card numbers, phone numbers, and any information that these attackers can use against the users to steal money or the user's identity.

[14] Ibid p.393

[15] Ibid. p.394

Cyber War: In this cyber-attack, the definition is "the act of nation state to penetrate another nation's computer or network in order to cause damage or disruption. "[15]
This can be measure in the foreign policy theory of Kenneth Waltz, as a state level, consequently, this is a governmental attack.

Cyber Terrorism: In this cyber-attack category, it's the "activity including acts of deliberate large-scale disruption of computer networks by use of tools such as computer viruses"[16] and commit any kind of terrorism activity. In other words, the disruption of the computer network by using the Trojan horses or any kind of viruses, for an act of terrorism, can be classify as cyber terrorism.

Cyber Espionage: One tool using by the hackers it's infect the computers with malicious software, including the Trojan horses and spy in order to get information in an individual or collective level. "It may wholly be perpetrated online from computer desks of professionals on bases in faraway countries. It may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmers." [17]

Cyber Security Strategy:

The *cyber security* it's interdisciplinary, because it can be analyzed in communications, computers hardware and software) in social, economy and political field among others. When the countries are prepared and have a strong *cyber security strategy*, they can avoid cyber-attacks or reduce the risk. The cyber security strategy, must be constructed to protect the data and information from the users, due to the fact that "holds a significant impact on national security, public interest, national life, or economic activities"[18]; because this has a real impact in the individual users, companies, organizations, institutions, etc. Nonetheless, in this research we are looking for an understanding of the cyber security strategy of the Taiwan in order to have a solid cyber diplomacy and how this strategy it's conducted by the government. But first, we need to describe the diplomacy and the concepts of cyber diplomacy.

[15] Ibid. p.394
[16] Ibid. p.394
[17] ibid. p. 393
[18] National Cyber Security program of Taiwan (2021-2024) p. 1

Diplomacy:

The diplomacy has existed for centuries; of course, the dynamic has been changing according to the era, but exactly a core term of diplomacy is (Bjola 2018):

> The relationship management and maintaining international order. At the micro-level, this is translated into diplomats building and managing relations of friendship. At the macro-level, diplomacy contributes through its core functions of representations, communications and negotiation to producing and distributing global public goods (security, development, sustainable environment, etc.)” (Cited at Bjola and Kornprobst, 2018, p. 04)

In addition, the contemporary concept of diplomacy in international relations, which in words of Pigman, 2010 “*it’s the process of conducting negotiations between representatives of states”* (Cited Attatfa et al. 2020, p.1). The diplomacy is also interdisciplinary and it’s important to be analyzed from the social science, global affairs, and politics.

Also, is identify as “the use of tools to promote broader diplomatic agendas, as well as the use of diplomatic techniques and mental modes to analyze and manage cyberspace problems, is separate but interdependent activities”. [19] According to Wight (1979) diplomacy is “the attempt to adjust conflicting interests by negotiation and compromise” (Cited at Barrinha & Renard, 2017, p. 4). This means that there is an interest of the nations to negotiate to strength their relations according to the needs, and as the world is changing so quickly, it is important to adapt with the changes of the world.

For authors like Hendly Bull (2002) there are five main functions to the diplomatic practice: to facilitate communication in world politics, to negotiate agreements, to gather intelligence and information from other countries, to avoid or minimize “friction in international relations” (Cited on Barrinha & Renard, 2017, p. 355) and, finally, to symbolize the existence of a society of states. Besides, the process of facilitating communications in world politics, nowadays, has been changing a lot, as exist different ways to communicate including social media and the computer system, on which we can find a weakness if they are not protected.

[19] Attatfa et al. (2020) p. 2

For Barston (1997) “the purpose of diplomacy is to contribute to the process of recognizing and identifying new interest at an early stage through continuous reporting and assessments, facilitating adjustment between different interest and contributing to policy implementation”[20]. This means that the diplomacy is a method through discuss and create new policies to be implemented in order to secure the national interest of the participant nations.

In addition, we observe that the technology has change the way that diplomacy use to be handle previously. For Pigman (2010) “Technology determines how communications can take place and, critically, at what speed. At a broad level communications and transport technology has driven globalization, which in turns has permitted new types of actors to become diplomats in an arena that once was dominates by nation-states: multilateral institutions, global firms and CSOs, in particular” (p. 110)

As a matter of fact, as the cyber security play an important role in the virtual communications, and the technology it’s a new tool used by the decision makers in politics, especially in diplomacy during the negotiations, its critical to understand the concept of cyber diplomacy and how it’s protected against hackers, cyber-crime or cyber terrorist, etc. Besides, we can find the digital diplomacy and the cyber diplomacy, in fact, both are different terms, that would be explained as follows.

Difference between digital diplomacy and cyber-diplomacy

The technological advance is growing so fast that we are trying to adapt as fast as possible. In fact, there are many core terms, which would be explaining it in order to understand the difference between digital diplomacy and the cyber-diplomacy.

Digital Diplomacy: The digital diplomacy, according to Leguey-Feilleux (2009) is “the new means of communication and remarkable access to information are changing the way diplomacy is conducted – event if diplomacy is not really being “reinvented” (p. 90).

[20] Barston (1997) p. 201

As we can see the new ways of digital communications, have change the way that diplomacy it’s been handling by the actors in the international arena. In other words, “it is the application of digital technologies”[21]. But what is the definition of digital technologies; we will define it as, “the use of social networking sites in order to foster dialogue with the online publics (Cited at Attafta et al. 2020 p.2) This means that all the tools of social media, such as Facebook, Instagram, Twitter, etc., can be a way to spread any governmental information, such is the case of the public diplomacy on which the information can be spread even by different actors than the state with this new technological tools.

For example, there is no need for an ambassador to travel for 30 hours to talk about an agreement, or conduct a negotiation, if they can do it through a video conference, or video call. Indeed, technology it´s an effective tool that is helping to improve the international relations between nations, and at the same time it’s a challenge to control and protect the security and the usage of these tools.

Furthermore, for the countries to have a strong *cyber security* strategy can protect them, when they are working on negotiations with other nations made through ***cyber diplomacy***: but what can we say about the ***cyber diplomacy***, this is a new concept a king of complex, and that has a lot of edges, where it can be seen, let’s start by understanding the theory of diplomacy, and then develop the cyber diplomacy concept.

Cyber Diplomacy: Cyber diplomacy can be defined as

> “Diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace. Such interests are generally identified in national cyberspace or Cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues on the cyber-diplomacy agenda include Cybersecurity, cybercrime, confidence-building, internet freedom and internet governance”[22].

[21]. Riordan, (2019) p. 9

[22]. Barrinha, A. and Renard, T. (2017) p. 355

In other words, with the cyber diplomacy the governments can use different tools to open international agendas and to work between nations with the common goal of protect themselves from cyber-attacks, or from actors (individual and collective) who want to steal information from their nations. The cyber diplomacy it’s handle by the diplomats meeting in bilateral formats or in the multilateral arena. Besides the traditional diplomacy and how the diplomats conduct it, now the diplomats “interact with various non-state actors, such as leaders of internet companies (such as Facebook or Google), technology entrepreneurs or civil society organizations. Diplomacy can also involve empowering oppressed voices in other countries through technology”.[23.] In addition, to have an effective cyber diplomacy involves: (1) building strategic partnerships with other countries around the world and engaging the many, many multilateral forums that are shaping cyber policy; (2) using diplomacy and diplomatic tools to directly respond to cyber threats; and (3) working with other agencies to facilitate law enforcement and technical cooperation and provide capacity building so other countries can better work with us[24].

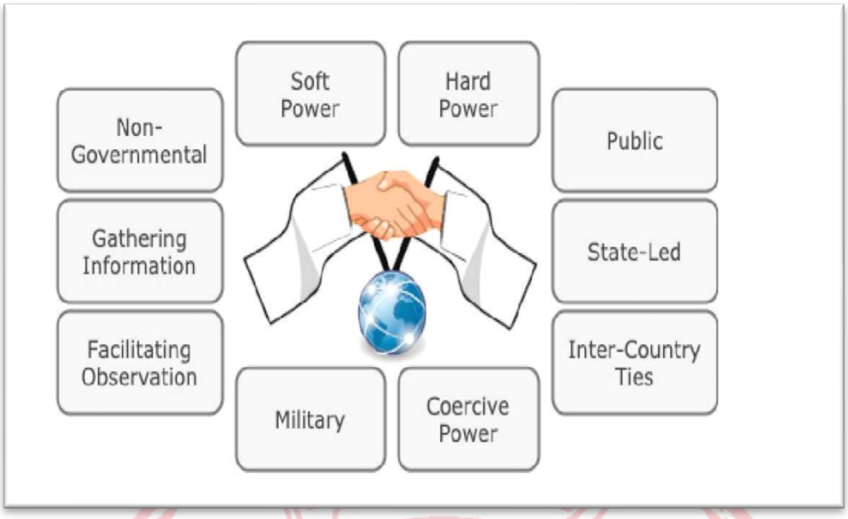
Regarding the strategic partnerships that can be built with other countries in international forums it’s a key to sign international agreements about the cyber-crime and how to extradite the cyber criminals between the nations involved in these agreements. The fact that the countries are communicating faster using cyber tools, it’s facilitating and consolidating the diplomacy. Also, it’s important to identify the actors involved in this phenomenon, due to the alliances that can be made in order to protect the information of the citizens and more important, the international agendas that can be created between nations.

Practioners of cyberdiplomacy:

These are the primary Practioners of the cyber diplomacy, the Ministry of Foreign Affairs, as they promote the cyber agenda in coordination with other governmental institution and non-state actors “who interact with diplomats and policymakers in conversations or negotiations on cyber problems include members of the academic community, business, industry, and civil society organizations”[25]. Also, the cyber diplomacy dimensions are:

[23] Ibid p.355
[24] US Cyber Diplomacy in an era of Growing Threats (p.5)
[25] Best Diplomat recovered from https://bestdiplomats.org/cyber-diplomacy/

Cyber Diplomacy Dimensions



Information retrieved from Sciencedirect Magazine cited on March 20, 2023 from file:///C:/Users/MONICA%20POZUELOS/Desktop/MONICA%20POZUELOS/BECA%20A%20TAIWAN/ARTICULO%20ACADEMICO/MARCO%20TEORICO/CYBERDIPLOMACIA.pdf

"Cyber security is national security"

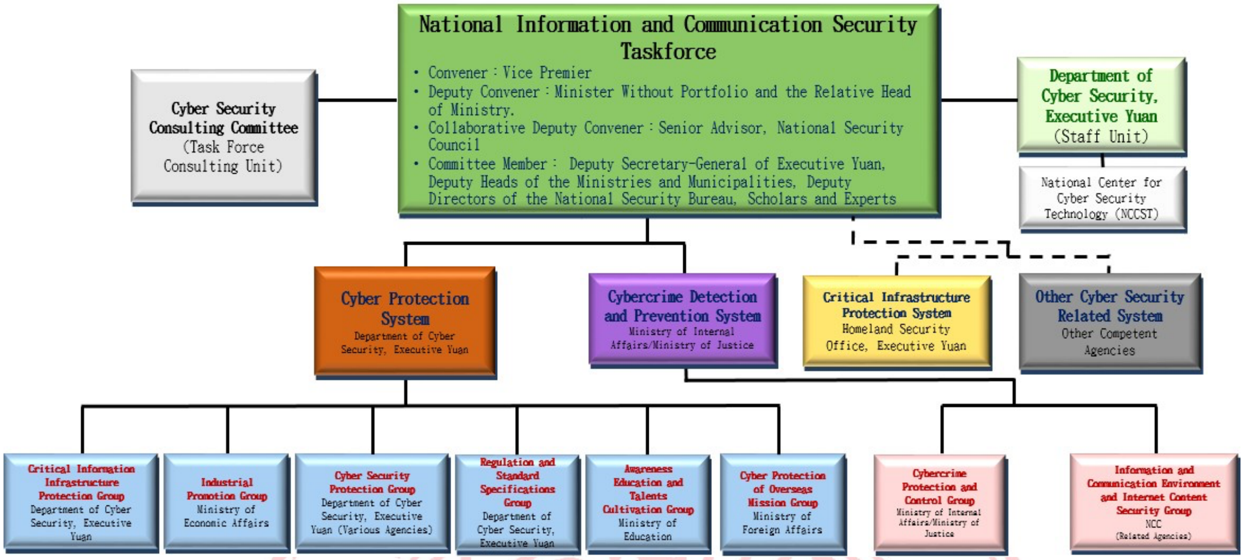
President Tsai Ing-wen

IV. Development of The Republic of China (Taiwan) national cyber-security Strategy from 2021 - 2024

The Republic of China (Taiwan) has this unique Cyber Security Culture, which is interesting to analyze due to the geopolitical situation in the Indo Pacific. The result of this consolidates cyber security program, where, Taiwan showed the effort and the priorities of the country. In order to create a resilient cyber security program, they activated different strategies for the public and private sector, also evaluating the computer systems capabilities to detect the cyber-attacks, with the evaluations level A - B.

This is one of reasons why the national cyber security program of Taiwan, it is an example to be describe in this research, in order to create a route for the Republic of Guatemala. In addition, to describe the National Cyber Security Program of Taiwan, first of all, we need to mention that it has been promoted by the National Information and Communication Security Taskforce, from the ***Executive Yuan***, since 2001, and the results have been positive for the Taiwan. The organization of the NCSP is the following:

Organization


National Information and Communication Security Taskforce
• Convener：Vice Premier
• Deputy Convener：Minister Without Portfolio and the Relative Head of Ministry.
• Collaborative Deputy Convener：Senior Advisor, National Security Council
• Committee Member： Deputy Secretary-General of Executive Yuan, Deputy Heads of the Ministries and Municipalities, Deputy Directors of the National Security Bureau, Scholars and Experts
Cyber Security Consulting Committee (Task Force Consulting Unit)
Department of Cyber Security, Executive Yuan (Staff Unit)
National Center for Cyber Security Technology (NCCST)
Cyber Protection System
Department of Cyber Security, Executive Yuan
Cybercrime Detection and Prevention System
Ministry of Internal Affairs/Ministry of Justice
Critical Infrastructure Protection System
Homeland Security Office, Executive Yuan
Other Cyber Security Related System
Other Competent Agencies
Critical Information Infrastructure Protection Group
Department of Cyber Security, Executive Yuan
Industrial Promotion Group
Ministry of Economic Affairs
Cyber Security Protection Group
Department of Cyber Security, Executive Yuan (Various Agencies)
Regulation and Standard Specifications Group
Department of Cyber Security, Executive Yuan
Awareness Education and Talents Cultivation Group
Ministry of Education
Cyber Protection of Overseas Mission Group
Ministry of Foreign Affairs
Cybercrime Protection and Control Group
Ministry of Internal Affairs/Ministry of Justice
Information and Communication Environment and Internet Content Security Group
NCC
(Related Agencies)

Note: Organization from the National Cyber Security Program of Taiwan (2021-2024) (p.25)

Also, this program was built as an interinstitutional effort, where all public institutions were part of this vision: due to the fact, that all the institutions are vulnerable of cyber-attacks, cyber-crime or cyber espionage, of course, the Ministry of Foreign Affairs is not the exception, and as they handle the cyber diplomacy it is important to understand how they protect the sensitive information. In fact, according to Audrey Tang Minister of Digital Affairs (MODA), Taiwan experiences 5 million cyberattacks attempts per day according to the National Security Council, so it's important to understand the phenomenon of the cyber security but the threats:

1. The intensification of personal data and digital certification leakage attacks.
2. The proliferation of ransomware attack risks.
3. The increase of threats of vulnerabilities of IoT and mobile devices.
4. APT targeted attacks to destroying supply chain security.
5. The hacking of cyber security (information) supplies destroying supply chain security.
6. The multiplication of critical information infrastructure security risk.[26]

The institutions in custody of the cyber security program and to protect the data/information are the National Institution of cyber security (NICS) and the Ministry of Digital Affairs (MODA)

[26] National Cyber Security Program of Taiwan (2021-2024) p.

which are the entities in charge of doing research in cybersecurity, propose new standards, impose new rules/laws and lead the cybersecurity maturity project in Taiwan.[27] In fact, The Ministry of Digital Affairs was created in January 2022 and was announce to a presidential order, and it is one of the achievements of this Cyber Security Program of Taiwan 2021-2024.

For this research it's important to mention the qualitive elements (Laws, policies, regulations, agreements) implemented in the program as, the "**cyber protection system**" (sponsored by the Executive Yuan) in charge of promoting the cyber security policies and task, such as the critical information infrastructure protection group, industrial promotion group, cyber security protection group regulation and standard specifications group, awareness education and talents cultivation group, cyber protection of overseas mission group[28].

First of all, the Critical Information Infrastructure Protection Group (sponsored by the Executive Yuan), "it's responsible of planning and promoting the security management mechanism of critical information infrastructure. The Industrial Promotion Group (depends on the Ministry of Economic Affairs), and is responsible of promotion the security industry between the industry, government, academic, and research resources. The Cyber Security Protection Group (sponsored by the Executive Yuan), is in charge of planning and promoting the security mechanism of communication and information application services of the government agencies. Regulations and standard Specifications Group (Structured by the Executive Yuan) responsible of research and formulation (revision) of cyber security-related laws and regulations, national standards, and formulation and maintenance of government agencies and reference guides. Awareness Education and Talents Cultivation Group, (structured by the Ministry of Education) is in charge of promoting fundamental cyber security education, improving the quality of cyber security in the population providing information and building a fully functional integrated platform, handling international-level, promoting industry-university exchanges, and reinforcing the cultivation of cyber security talents. And last but not least, the Cyber Protection of Overseas Mission Group (sponsored by the Ministry of Foreign Affairs MOFA) in charge of integrating the information and cyber management of the foreign agencies and representative offices to enhance their cyber security protection capabilities and reduce the risk of hacking and cyber security incidents.[29]

[27] Interview with Ph.D. Ricardo Neftali Pontaza Rodas, Senior Researcher at the National Institution of cyber security (NICS) and the Ministry of Digital Affairs (MODA), November 24, 2023.

[28] National Cyber Security Program of Taiwan (2021-2024)

[29] Ibid. pp. 25-26

In fact, this an interinstitutional effort, to coordinate and structured the regulations, laws, policies and promotion the cyber security strategy, in the public sector, working hand by hand with the private sector. In this program they worked in a duty division by agencies according to the strategy which are four. **Strategy no. 1** Attach high-level talents all over the world; cultivate independent power of research and innovation. **Strategy no. 2** the Promotion of public-private partnership collaborative governance, enhancement of the resilience of critical infrastructure**. Strategy no. 3** Utilization of smart and forward-looking technology; Proactive defense against potential threats. **Strategy no. 4** Budling a secure and smart IoT; enhancement of non-governmental protection energy.[30]

For research proposes we will focus on the Strategy no. 2 and Strategy no. 3, describe in the next duty division by agencies table, in order to describe a governmental route for Guatemala, to establish some institutions in charge, regulations, polices, people responsible of the cyber security program, etc.

[30] Ibid. pp. 65,66,67,68, 69.

Table no. 1

Duty Division by Agencies- Strategy no. 2

Strategy 2: The Promotion of public-private partnership collaborative governance; Enhancement of the resilience of critical infrastructure	
1. Build Public-private partnership Collaborative Governance Operational Mechanism in various fields	
1-1 Continue to promote the implementation of the cyber security management law, and review it in due course to respond to the trend of international cyber security protection	Department of Cyber Security, Executive Yuan; (Various Agencies)
1-2 Promote the implementation of cyber security protection baseline of critical infrastructure	Various CI Competent Agencies
1-3 Establish the maturity of cyber security governance in the industrial control field	Department of Cyber Security, Executive Yuan; (Various CI competent agencies)
1-4 Promote national-level cyber security risk assessment	Department of Cyber Security, Executive Yuan; (Various CI competent agencies)
2. The enhancement of personnel' cyber security awareness and reinforcement of cyber security capacity construction	
2-1 Set up Chief Information Security Officer (CISO) and strengthen personnel's cyber security professional capabilities	Various CI competent authorities
2-2 Establish a simulated field as a practical response capability; incorporate cyber security situation into teaching and training	Department of Cyber Security, Executive Yuan; Board of Science and Technology, Executive Yuan; (Various CI Competent Authorities)

3. Public-private partnership cooperation to deepen the exchange of information and implementation of response drills in normal times	
3-1 Improve the cyber security united defense mechanism (information sharing, response notification, cyber security monitoring) of the circital infrastructure	Department of Cyber Security, Executive Yuan; Various CI Competent Authorities
3-2 Regularly conduct public-private united offensive and defense drills	Various CI Competent Authorities
3-3 Handle cross-regional (or transnational) offensive and defensive drills for critical infrastructure	Department of Cyber Security, Executive Yuan; (Various CI Competent Authorities)

Note: Information from National Cyber Security Program of Taiwan (2021-2024)

Table no.2

Duty Division by Agencies- Strategy no. 3

Strategy 3: Utilization of smart and forward-looking technology; Proactive defense against potential threats	
1. Continue to promote centralized sharing of government information (cyber) security	
1-1 Connect with the independent needs of national defense and develop the ecosystem of the domestic cyber security industry	National Development Council; Department of Cyber Security of Executive Yuan; (Various agencies)
1-2 Establish the mechanism to actively discover, report and repair the vulnerabilities of the information and communication system	Department of Cyber Security, Executive Yuan; (Various agencies)
2. Expand international participation and deepen cross-border intelligence and capital sharing	
2-1 Development of forward-looking research and technology application of active defense	Ministry of Economic Affairs
2-2 Integrate domestic and foreign sources of information, and deepen international cooperation	Department of Cyber Security, Executive Yuan;v (Various CI Competent Authorities)
3. Defend in Advance to Block the Attack at Borders	
3-1 Apply emerging technologies to quench effective intelligence and develop proactive defense technologies	Department of Cyber Security, Executive Yuan
3-2 Improve the comprehensiveness of the defense-in-depth of the government service network.	Department of Cyber Security, Executive Yuan; National Development Council
4. Enhancing the power of technological investigations to prevent emerging cybercrimes	
4-1 Strengthen the detection capabilities of emerging cybercrimes	Ministry of Internal Affairs; Ministry of Justice
4-2 Improve the source tracing and tracking capabilities of cyber security events	Ministry of Internal Affairs; Ministry of Justice; Department of Cyber Security, Executive Yuan
4-3 Strengthen the investigation mechanism of cross-border cybercrime	Ministry of Internal Affairs; Ministry of Justice

Note: Information from the National Cyber Security Program of Taiwan (2021-2024)

In addition, for the implementation of the strategy no. 2, the drills and exchange of information between the private and public sector, also to develop the personnel capabilities in order to improve the cyber security program. To establish the maturity of cyber security governance, it's an important step, to reaffirm the protection the computer system. Actually, "for the following decade, Taiwan will look forward to improve the maturity of the cybersecurity of their institutions. This maturity increase will be done by applying cybersecurity's best-practices and enforcing the requirement of certifications for the private sector. The idea is that it is extremely hard to protect the private sector just by the public sector. Ideally, the private sector must learn to protect itself, and the public sector will be the orchestrator of the interactions between entities in the private sector".[31]

The maturity of the cyber security strategy becomes with the capability of reaction during a cyber-attack, and also with international certifications such as the ISO 27001 ITIL v3, COBIT 4.1, ISO/IEC 27002:2005, in both sectors. Also, by evaluating the levels of maturity, the that a company or organization take to respond its crucial in a cyber-attack.

Challenges: During the cyber security program 2021-2024, there are some challenges to be mention, such as the cyber-attacks from China that have been so transformed to be tacit and effective that most citizens of Taiwan cannot see them. [32]. As this is a recent phenomenon there are always challenges to confront and this also help to cultivate and improve the cyber security program.

"There were three fundamental challenges that were raised at the last phase of the NICS program. First, education for personnel. It was mandatory to train the personnel in the certificates that were planned to be enforced to the private sector soon. Second, allocation of personnel and budget for short- and long-term projects. The projects' proposals needed clear development plans and clear and achievable goals, which required a substantial amount of discussion and planning. Third, personnel retention was a problem that required a quick solution. As with any new institution, the turnover rate of personnel was high at the beginning, so creating a clear schematic of the personnel

[31] 31. Interview with Ph.D. Ricardo Neftali Pontaza Rodas, Senior Researcher at the National Institution of cyber security (NICS) and the Ministry of Digital Affairs (MODA), November 24, 2023.

[32] 32. Interview with Ph.D. Yen Pin Su Professor from the Department of Political Science of the National Chengchi University, September 9, 2023.

with attributions and responsibilities was providential to avoiding overwork and creating an effective work path.”[33]

4.2 The Republic of China (Taiwan) Cyber Diplomacy:

The Republic of China (Taiwan) had been improving its cyber-security strategy by including elements as the exchange of international personnel and the consolidation of the Cyber Protection of Overseas Mission Group in order to protect the data from the foreign agencies and the representative offices, so they can reduce the risk of a cyber-attack, cyber espionage or any incident related to the cyber security.

Assisting to international forums about cyber security have been increasing the knowledge and possible allies in the international arena. According to Pontaza (2023), the United States has proved to be one of the greatest international allies in terms of cybersecurity. The US has multiple institutions aiming to guide the Research and Development of cybersecurity, cybercrime prevention and correction, and the creation of guidelines for the private sector. Besides the US, the European Union (UE) also has the development of cybersecurity measures as one of their primordial goals for this decade. Institutions like ENISA provide similar guidelines to NIST does in the US. Additionally, Canada and Israel have been increasing the budget and investment in cybersecurity lately, so their presence in the cybersecurity environment as leaders will be noticeable soon. [34]These countries are allies, as the cyber security research can be exchange to improve the strategies and strengthen the cyber diplomacy. Specifically, the Ministry of Foreign Affairs (MOFA) has different challenges due to the international and geopolitical situation of Taiwan.

As a matter of fact, for Taiwan, cyber diplomacy is a kind of international cooperation for enhancing the freedom of speech through cyber platforms and cyber security. [35] This improves and save governmental resources, as the information is sent through a digital via and it’s no longer necessary for the diplomats to travel for meetings. Of course, this represents a challenge because the information must be protected in the cyber space.

[33] Interview with Ph.D. Ricardo Neftali Pontaza Rodas, Senior Researcher at the National Institution of cyber security (NICS) and the Ministry of Digital Affairs (MODA), November 24, 2023.

`[34] Ibid.

[35] Interview with Ph.D. Yen Pin Su Professor from the Department of Political Science of the National Chengchi University, September 9, 2023.

4.3. Guatemala´s cyber–Security Strategy nowadays:

According to EU-Central America Association Agreement (2022), in Guatemala exists a cyber-security strategy since 2018; this represents the first step for this Central American country to establish some guidelines and plans to have a reliable cyber security. The proposed of this cyber security strategy is:

> a) Regulate the protection of digital information systems in the public and private sectors in order to guarantee the continuity of their services; b) Establish coordination organizations (CSIRT-GT) to implement the national cyber security; and c) Design a national protection plan for critical infrastructures for strengthen contingency and recovery plans. Guatemala's CSIRT-GT is an incident response team under the supervision of the Ministry of the Interior 196 and is a member of the CSIRT Americas network (p. 4)

This strategy was created for the Ministry of interior, although, it's a complete cyber security strategy in paper, but it's about political willing and governmental budget missing in order to improve this cyber security strategy in the past governments; that is the main reason why to describe the cyber security program of Taiwan will be a great strategy for Guatemala.

On 2022, the "Congress of the Republic of Guatemala approved Decree 39-2022, which contains the Law on Prevention and Protection against Cybercrime. The law includes criminal sanctions for cyber activities that violate personal data, sensitive computer data, confidentiality, integrity, and availability of information and data stored in computer systems or systems that use information technology and communications to transmit information by such means. The regulations issued seek to strengthen computer security and promote the responsible use of digital tools. In addition, they create the Institutional Security Center for Technical Response to Computer Incidents. On August 24, 112 deputies to the Congress of the Republic of Guatemala voted in favor of the objections to Decree and as a consequence, the so-called Cybercrime Prevention and Protection Law, created by bill 5601, was shelved. Due to its filing, the Law will no longer be sent to the Executive for sanction and publication, nor will it take effect. Several experts, academics and several other opponents concluded that said decree is dangerous because it could be used to limit freedom of expression and criminalize comments towards officials and political figures who have been criticized and questioned for the performance of their duties". [36]

For the next governments should be a priority or part of the national security to strengthen the cyber security program, because this phenomenon affects the collective and individual users who have been suffering of cyber-attacks from group of criminals who stole big amounts of the money, also customer's data, etc. Also, for Kaspersky (2022) is a cyber-security and digital privacy company, said, during the 2021 and 2022, Guatemala was the most Latin-American country that suffers from cyber-attacks, especially malware attacks, it increases in 30% due to the pandemic.[37] Without mentioning the big problem that is ***phishing,*** it consists in stealing personal information through fake web pages, such as banking credentials, social networks, online services, using financial services to steal passwords and payment data such as credit cards. According to the interviews with cyber security experts from Guatemala, there is a Cybersecurity strategy approved in Guatemala in 2018, there is a lack of follow up regarding the governmental budget, the qualify personnel and a strong law infrastructure. [38]

4.3.1 Challenges for Guatemala in the cyber-diplomacy filed:

There are different challenges Guatemala faces in the cyber diplomacy field. This is due to the fact, that there is a correlation between the Cybersecurity strategy and the cyber diplomacy variables. In other words, if the country does not have a strength "***Cyber security strategy"*** we won't be able to protect the most valuable resources, such as the sensitive information of the citizens' data. Guatemala it's looking for new ways to find allies in Latin America and has been requesting the support of the Organization of the American States. Back in the 2020 the Organization of American States was the location to foster cooperation and exchange of best practices on cyber diplomacy, cybersecurity and cyberspace, though, for example, the establishment of working groups, other dialogue mechanisms, and the signing of agreements among states.[39]

[36] EU-Central America Association Agreement 2022 p.4
[37] Kaspersky Daily. https://latam.kaspersky.com/blog/panorama-amenazas-latam-2022/25509/
[38] Interview with Ph.D. Armando Monzon Escobar Researcher from INCIBE Guatemala on March, 14, 2023
[39] Organization of American States OAS (2020) https://mfcs.oas.org/Home/CountryDetailMFCS?measureId=40&countryId=95&year=2020

There are a lot of challenges regarding the critical infrastructure in both sectors (private and public) but specially in the Ministry of Foreign Affairs of Guatemala, it's imperative to construct and approved some regulations, laws, and policies to protect our systems.

These are some recommendations that can be applied to Guatemala. "First, as stated in ISO 27-001, there should be an enforced standardization of the process of logging the processes, corrections, and operations performed by the users in high-level positions (for example: DB managers, Network managers, IT directors, etc.) Second, there should be a continuous training for the users and administrators. The continuous training should be mandatory and enforcing the learning and implementation processes of cybersecurity's best practices. Third, there should be a clear and standard process performed while discarding used/broken equipment. Cybersecurity attacks are extremely common in discarded equipment, so the training of the personnel regarding this will create a cleaner process in terms of equipment destruction. Finally, there should be an overall training of the personal regarding online hygiene, as multiple successful attacks are done by deceiving/tricking the users to click malicious links, submit sensitive login information to fake forms, install unsecure software in network devices, etc"[40].

These recommendations apply in both sectors, but specially to the technical personnel of the Ministry of Foreign Affairs (MOFA) of Guatemala, so we can improve our cyber diplomacy but more important to protect the data/information of the Guatemalan people. A good recommendation, it's built stronger connection with international community of cyber security by attending the activities and signing agreements. Also, build routine channels with the United States for cyber security issues[41].

[40] Interview with Ph.D. Ricardo Neftali Pontaza Rodas, Senior Researcher at the National Institution of cyber security (NICS) and the Ministry of Digital Affairs (MODA), November 24, 2023.

[41] Interview with Ph.D. Yen Pin Su Professor from the Department of Political Science of the National Chengchi University, September 9, 2023

Conclusion

The cyber security is a recent concept which is part of the cyber space including physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by the citizens of a country. In fact, it's very dynamic and changing, as the technology is advancing every day, so the human beings need to keep an eye on how their data/information is protected and handle by the companies, platforms, banks, institutions, organizations, etc. or whoever uses and requested our information online.

Depending on the cyber security strategy that a country handles, the protection of the data is either strong or can be penetrated by any individual or a criminal group (cyber terrorist, cyber criminals, hackers, etc.), and it is a good time to learn and analyze this phenomenon looking for the best strategies, to protect the most important resources which are the information of the citizens.

In this research we found some remarkable elements to describe and design a route for Guatemala to strengthen the cyber security strategy and to improve cyber diplomacy. For example, to establish public-private partnership working together to create a safety cyber security environment. To invest in research institutes to cover also the public sector and to make the drills standardizing the evaluation (Level A/B) to be used in both sectors.

The creation of the Ministry of Digital Affairs it's an achievement reached by the Government of Taiwan, as they handle the cyber security strategy program regulated form the public sector to the private sector. The proposal for Guatemala is to start with an office belonging to the Ministry of Interior, while they can reach more budget to establish a Ministry, due to the fact, that the cyber security should be part of the national interest. But we need to create this Ministry so all the policies, laws and regulations will be leading by this future Ministry. As the government budget of Guatemala it's been reduce by other priorities, the recommendation is to look forward international cooperation and once it's established, keep working with our own financial resources.

Also, we need to invest in our human resources, working hand by hand between ministries (Ministry of Education in coordination with universities, Ministry of Foreign Affairs, and Ministry of Digital Affairs or the Ministry of Internal meanwhile the other ministry is created) as an interinstitutional effort in order to cultivate new talents in the cybersecurity and cyber diplomacy field. The recommendation is to create bachelor, master and Ph.D. focusing on the cyber security topic and promoting scholar exchange between nations, by creating incentives for the better students, so they can be part of the exchange program.

As a matter of fact, Guatemala and Taiwan have been diplomatic allies for more than 80 years, and recognizing the success of Taiwan's cyber security program, the recommendations is to compromise a percentage of the scholarships (Bachelor, master or Ph.D.) at least 20% for the best Guatemalan students related to the engineering field and increase the human resources to strengthen our cyber security strategy.

Another achievement from the cyber security program of Taiwan is the recruitment of international talents to be responsible for the short-to-mid-term applied technology research required by the agencies. The fact of recruiting foreign talent it's a high-level step, so this talent can train the personnel who will be handling and proposing the policies and regulations. This is an element to consider, because Guatemala can take advantage of the international organizations and requests the assistance and experience of another countries, as the platform of the Organizations of American States (OAS) and sign some agreements requesting the international talent to come to Guatemala and train our people. Once we set up the agreements to have the internationl talent, we need to integrate domestic and foreign sources in the same platform to enhance threat collection and active detections capabilities in order to promote standard intelligence formats.

Regarding the international relations and the cyber diplomacy, it's important to invest in the computer systems, so the information, agreements and meeting can be protected. Also, work on annual and monthly trainings to all diplomats and the people involved in the cyber diplomacy filed. In addition, to promote a cyber security competition (between think tanks, universities, private research entities, etc.) in order to recruit talents on the cyber security field to get quality teachers who can spread the knowledge about this topic.

For Guatemala the improvement in the legal infrastructure, it's crucial to start walking in the right path; and this is a duty of the Congress of the Republic of Guatemala, as they already tried to approved one decree back in the 2022, it’s necessary to review it and change what can provoke a misunderstanding in the future; but of course, it’s necessary to have a law typification about the cybercrime.

The cyber security Strategy of Guatemala must include the training to the citizens so they can be aware of the risk of a cyber-attack, how they can be victims of these criminal groups or individuals and how they can avoid it, but this information must be spread by the public and private sector. working in a partnership.

Describing two out of the four strategies, from the Blueprint initiative provides of some important elements; for example, the strengthen the detection of capabilities of emerging cybercrime it’s a task that the Ministry of Internal Affairs and the ministry of Justice. In order to enhance the power of the technological investigations to prevent the cybercrime. This means that, once the typification of the cybercrime is approved by the Congress of Guatemala, the Ministry of Justice and of Internal Affairs must be in charge of the detection of cybercrime and prevent it.

In conclusion, the cyber security strategy should be handled, regulated and control by the government in order to standardized the process and formats. Of course, the academia plays an important role in this phenomenon, changing the educational curricula in the schools, to start talking about the cyber security the threats and the windows of opportunities, and the partnership between universities (the public and private universities) is also a key to increase the amount of professional who handle the cyber security.

Bibliography

Attatfa, A., Renaud, K., & de Paoli, S. (2020). Cyber diplomacy: A Systematic Literature Review. *Science Direct*, *176*, 60–66. Retrieved from June 6, 2022 https://www.sciencedirect.com/science/article/pii/S1877050920318317

Barrinha, A. and Renard, T. (2017) Cyber Diplomacy: the making of an international society in the digital era. *Global Affairs* Volume (3) Nos 4-5 p. 353-361.

Barston, R. (1997) Environmental Diplomacy. *Modern Diplomacy.* Second Edition. Routledge

Bjola, C., & Kornprobst, M. (2018). *Understanding International Diplomacy* (2nd ed.). Taylor and Francis. Retrieved from https://www.perlego.com/book/1574488/understanding-international-diplomacy-theory-practice-and-ethics-pdf (Original work published 2018)

Burgers, T., Hellmann, M., & Rimaniuk, S. (2021). In the line of fire, Taiwan's legal, political and technological Cybersecurity posture. *Routledege Companion to Global Cyber-security strategy*. https://doi.org/10.4324/9780429399718

C. Barry, L. Lee & M. Rewers. International Cyber Security Conference Final Report, Center for Technology and National Security Policy, National Defense University, June 2009.

Canongia, C., & Mandarino, R. 2014. Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGI Global. http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

Craigen, D., Diakun, N., & Purse, R. (2014, 1 octubre). *Defining Cybersecurity*. Technology Innovation Management Review. Recuperated on June 9, 2022, de https://www.timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

Cyber Security: Protecting Our Federal Government from Cyber Attacks, the 2009 data breach investigations report, 2009.

Cyber security sector in Central America. Sector Fiche. November 2022. https://trade.ec.europa.eu/access-to-markets/en/country-assets/euca_05_Cybersecurity%20sector%20in%20Central%20America.pdf

Deibert, R. & Rohoziinski, R. (2010) Liberation Vrs. Control in Cyber Space. Journal of Democracy. Vol. 21. p. 14

EU-Central America Association Agreement (2022) Retrieved from https://trade.ec.europa.eu/access-to-markets/en/country-assets/euca_05_Cybersecurity%20sector%20in%20Central%20America.pdf

Jing, B. (2019, 1 September). *Cybersecurity as a Sine Qua None of digital economy: Turning Taiwan into a Reliable Digital Nation?* Disinformation, Cybersecurity, & Energy Challenges.

Recuperated on June 6 2022 from https://www.stimson.org/wp-content/files/file-attachments/StimsonTaiwanSecurityBrief2019.pdf

Kapersky Daily (2023). Financial attacks are growing in Latin America and concern about the use of piracy increases https://latam.kaspersky.com/blog/panorama-amenazas-latam-2022/25509/

Leguey-Feilleux, J. (2009) The Impact of Technology. *The Dynimics of Diplomacy*. pp. 85-100. Lynner Rienners Publishers, UK.

Mamchi, O. (2023). The significance of Cyber Diplomacy in the 21st Century. Best diplomat. **https://bestdiplomats.org/cyber-diplomacy/**

Ministry of Digital Affairs (August 3, 2023) Cyber security Policies and Regulations.
https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648

National Cyber Security Strategy of the Republic of Guatemala. (2018) https://ogdi.org/ogdi/uploads/2021/08/Estrategia-Nacional-de-Seguridad-Cibernetica.pdf

National Information & Communication Security Taskforce-Cybersecurity Development Program. (2013, 25 December). Cybersecurity Development Program. Cited on June 4 2022, from https://nicst.ey.gov.tw/en/807491F2A43DF876

Organization of the American States (2020). Retrieved from https://mfcs.oas.org/Home/CountryDetailMFCS?measureId=40&countryId=95&year=2020

Painter, C. (2018). Diplomacy in Cyberspace. The Foreign Service Journal https://afsa.org/diplomacy-cyberspace

Pigman, G. (2010). Technological Change and Diplomatic Process. Contemporary Diplomacy. Polity Press, UK

Pryor, C. (2018). Taiwan´s Cybersecurity Landscape and Opportunities for Regional Partnership. Cited on March 7, 2023 from https://www.jstor.org/stable/pdf/resrep22549.5.pdf

Riordan, S. (2019) Cyber-diplomacy: Why Diplomats Need to Get into Cyberspace. Public Diplomacy Magazine. https://publicdiplomacy.org/docs/CyberDiplomacy+Magazine.pdf

Sciencedirect Magazine (2018) The Practioners of the cyber diplomacy. file:///C:/Users/MONICA%20POZUELOS/Desktop/MONICA%20POZUELOS/BECA%20A%20TAIWAN/ARTICULO%20ACADEMICO/MARCO%20TEORICO/CYBERDIPLOMACIA.pdf

Singer, P. W., & Friedman, A. 2013. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press

Uma M. and G. Padmavathi (2013). A Survey on Various Cyber Attacks and their Classification. http://ijns.jalaxy.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf

US Cyber Diplomacy in the Era of Growing Threats (2018). Statement of Mr. Christopher Painter, Commissioner Global Commission for the stability of Cyberspace. file:///Users/monicapozuelos/Downloads/810670%20(1).pdf 31

Zhou-Peng Liao, C. (2018). Digital Nation & Innovative Economic Development Program in Taiwan. IAC Online Journal CIO and Digital Innovation, 20–22. Recuperated on June 5, 2022 from https://iacio.org/wp-content/uploads/2019/04/IAC-Journal-of-CIO-and-Digital-Innovation-2018_rev4_final1.pdf#page=20