Faculty of Humanities and Social Sciences

Master in International Security Management

Final thesis

China's Impact on Taiwan's Critical Maritime Infrastructure: Assessing Key Challenges

Luis Alberto Moreno Martin-Portugués

2025-2026

Table of Contents

1. Introduction

1.1 Strategic Background

Until very recently, critical maritime infrastructure was seen mainly as a logistical component in the functioning of modern societies, especially in relation to transport needs, both for goods and for information, which form the backbone of modern societies. Submarine cables carry our data, while energy terminals and ports are essential components, although they do not receive much attention from a geopolitical point of view. However, in recent years it has also become clear that these infrastructures can become targets. They create dependencies that can be exploited by governments and other actors to gain an advantage and achieve strategic objectives.

This reality is especially relevant in the Indo-Pacific, home of some of the world's busiest trade routes and where some of the world's most important ports are located. Both elements are highly sensitive to disruption, with very important consequences for regional stability as Taiwan occupies a particularly vulnerable position in this region and represents a significant concern for global stability. On the one hand, the island is a strategic node in the global semiconductor supply chain. Its most important company, TSMC, produces more than 90% of the world's most advanced chips (Byman et al., 2024). This means that any event affecting the island has a direct impact on the global economy.

On the other hand, Taiwan imports more than 95% of the energy it uses and has very limited storage capacity, especially in the case of LNG (Byman et al., 2024). For this reason, it has a strong need to keep the whole logistics supply system working. Its economy is open, dynamic and export-oriented, but these same strengths can become fragility if there are a partial or total disruption of trade flows and the data needed to maintain this activity. Ports, LNG terminals, port facilities, submarine cables, maritime routes, AIS systems and logistics platforms are not independent elements. They are part of a highly complex system, which is difficult to keep operational if an actor tries to damage it. Therefore, Taiwan is a very interesting case for analysing critical maritime infrastructure and the risks it represents for advanced economies that depend heavily on communications and international trade.

1.2 Literature Overview

Critical maritime infrastructure has usually been studied from a technical or operational point of view. Ports, submarine cables, energy terminals and logistics systems were often treated as engineering assets, rather than as objects of geopolitical competition. This has changed in recent years. The disruption of supply chains, the growing attention to undersea cables, and the use of coercive actions below the level of open war have pushed this topic into the field of security studies. In the case of Taiwan, this change is particularly relevant. The island depends heavily on maritime connections for trade, energy imports, communications and military resilience. For this reason, the literature on Taiwan's critical maritime infrastructure brings together several debates: maritime security, hybrid warfare, cyber threats, economic coercion, blockade scenarios and cross-Strait relations.

A first group of studies deals with critical maritime infrastructure as a security problem. Bueger and Liebetrau (2023) argue that this infrastructure should not be understood only as a group of physical assets, but as part of a wider system involving legal, political, economic and technological dimensions. This approach is useful for Taiwan because its ports, submarine cables and LNG terminals are not independent elements. They are connected to each other, and pressure on one part of the system can create consequences in others. Fridbertsson (2023) also stresses the role of technology in protecting maritime infrastructure, especially through monitoring, surveillance and resilience tools. Su (2026), from a maritime governance perspective, also supports the idea that protection must be multi-domain. These works are important because they help move the discussion beyond a view of maritime infrastructure as only physical.

A second area of the literature focuses on submarine cables. There has been a lot of literature on submarine cables on the recent years, as these have received growing attention after incidents in Europe and East Asia showed how exposed undersea systems can be, and how difficult it is to attribute responsibility when damage occurs. Asia-Pacific Economic Cooperation (2012) had already pointed out the economic costs of submarine cable disruptions in the Asia-Pacific. More recent works have applied this concern to Taiwan. Chen (2025) studies the limits and possibilities of Taiwan's cable security, while Huang (2025) looks at how Taiwan could strengthen this area. Kim (2025) places cable security in the broader East Asian context, and Cannon, Matsuo and Matsuda (2026) add a more geographical perspective by linking cables, risk and geopolitics. Together, these

studies show that submarine cable vulnerability is not simply a technical issue. It is also shaped by geography, repair capacity, redundancy, political risk and the behaviour of hostile actors.

A third group of literature examines hybrid threats and grey-zone operations. Hoffman (2007) provides an early conceptual basis for hybrid war, understood as the combination of conventional and irregular methods. This concept is useful in the Taiwan case because China does not need to launch a full military attack to put pressure on the island. Helmus (2024) explains how China's maritime grey-zone activity can involve coast guard vessels, maritime militia, civilian ships and constant pressure around contested areas. Macias and Jensen (2025) provide a data-based analysis of Chinese maritime activity near Taiwan and show that this pressure is persistent rather than occasional. Insisa (2026) applies this logic to submarine cables and the information domain, stating that cable disruption could have both practical and psychological effects. Germond (2026) also contributes to this debate by suggesting that threats to critical maritime infrastructure should be analysed in a context where ambiguity can be as important as direct damage.

Blockades in the case of Taiwan have also been a widely analysed topic in recent years, so there are many highly relevant studies on this issue. Jestrab and Hadley (2023) analyse how a maritime blockade of Taiwan could be used by the People's Republic of China as a tool of fear and coercion. The Center for Strategic and International Studies (2025) also studies a Chinese blockade through wargaming, focusing on the economic and military pressure that this scenario would create. These works are useful, but they normally focus on broader military or strategic outcomes. This thesis takes a more specific angle. It does not ask whether China could blockade or invade Taiwan, but how different forms of maritime pressure could affect ports, LNG terminals, submarine cables and shipping routes. This distinction matters because coercion does not need to reach the level of a full blockade to create serious disruption.

Cyber threats are another important part of the literature. Taiwan's maritime infrastructure is not only physical. Ports, logistics platforms, energy terminals and communications networks all depend on digital systems. Lewis (2023) explains how cyberattacks against critical infrastructure could be used in a Taiwan scenario. Byman, Jones and Blanchette (2024) include cyber operations among the tools that China could use to pressure Taiwan and test its resilience. The Taiwan National Security Bureau (2026) offers a Taiwanese perspective on Chinese cyber threats to critical infrastructure, while

Lee (2026) reports the high volume of cyberattacks directed at Taiwan's infrastructure. Butler (2024) adds the information operations dimension by analysing Chinese-linked online influence activity. This literature shows that cyber and information tools can support maritime pressure by creating confusion, disrupting services or weakening public trust during a crisis.

The economic perspective is also central. Reinsch and Whitney (2025) underscore Taiwan's importance to global economic security, particularly in semiconductors. Taiwan Semiconductor Manufacturing Company (2025) also shows the importance of Taiwan's chip industry for global supply chains. This matters because the disruption of Taiwan's maritime infrastructure would not only affect Taiwan. It could also damage international technology markets. The U.S. Energy Information Administration (2026) is also useful because it highlights Taiwan's dependence on imported energy. This dependence makes ports, LNG terminals and maritime routes essential not only for the economy, but also for social stability and national security.

In addition to Western and Taiwanese sources, Chinese sources are necessary to understand how Beijing understand Taiwan and the strategic environment around the island. The Taiwan Affairs Office and the State Council Information Office (2022) present Taiwan as part of China's national reunification project. This is useful for understanding China's official narrative. The State Council Information Office (2019) also gives insight into China's defence priorities, especially sovereignty, territorial integrity and military modernisation. Statements by the PLA Eastern Theater Command on Joint Sword-2024A and Joint Sword-2024B show how China see military exercises around Taiwan as a response to separatism and foreign interference. These sources are important because they link Chinese military pressure with political signalling.

Chinese legal and regulatory sources also add value. The State Council of the People's Republic of China (2021) regulation on critical information infrastructure shows that China itself treats sectors such as communications, energy and transport as national-security assets. This is relevant because it shows that critical infrastructure is not only a Western analytical concept but also appears in Chinese security thinking. The National People's Congress (2021) Coast Guard Law is also useful for understanding maritime grey-zone dynamics, because it strengthens the role of the China Coast Guard in protecting what Beijing defines as maritime rights and interests. Chinese academic

sources, such as Cao (2022, 2023), can also help show how some Chinese scholars discuss crisis management, escalation and maritime blockade in the Taiwan Strait.

Even with this growing literature, several gaps remain. First, many studies focus on one type of infrastructure, especially submarine cables, but give less attention to the interaction between cables, ports, LNG terminals and digital systems. Second, much of the literature concentrates on invasion or full blockade, while limited disruption and ambiguous coercion receive less attention. Third, Taiwan is often presented mainly as the target of Chinese pressure. However, Taiwan can reduce some vulnerabilities through redundancy, stockpiling, cybersecurity and crisis planning.

This thesis addresses these gaps by analysing Taiwan's critical maritime infrastructure as an interconnected system exposed to Chinese pressure. It combines the physical dimension of maritime infrastructure with the cyber dimension of modern coercion. It also includes Chinese official and academic sources, not to accept Beijing's position, but also not to reject it, so to understand how China frames Taiwan, maritime security and critical infrastructure. This allows for a more balanced analysis of how China could affect Taiwan's ports, energy flows, submarine cables and maritime connectivity, while also considering how Taiwan could respond and reduce some of these risks.

1.3 Problem Statement

Taiwan remains one of the most sensitive issues in China`s foreign and security policy. Its integration into the People's Republic of China is of maximum interest to the Chinese leadership, as shown by the recent summit between the United States and China (Cheng, 2026). Beijing considers Taiwan to be part of its territory and has repeatedly stated that unification is a non-negotiable objective. At the same time, Taiwan is a critical element in the global supply chain, because its semiconductor industry is essential for the functioning of technology industries worldwide. This creates a structural tension. On one hand, China may have incentives to increase pressure on Taiwan. On the other hand, a large-scale conflict would be extremely risky. It could damage the Chinese economy, trigger international sanctions, disrupt global markets and involve the United States and other Taiwan allies. For this reason, China has strong incentives to use instruments that apply pressure without crossing the threshold of war.

Taiwan's maritime dependence makes this type of strategy easier. The island depends on maritime access mainly to import energy (Byman et al., 2024), as well as raw materials and basic goods. Its LNG terminals, oil facilities and ports are critical not only for the economy, but also for social stability and readiness against the permanent threat of a Chinese invasion. Taiwan's digital connectivity also depends on submarine cables and communications infrastructure that are difficult to defend and repair in a crisis. There is an important dependence between physical and digital infrastructure. A port is not only a physical space where ships dock. It is also a digital system that coordinates cargo, customs, schedules, cranes, storage, energy flows and security access. An LNG terminal is not only a storage facility. It also depends on digital control systems, maritime transport schedules, insurance and security procedures. This means that an interruption or disruption in any of these elements can create cascading effects across the rest of the system.

The problem addressed by this thesis is that Taiwan's critical maritime infrastructure is highly exposed to Chinese pressure because of the combination of geographical proximity, maritime dependence, energy vulnerability, interdependence between infrastructures and digital interdependence. China could exploit these vulnerabilities through a wide range of tools that remain below the threshold of open war (Loik, 2024). The main research question is: To what extent, and through which mechanisms, can China alter Taiwan's stability through its critical maritime infrastructure?

Rather than testing formal hypotheses, the thesis uses a qualitative analytical framework to assess how exposure, criticality and recoverability shape Taiwan's vulnerability to Chinese pressure. The expectation is that cyber and hybrid pressure may be more useful for China than military attacks because they can create disruption while preserving ambiguity.

1.4 Theoretical Framework

This thesis uses securitisation theory as its main theoretical framework. The theory was developed by the Copenhagen School, particularly through the work of Barry Buzan, Ole Wæver and Jaap de Wilde. Its main contribution is that it understands security not only as an objective reality, but also as a political process. In other words, an issue becomes a security concern when relevant actors present it as an existential threat and argue that it requires special attention or exceptional measures to be managed. For securitisation to

take place, three elements are needed: a securitising actor, a referent object that is presented as needing protection, and an audience that accepts, rejects or questions this frame (Buzan et al., 1998).

The mechanism of securitisation is therefore not automatic. It depends on how a threat is presented, who presents it, and whether the audience considers the argument credible. In the original Copenhagen School approach, the speech act is central: by naming something a security threat, political actors seek to move it out of normal politics and into the realm of urgent security action (Buzan et al., 1998). However, later authors have shown that this process also depends on the wider context. Balzacq (2005) argues that successful securitisation is audience-centred, context-dependent and linked to power relations. This means that a security claim is more likely to succeed when it connects with existing fears, political interests or institutional practices. Stritzel (2007) also stresses that securitisation should not be seen only as a single speech act, but as a broader process in which discourse, social context and the position of the actor all matter.

This is important for the analysis of critical maritime infrastructure because infrastructure does not become a security issue simply because it is technically important. They become securitised when political or security actors manage to present their disruption as a threat to something wider, such as national survival, economic stability, energy security or strategic autonomy (Balzacq, 2005; Stritzel, 2007). A port, a submarine cable, a shipping route or an LNG terminal is not automatically seen as a security issue. It becomes one when security actors state that its disruption could affect national security, economic continuity, energy supply or social stability. From this perspective, infrastructure is more than a technical asset. It becomes part of a wider security debate.

This is particularly important in the case of Taiwan. The island depends heavily on maritime connectivity for energy imports, trade, digital communications and the functioning of key industries such as semiconductors, that its critical for global technology. Securitisation theory helps explain why these infrastructures have gained more attention in Taiwan's security thinking. They are vulnerable assets, but they are also connected to broader concerns about resilience, deterrence and national survival. This matters especially because pressure from China does not need to take the form of a military attack. It could also involve grey-zone activities, cyber operations, maritime pressure, economic coercion or a limited blockade. These types of pressure may remain

below the threshold of open war, but they can still affect the systems that Taiwan needs to function.

At the same time, not every discussion about infrastructure should be treated as securitisation. Many infrastructure debates remain technical, economic or administrative. For this reason, the analysis focuses only on cases where maritime infrastructure is connected to broader strategic concerns, such as national survival, energy security, or resistance to potential Chinese coercion. This distinction is important because it avoids using the concept too broadly.

Securitisation theory is also useful because it allows to connect physical and non-physical dimensions of security. Critical maritime infrastructure can also be affected through cyberattacks, information operations, commercial uncertainty or political intimidation. The value of the theory is that it helps explain how these different forms of pressure come to be understood as security threats, even when they do not amount to conventional war.

Overall, this framework supports the central purpose of the thesis: to assess how China could potentially affect Taiwan's critical maritime infrastructure, and how these infrastructures are increasingly understood within Taiwan's broader security strategy. It provides a link between material vulnerability and political interpretation. On the one hand, Taiwan's maritime infrastructure can be examined in terms of exposure, criticality and recoverability. On the other hand, securitisation theory helps explain why these same infrastructures are increasingly framed as essential to national resilience and strategic survival (Potcovaru & Mustață, 2026). In this way, the thesis does not treat critical maritime infrastructure simply as a collection of physical assets. It analyses it as part of a wider security process, where ports, cables, terminals and maritime routes become politically meaningful because of what they represent for Taiwan's survival, stability and capacity to resist coercion.

1.5 Structure of the Thesis

The thesis is divided into six sections. This introduction presents the problem to be analysed, the hypotheses to be tested, the theoretical framework and the expected results. The second section defines the research perimeter, establishes the main elements both in general terms and in their application to the geographical area of study, and presents the analytical framework. The third section reviews a first group of scenarios related to

Chinese strategic approaches to CMI disruption, including grey-zone operations and maritime militia and Coast Guard activities, from both a logistical and economic point of view. It also compares the different strategies from several perspectives. The next section reviews a second group of scenarios related to cyber threats against Taiwan's critical maritime infrastructure. This section examines the digitalisation of maritime infrastructure, Chinese cyberattack strategies, and some cyber disruption scenarios. It also concludes with a comparative analysis. The fifth section reviews the implications of these strategies for Taiwan's stability, develops a series of policy recommendations and analyses their effects on regional security. Finally, the thesis includes a conclusions section, summarising the key findings, answering the research questions proposed at the beginning, and reviewing the contribution made and the possible future lines of research.

The thesis assesses Taiwan's critical maritime infrastructure through three variables: exposure, criticality and recoverability. Exposure refers to the likelihood that an asset can be targeted or pressured; criticality refers to the importance of the function it performs; and recoverability refers to the ability to restore that function after disruption.

The thesis expects to show that, under many crisis conditions, a limited and ambiguous strategy could be more attractive for China than a total blockade or a direct attack. It is more likely that China could try to achieve its strategic objectives through hybrid pressure combining cyber operations, maritime grey-zone activities and economic coercion. These tools could allow Beijing to test Taiwanese resistance without provoking escalation. The thesis also expects to show that Taiwan's vulnerability is systemic and not isolated. The greatest risk is not simply that a port, a cable or an LNG terminal may be disrupted. The deeper risk is that several infrastructures could be pressured at the same time, both physically and cybernetically, creating disruption in logistics, energy, communications and decision-making, and reducing the endurance against the unification with China.

The main limitation is the length of the study. A thesis of 10,000 words cannot address the complexity of Taiwan's critical maritime infrastructure with the needed level of detail. The analysis is also limited by the difficulties of attribution in cyber operations and by the uncertainty involved in scenario modelling. Many available scenarios focus on a total blockade or an invasion, while this thesis pays more attention to gradual forms of coercion below the threshold of war.

2. Research Perimeter

2.1 Defining Critical Maritime Infrastructure

The European Union defines critical infrastructure as “an asset or system which is essential for the maintenance of vital societal functions”. Maritime infrastructure widely accepted as critical includes undersea cables for telecommunications and energy transmission. Critical maritime infrastructure also includes ports, navigation channels, marine terminals, offshore installations and related communication systems, and plays a vital role in global supply chains and international trade (Fridbertsson, 2023). The concept is broader than traditional naval security, because it includes civil and commercial assets, both in the physical and digital domains.

This definition is important because modern maritime infrastructure is not limited to the sea (Fridbertsson, 2023). It connects the sea, land and cyberspace. A container arriving at a port depends on maritime routes, cranes, navigation software, communications and digital tracking systems. LNG imports depend on ships, terminals and storage tanks (Jestrab & Hadley, 2023). Submarine cables depend on landing stations, telecommunications operators, repair vessels and backup systems. Critical maritime infrastructure is therefore an interdependent system. This interdependence creates vulnerabilities in crisis contexts. When systems are connected, a disruption in one area can quickly spread to others. A cyberattack against a port platform can delay the unloading of goods. A delay in LNG deliveries can affect electricity generation (West & Insisa, 2024). A cable cut can reduce communication capacity and make crisis coordination more difficult. These cascading effects are the central argument of this thesis.

In the case of Taiwan, this thesis defines critical maritime infrastructure as four main components. First, ports, especially those that handle container traffic, energy imports and industrial exports. Second, energy terminals, including LNG, oil and coal facilities. Third, submarine cables and their landing stations, which are the most vulnerable part of this infrastructure (Asia-Pacific Economic Cooperation, 2012). Finally, maritime digital systems, including AIS, port management software and logistics databases. This thesis does not treat these elements as separate. It analyses them as a single strategic system. This approach is necessary because Chinese actions are likely to exploit this interdependence, which creates the greatest challenges for incident response and recovery.

2.2 Taiwan's Maritime Infrastructure System

Taiwan's maritime infrastructure system reflects its geography and the needs of an industrialised country that is also one of the main global suppliers of high technology. As an island economy with limited energy resources, Taiwan depends heavily on maritime imports. Its ports connect the island with global markets, while its energy terminals receive the fuel that supports electricity generation and industrial production. Its submarine cables sustain digital connectivity, which is critical for the normal functioning of industry and society in a modern country.

Taiwanese ports are important for external trade. Kaohsiung, Keelung, Taichung and Taipei Port are the main points of connection with the outside world. Kaohsiung is especially important due to its role in container traffic and in the industrial ecosystem of southern Taiwan. Taichung and other ports are relevant for energy imports and industrial logistics (Jestrab & Hadley, 2023). Any disruption in these ports affects not only commercial activity, but also Taiwan's ability to maintain normal economic life during a crisis. Energy is one of the most sensitive areas. Taiwan imports most of its energy needs, including crude oil, coal and LNG. LNG is particularly important because of its limited storage capacity, around seven days of consumption. In addition, LNG power generation has a relevant weight in Taiwan's electricity mix. This creates a vulnerability: even if Taiwan has some fuel reserves, a prolonged disruption of maritime energy flows could put pressure on electricity supply and industrial production (U.S. Energy Information Administration, 2026).

The semiconductor sector makes this vulnerability even more important. TSMC and related companies depend on a stable and continuous electricity flow (Taiwan Semiconductor Manufacturing Company, 2025). A direct attack against TSMC (Reinsch & Whitney, 2025), or against any other semiconductor company, could trigger a strong international reaction (Byman et al., 2024). However, indirect pressure on energy terminals, transport systems or ports could also affect the sector, making coordinated action by Taiwan's allies more difficult. This is one of the reasons why critical maritime infrastructure is strategically relevant: it allows coercion to be applied against the pillars that support Taiwan's economy without directly attacking its most visible assets.

Submarine cables are another key vulnerability. Taiwan's main island and its outer islands depend on submarine cables for communications. The damage to cables affecting the Matsu Islands in 2023 (Insisa, 2026) showed that even limited disruptions can have

significant social and political effects. Cable repair requires specialised vessels, of which there are very few; and some of them are Chinese-owned. Repairs also require favourable weather conditions and an uncertain amount of time, depending on factors such as how easy it is to locate the fault, the type of damage to the infrastructure, or the number of points where the cable has been cut (Kim, 2025). During a crisis, access for repairs could be delayed by maritime pressure or security risks. Taiwan's critical maritime infrastructure system is therefore exposed in three ways. It is geographically exposed because many assets are located near disputed waters. It is functionally exposed because energy, trade and communications depend on maritime access. And it is digitally exposed because physical operations increasingly depend on data and connected systems.

2.3 China's Potential Strategic Toolkit

China has a wide set of tools available if it wished to put pressure on Taiwan without going into open military operations. These tools, many of which could already being tested to assess their impact and the reactions they generate, include military exercises, Coast Guard activity, maritime militia operations, air and naval incursions into Taiwan's airspace and maritime areas, threats of economic and trade restrictions against the island, disinformation campaigns and cyber operations (U.S. Department of Defense, 2026). This set of tools would give China a wide variety of options, depending on the geopolitical context, to apply different levels of pressure on the authorities of the Republic of China.

Grey-zone tactics are key in this scenario. They would allow China to gradually change facts on the ground or at sea, making it very difficult to justify a response by Taiwan or any of its allies, especially the United States. This Chinese activity may include maritime and air patrols, military manoeuvres simulating a blockade of the island, the presence of fishing vessels, maritime surveys and the use of civilian actors, as well as damage to submarine cables. These actions could be presented as accidental, legal or innocent, even if they serve strategic objectives (Byman et al., 2024). The Chinese Coast Guard and maritime militia are especially important. The Coast Guard, with its dual status as both a law-enforcement and military body, can operate in the space between policing and military coercion. It can board vessels, conduct patrols, challenge Taiwanese authority and normalise the Chinese presence in disputed waters. The maritime militia is especially important because it adds another layer of ambiguity by using vessels that appear civilian

but can support state objectives, while the Chinese government can argue that it does not have control over their actions (Macias III & Jensen, 2025).

Chinese cyber capabilities add a second dimension, which, as already mentioned, is especially difficult to trace. Cyber operations can target government agencies, companies, infrastructure operators, communication systems and data platforms (Lee, 2026). In the maritime domain, this could include port management systems, transport databases, AIS data manipulation, customs systems or energy control networks. Cyber operations are especially attractive because they can be combined with physical pressure. For example, during a crisis, cyber disruption could create delays in ports while Coast Guard pressure increases at sea.

Economic and logistical pressure is also important. China could try to influence shipping companies, insurers, energy suppliers or regional port operators. It could increase the perceived risk of operating in Taiwanese ports, raise insurance costs or create uncertainty about future access to the Chinese market. This type of pressure may be less spectacular than a blockade, but it can have an even bigger impact on commercial decision-making (Jestrab & Hadley, 2023). China's potential toolkit is therefore flexible and scalable. It allows Beijing to gradually increase pressure, observe Taiwan's response and stop before crossing a threshold that could justify direct intervention by external powers.

2.4 Analytical Framework

The analytical framework of this thesis evaluates the vulnerabilities of Taiwan's critical maritime infrastructure through three variables: exposure, criticality and recoverability. Exposure refers to the degree to which an infrastructure can realistically become the target of disruption. An infrastructure may be exposed because of geographical proximity, maritime harassment, cyber intrusion, supply-chain pressure or physical attack. Ports and cables are highly exposed because they are in open or semi-open maritime spaces. Digital systems are exposed because they depend on connected platforms and external software.

Criticality refers to the importance of an infrastructure for Taiwan's viability, both political and economic. An asset is highly critical if its disruption produces serious short-term consequences. LNG terminals, major ports and submarine cables have high criticality because they support energy supply, trade and communications. Criticality also

depends on the chance to find an alternative to the damaged asset. If an asset can be easily replaced, its criticality is lower. If there are few alternatives, its criticality is higher.

Recoverability refers to the capacity to restore an infrastructure after a disruption. Some disruptions are serious but can be recovered quickly. Others require specialised repair capabilities, specific components that are difficult to obtain, or support from other countries. Submarine cables are a good example of low recoverability, because repairs depend on specialised vessels and safe access to the point where the cable has been damaged.

Using these three variables, the thesis classifies vulnerabilities into three categories. The first includes assets with high exposure, high criticality and low recoverability. These are the most serious vulnerabilities. The second includes critical assets that are more recoverable, such as some port operations. The third includes assets of lower criticality that may still have political or psychological value if disrupted. This model helps avoid a merely descriptive analysis. Instead of simply listing threats, it allows different forms of coercion to be compared. A cyberattack against a port system can be very effective if it affects a critical function and is difficult to attribute. A cable incident may have a limited physical scale, but it can have important political value because it creates uncertainty about digital resilience, which is vital economically and militarily.

3. Chinese Strategic Approaches to Taiwan's CMI Disruption

The aim of analysing Taiwan's critical maritime infrastructure is not to examine a direct military conflict, or even a complete blockade of the island by Chinese naval and air forces. In such a scenario, these infrastructures would not necessarily be the key to understanding how events develop. The aim of this thesis is to analyse the different instruments that China could use to put pressure on Taiwan without giving Taiwan or its allies a clear justification to cross the threshold of armed intervention. This appears to be one of the most relevant features of China's pressure strategy potential capacity towards Taiwan: the gradual, ambiguous and cumulative use of different mechanisms of pressure.

From this perspective, critical maritime infrastructure, whether ports, logistics routes, energy terminals or submarine cables, should not be understood as military targets. Its most important role is as a point of social, political and economic pressure. China could

try to alter its functioning, create uncertainty, increase costs, change commercial behaviour or weaken the confidence of Taiwanese society in its own capacity to resist. This section analyses different strategic approaches that China could use to affect Taiwan's critical maritime infrastructure without directly resorting to military aggression. The objective is to show that there is a wide intermediate space between peace and war, and that in this space critical maritime infrastructure is especially useful for the aggressor and vulnerable for the target.

3.1 Grey-Zone Operations

Grey-zone operations are one of the most relevant tools in Chinese pressure against Taiwan. These are actions below the threshold of open war, but they seek to modify the strategic balance gradually (Germond, 2026). Instead of producing an immediate and visible impact, these operations erode their targets over time. Their logic is not to destroy the adversary directly, but to wear it down, force it to react and gradually reduce its room for manoeuvre. In Taiwan's case, the grey zone potentially would allow China to apply pressure without making an international response clearly justifiable. This is an important advantage. An invasion or total blockade of the island would generate an immediate global reaction, probably including sanctions, a military response from Taiwan's allies and a very high political cost for Beijing (Jestrab & Hadley, 2023). By contrast, actions that can be interpreted in different ways are harder to respond to. It is not always clear whether they are aggression, provocation, an administrative measure or simply a show of force. This ambiguity would be precisely one of China's most useful tools. When an action can be interpreted in several ways, the adversary's response becomes more complicated. Taiwan may perceive a clear threat, but its international partners may be more cautious if there is no obvious aggression. This gives Beijing room for manoeuvre, allowing it to increase pressure without assuming all the costs of open military escalation (Byman et al., 2024).

Applied to critical maritime infrastructure, this type of operation can have significant effects. For example, the repeated presence of Chinese vessels near key maritime routes can increase the perception of risk among shipping companies, insurers and logistics operators. This can make insurance more expensive, delay routes or lead some companies to stop operating in these waters and seek lower-risk destinations. In this way, China potentially does not need to block Taiwanese ports to affect their functioning. It may be

enough to create doubts about the security and stability of the maritime environment. In addition, grey-zone operations have a psychological component that is probably even more relevant in this context. Constant pressure can create a sense of vulnerability in Taiwanese society and send the message that China can disrupt daily life on the island at any time. This pressure can be especially useful if it affects sensitive sectors such as energy, communications or external trade. In this sense, the grey zone does not only seek military effects, but also political, economic and social ones.

From the point of view of the variables used in this thesis, grey-zone operations mainly increase the exposure of Taiwan's critical maritime infrastructure. This type of pressure makes maritime routes, port accesses and areas close to sensitive infrastructure more vulnerable, even if they formally continue operating (Helmus, 2024). In terms of criticality, these operations affect infrastructure that supports the island's basic functions: external trade, energy supply, digital connectivity and industrial activity. Criticality comes from the consequences that disruption would have. For this reason, even limited pressure on maritime routes or port accesses can have very relevant effects (Bueger & Liebetrau, 2023). Finally, recoverability in this case is complex because grey-zone operations do not usually cause physical damage that can be repaired quickly. The problem is not rebuilding destroyed infrastructure, but restoring normality, commercial confidence and logistical stability, which can take time.

3.2 Maritime Militia and Coast Guard Activities

The Chinese maritime militia and Coast Guard are especially useful instruments of pressure in this grey area between civilian activity, coercion and military pressure (Byman et al., 2024). Unlike the People's Liberation Army Navy, these forces potentially give China greater flexibility. Their presence can appear as surveillance, law enforcement, fishery protection or administrative control, although in practice it may have a clearly threatening purpose. The continued presence of these vessels in areas close to the island forces Taiwan to mobilise surveillance resources and systems. Although each isolated incident may seem limited, the cumulative effect can be considerable. Taiwan would be forced to respond constantly, with the risk of making mistakes or reacting in a way that China could quickly use to justify escalation or simply suffering long-term operational attrition (West & Insisa, 2024). China could deploy many civilian vessels, fishing boats, Coast Guard ships or support vessels in areas close to maritime routes, ports or outer

islands. This massive presence would make it difficult to distinguish between normal civilian activity and a coordinated operation. It would also force Taiwan to decide how far it should respond.

This dynamic allows a gradual erosion of Taiwanese maritime control. The key is not necessarily to take a port or block a route, but to normalise the Chinese presence in areas where it was not previously so common (U.S. Department of Defense, 2026). Over time, this normalisation will have consequences for control of those waters. If Chinese vessels appear constantly near certain areas, Taiwanese maritime activity, as well as shipping companies, insurers and logistics firms operating in the region, will include that presence in their decisions.

The Chinese Coast Guard also has a particular advantage: it can operate under the appearance of legality. Beijing can justify its actions as maritime control, inspection, resource protection or defence of its territorial claims. This makes an international response more difficult because the action may be perceived as policing. However, from Taiwan's point of view, the effect can be highly effective (Jestrab & Hadley, 2023). In this sense, the maritime militia and Coast Guard are key tools for pressuring critical maritime infrastructure without attacking it directly. They can create insecurity around supply routes, make commercial shipping more difficult, increase operating costs and force Taiwan to devote resources to monitoring its maritime environment. The result is a potentially effective form of pressure that may reduce Taiwan's room for manoeuvre.

Regarding the analytical variables, these tools increase exposure because they allow a constant and ambiguous presence near sensitive maritime spaces. This increases the vulnerability of maritime routes, outer islands, port accesses and areas close to cables or offshore energy infrastructure. In terms of criticality, the problem is not only that these vessels may interfere with a specific route, but that they can also gradually erode Taiwan's ability to control its own maritime environment (Macias III & Jensen, 2025). Finally, recoverability would be uneven. If pressure is limited to isolated incidents, Taiwan could return to normality relatively quickly. But if the presence of the Coast Guard and maritime militia becomes a sustained practice, recovery would be more difficult, because it would mean reversing a new "normality" imposed by China. In other words, it would not only be a matter of repairing damage, but of recovering control, confidence and operational freedom.

3.3 Economic and Logistic Pressure

Economic and logistical pressure is another key mechanism for affecting Taiwan's critical maritime infrastructure. Unlike a military attack, this type of pressure acts indirectly, through companies, trade routes, insurance, suppliers and logistics and port networks. Its relevance comes from the fact that maritime infrastructure does not function in isolation. China potentially can exploit this interdependence without acting directly against Taiwan. For example, it could pressure shipping companies, shipowners or insurance companies to reconsider their operations towards Taiwanese ports during a crisis. It could also create legal or commercial uncertainty, raising the cost of operating in the area. Even an informal threat or administrative warning may be enough to change the behaviour of some companies, especially if they believe that operating with Taiwan could affect their interests in the Chinese market. There are many examples of the Chinese government using these practices to achieve its objectives. One example is the lack of international recognition of Taiwan and the pressure faced by countries that strengthen their relations with the island. A clear case was the opening of Taiwan's commercial office in Lithuania at the end of 2021, using the term "Taiwan" in its name, which led to strong Chinese pressure on Lithuania and on other countries with commercial relations with Lithuania (Andrijauskas, 2022). This point is important because many critical infrastructures depend on actors that make decisions based on risk and cost. A shipping company does not need a formal blockade to reduce its activity if it considers the risk too high. An insurer may raise premiums or limit coverage if it perceives an unstable environment. A supplier of critical components may delay deliveries if it fears sanctions, retaliation or regulatory problems. In this way, Chinese pressure can be transmitted to Taiwan through third parties (Jestrab & Hadley, 2023).

In addition, China has great influence over regional logistics networks and many economic actors operating in the Indo-Pacific that could be used following its goals. This influence can be used to isolate Taiwan, not through a formal ban, but through more subtle mechanisms: delays, inspections, regulatory changes, commercial pressure or warnings to companies. The result could be a progressive degradation of Taiwan's maritime connectivity (U.S. Department of Defense, 2026). This type of coercion is especially threatening around energy supplies. More than 95% of Taiwan's energy is imported by sea. Even if China potentially does not physically interrupt all maritime flows, it could

create conditions that make their continuity more difficult. An increase in risk along maritime routes near Taiwan can affect vessel availability, transport costs or the will of insurers to cover certain routes. In a prolonged scenario, this could put pressure on Taiwan's energy system even without a total blockade (Byman et al., 2024). Logistical pressure would also affect the industrial sector. Taiwan, and especially its semiconductor sector, needs reliable supply chains. Production depends on stable electricity, water, chemicals, specialised machinery, spare parts and international transport (Byman et al., 2024). A disruption of maritime schedules or route availability can create cascading effects.

In short, economic and logistical pressure potentially offers China a less visible but very effective path of coercion. It does not need to close all ports or cut all routes. It can try to make operating with Taiwan more expensive, slower, more uncertain and politically more sensitive. This gradual degradation can have significant effects on the island's will to resist.

Regarding the analytical elements, economic and logistical pressure affects exposure in a less visible but very important way. It affects a wide range of elements on which Taiwan depends heavily. China could increase Taiwan's exposure by pressuring these third parties and making operations with the island more problematic. The criticality of this dimension is high because it directly affects the flows that allow Taiwan's economy to function. A port may remain open, but if insurers raise premiums, if some vessels avoid the area or if suppliers delay deliveries, the result can be a real degradation of maritime connectivity. In this sense, critical maritime infrastructure should not be understood only as physical assets, but also as networks connecting geographical and operational elements. Critical maritime infrastructure includes transport, energy and data systems, which fits this broader view of logistical dependence (Bueger & Liebetrau, 2023). Recoverability would depend on the level of pressure applied. If it affects one supplier or one specific route, recovery may consist of replacing routes, finding new suppliers or activating reserves. But if the pressure extends to vessel availability, energy supply or supply chains, recovery would be much slower. In that case, Taiwan would not only need to solve a logistical problem but also rebuild the confidence of international actors.

3.4 Comparative Effectiveness of Each Step

The effectiveness of the different pressure models that China could use against Taiwan's critical maritime infrastructure depends on three main factors: the degree of exposure they create, the criticality of the functions affected and the difficulty of recovery after disruption. From this perspective, grey-zone operations, maritime militia and Coast Guard activities, and economic and logistical pressure do not have the same impact or work in the same way, although they can reinforce each other (Germond, 2026). Grey-zone operations would be probably the most useful environment for China in terms of exposure. Their main advantage is that they increase Taiwan's vulnerability without directly attacking its critical infrastructure. The sustained presence of vessels, military exercises or unclear activities near maritime routes and ports can alter the perception of security among shipping companies, insurers and logistics operators. In this case, the infrastructure may continue to function physically, but its operating environment becomes more uncertain. Its criticality is high because it affects basic systems for the island, such as external trade, energy and communications. However, its most important effect lies in recoverability: because there is no clear physical damage, repairing the installation is not enough. The difficult part is to recover confidence, logistical normality and the perception of stability. For this reason, the grey zone is especially effective as a mechanism of long-term pressure (Jestrab & Hadley, 2023).

The activities of the maritime militia and the Coast Guard are more direct and visible, although they still maintain a high level of ambiguity. Their effectiveness is based on constant presence and the ability to saturate Taiwan's maritime environment. Compared with the grey zone in a broader sense, this environment creates a more physical exposure: routes, outer islands, ports and areas close to cables or energy infrastructure may be subject to surveillance or interference. Its criticality does not only come from possible damage to a specific infrastructure, but also from the gradual erosion of Taiwanese maritime control. If China could manage to normalise its presence in certain areas, Taiwan may still maintain ports and routes, but with less real freedom to operate. Recoverability would depend on the duration of the pressure. Isolated incidents would be manageable; a sustained presence would be much harder to reverse, because Taiwan would need not only to restore operations, but also to recover control and authority over its maritime space (Macias III & Jensen, 2025).

Economic and logistical pressure is perhaps the least visible environment, but it may be the most strategic. Its strength does not lie in immediate physical exposure, but in Taiwan's dependence on external actors: shipping companies, insurers, energy suppliers, port operators and industrial groups (U.S. Energy Information Administration, 2026). China could increase Taiwan's exposure by pressuring third parties, without acting directly against the island. Its criticality is very high because it affects the core of Taiwan's economy: energy, industrial components, maritime transport and supply chains. It can also affect the semiconductor sector, which depends on stable electricity, materials, machinery and international logistics. In terms of recoverability, this environment is especially dangerous if the pressure spreads. Changing a supplier or route may be possible; rebuilding the confidence of insurers, shipping companies and industrial partners would be much slower.

Overall, the grey zone is effective in creating uncertainty; the militia and Coast Guard are effective in eroding maritime control; and economic pressure is effective in weakening Taiwan's connectivity. The combination of all three would be more dangerous than any of them separately. It would not necessarily destroy critical maritime infrastructure, but it could make it less secure, more expensive, less reliable and harder to recover.

4. Chinese Cyber Threats to Taiwan's CMI

4.1 Digitalization of Maritime Infrastructure

Maritime infrastructure has become increasingly digitalised. Ports use automated systems to manage containers, cranes, customs, security access, schedules and cargo tracking. Shipping companies depend on digital platforms to coordinate routes, documents, payments and logistics. Energy terminals use industrial control systems to supervise storage, safety, regasification and distribution. Communication networks connect all these operations. This digitalisation improves efficiency, but it also creates vulnerability. A port can be compromised without physical damage if its digital systems are affected. Cargo can be delayed if databases are corrupted. Ships can receive wrong information if navigation data or schedules are manipulated. Energy terminals may be forced to slow down operations if their control systems are affected (Macias III & Jensen, 2025).

The key issue is that cyberattacks can have physical consequences. A cyberattack can close a terminal, delay unloading or even force the use of manual procedures when the technological platforms that govern the systems are not available. In a crisis, even temporary delays can have strategic effects. They can create uncertainty, increase costs and weaken public confidence (Su, 2026). Taiwan's critical maritime infrastructure is therefore exposed to cyber risk, as its economic model depends on speed, reliability and integration. A highly efficient logistics system can be fragile if it lacks redundancy. The more Taiwan depends on online information exchanges, digital coordination and external providers, the more valuable cyber disruption potentially becomes for China (Vogt et al., 2025).

4.2 China's Cyber Strategy and Capabilities

The cyber component plays a fundamental role in Chinese pressure against Taiwan. It should not be understood only as a technical threat or as a series of isolated attacks against computer networks. It forms part of a broader strategy of intelligence and operational preparation (Butler, 2024). China could use cyberspace to obtain information, test vulnerabilities, create uncertainty, disrupt essential services and complement other forms of pressure, such as grey-zone operations, economic coercion or maritime pressure exercised by the Coast Guard or maritime militia. In a scenario of tension with Taiwan, cyberattacks would allow Beijing to affect critical infrastructure without resorting to military action, which fits with a gradual pressure strategy, made even more effective by the difficulty of attribution.

China's strategy could combine two objectives. The first is cyberespionage, aimed at obtaining political, military, technological and industrial information. This objective is especially relevant in Taiwan's case because of the importance of its public institutions, defence systems, telecommunications and semiconductor industry. The second objective is disruption capacity, that is, the possibility of affecting critical services in the event of a crisis. China could carry out attacks against civilian critical infrastructure, although it would have to calculate the risk of causing a larger escalation, especially if the attacks also affected the United States or its regional allies (Lewis, 2023).

In terms of exposure, the cyber threat significantly expands Taiwan's vulnerable surface. Critical maritime infrastructure does not depend only on docks, cranes, ships or energy

terminals, but also on digital port management systems, communications, billing, access control, logistics planning, navigation, electricity networks and technology providers. This means that China would not need to launch a missile attack against a port or LNG terminal to cause significant effects. It could try to compromise the IT systems of logistics operators, energy companies or suppliers linked to these infrastructures. According to reports by Taiwan's National Security Bureau, Chinese actors exploit vulnerabilities in equipment used in critical infrastructure, use denial-of-service attacks, social engineering and supply-chain attacks (Taiwan National Security Bureau, 2026).

The criticality of this threat is high because many essential functions depend on digital systems. A cyberattack against maritime infrastructure would not need to physically destroy any asset to cause serious effects. It would be enough to delay port operations, alter logistics data, affect communications, interrupt external services or create doubts about the reliability of the systems. In a crisis context, even a temporary service disruption could have a significant impact, since it would affect sensitive sectors such as energy, transport, telecommunications or semiconductors. According to Reuters, citing the National Security Bureau, Chinese cyberattacks against Taiwanese critical infrastructure reached a daily average of 2.63 million in 2025 and affected sectors such as healthcare, energy, emergency services, telecommunications and companies related to the semiconductor industry (Lee, 2026).

From the perspective of recoverability, cyberattacks create a specific problem. Sometimes they can be reversed quickly if there are backups, continuity plans and prepared teams. However, their effect can last longer if they affect interdependent systems or damage trust in data integrity. In a port, for example, it is not enough for cranes to work physically if cargo systems or coordination systems with shipping companies are not reliable. For this reason, recoverability does not depend only on repairing servers, but also on restoring operational trust. The Taiwan Digital Blockade Wargame by the U.S. Naval War College highlights precisely the need to strengthen the resilience of Taiwanese infrastructure in the event of conflict with the People's Republic of China (Vogt et al., 2025).

Overall, the Chinese cyber threat is especially effective because it combines low visibility, a strong ability to deny responsibility and possible systemic impact. In terms of exposure, it multiplies the vulnerable points of critical maritime infrastructure. In terms of criticality, it can affect essential functions without destroying physical assets. And in terms of recoverability, it can create damage that is difficult to measure, because the main problem

may not be technical repair, but the recovery of trust, operational continuity and stability during a crisis (U.S. Cyber Command, 2024).

4.3 Cyber Disruption Scenarios

A cyber offensive against Taiwan's critical maritime infrastructure would not necessarily be limited to a single attack. It is more likely to work as an accumulation of partial interference at different points of the system: ports, energy terminals, submarine cables, navigation systems, logistics platforms and data networks. Its value would lie in this ability to create interference in the normal development of activities. The target would not be to completely paralyse the island, but to alter the speed, reliability and confidence in the systems that allow Taiwan to continue functioning and remain connected with the outside world (Cannon et al., 2026). In the case of ports, a cyberattack would mainly affect operational coordination. A modern port does not function only with docks, cranes and warehouses, but also with complex software, databases and container tracking platforms. China could try to attack these systems to create delays, terminal congestion or problems in planning entries and departures. In fact, Taiwan is investing significantly in systems to protect this infrastructure against cyberattacks (Reuters, 2024). From the point of view of exposure, ports are vulnerable because they connect many actors: the port authority, transport companies, customs, shipping companies and customers. The more different elements are connected, the more entry points there are. Their criticality is high because a port disruption affects external trade, the supply of goods to Taiwan's population and the export industry. Their recoverability would be medium: some operations could be moved to other ports or handled manually, but the loss of confidence could increase recovery times (Su, 2026).

Energy terminals, especially those linked to LNG, follow a different logic. Here, the main problem would not be logistical delay, but operational safety. An energy terminal depends on control systems, safety procedures, unloading schedules and coordination with specialised vessels. A cyberattack could force operations to stop as a precaution, even if there was no physical damage. In terms of exposure, these facilities are attractive because they combine industrial technology, external suppliers and links with maritime logistics networks. Their criticality is very high because Taiwan depends on energy imports to maintain electricity generation and industrial activity. In addition, LNG is more difficult to store for long periods than other fuels. Their recoverability would be lower than that

of ports, because it is not always possible to quickly replace a terminal, a control system or an energy supply chain (Center for Strategic and International Studies, 2025).

Submarine cables have an even more sensitive logic. Although they are often seen as physical infrastructure that can be cut, they also depend on landing stations, telecommunications operators, management networks and traffic rerouting systems. A cyberattack might not cut the cable, but it could degrade connectivity, saturate systems or make it harder to manage repairs after a physical incident. Their exposure is high because they combine a maritime section that is difficult to protect with digitally connected land infrastructure. Their criticality is also very high, because they support civilian communications, financial activity, government coordination and, in a crisis, strategic communication. Their recoverability is low if the cyberattack is combined with physical damage or maritime pressure, because repair depends on scarce specialised vessels that need access to the repair area and time to reach the damaged point (Huang, 2025).

Finally, maritime digital systems — AIS, port management software, logistics databases, customs systems and route planning platforms — are probably the most flexible target for a Chinese cyberattack campaign. Manipulating AIS information or introducing errors into databases could create confusion without destroying anything. Their exposure is very high because they depend on software, connectivity and external providers. Their criticality varies depending on the system, but it can increase quickly if the disruption affects operational decisions. Their recoverability depends on data integrity (Macías III & Jensen, 2025).

Overall, a digital offensive would be effective because it could multiply the effects of other types of pressure on Taiwan (Lewis, 2023). A port delay, doubts about the safety of an energy terminal, a partial loss of connectivity or an alteration of logistics data may seem like isolated technical incidents. However, if they happen at the same time as military exercises, Coast Guard or maritime militia pressure, or economic warnings, they can become a much more powerful tool of coercion. From this perspective, the main risk for Taiwan is not that China can attack one or several infrastructures, but that it manages to weaken confidence in the system.

4.4 Comparative Effectiveness: Cyber vs Physical Disruption

When comparing the components of an attack against Taiwan's critical maritime infrastructure, the main difference lies in the type of pressure generated. The physical component is more visible, more direct and easier to attribute. A cut submarine cable, a damaged LNG terminal, a blocked port or a restriction on commercial shipping has an immediate impact and can quickly be interpreted as a hostile action. This visibility increases its value as a signal of China's determination to achieve its objectives, but it also immediately alerts Taiwan and increases the risk of justifying a clearer response by Taiwan's allies. By contrast, a cyberattack offers a more flexible path of action (Insisa, 2026). It can delay operations, alter data, affect control systems or create confusion without responsibility being directly attributed to China. For this reason, it fits better with a logic of pressure below the threshold of open war (Lewis, 2023).

From the perspective of exposure, the cyber component potentially offers China a wider range of attack options. A physical attack requires proximity to the target or the ability to act against a specific asset: a cable, a port, an energy terminal or a maritime route. Cyber action, by contrast, could allow China to act against digital systems, external suppliers, logistics platforms, databases, AIS systems or industrial control networks. This means that China could affect the functioning of infrastructure without physically touching the main asset (Su, 2026). A port may remain intact, but operate slowly if its cargo, documentation or coordination systems with shipping companies are compromised.

In terms of criticality, physical disruption is usually more serious when it affects elements that are difficult to replace, such as submarine cables or energy terminals. However, cyber disruption can achieve similar effects if it affects key functions. For example, altering the systems of an LNG terminal could force unloading operations to be suspended for safety reasons, even if the facility has not suffered physical damage. Similarly, manipulating port data could create congestion, delays or loss of confidence among logistics operators. In an advanced economy such as Taiwan, whose elements are closely interconnected, an apparently limited problem can generate cascading effects (Vogt et al., 2025).

Recoverability is the point where the comparison becomes most interesting. Physical disruption may require slow repairs, especially if it affects submarine cables or specialised terminals. But the damage is usually identifiable. In cyber disruption, recovery may be faster if redundant systems exist, but it can also be more confusing: it is not always clear which systems have been compromised, whether the data is reliable or whether the

attacker remains inside the network. Therefore, recovery is not only about restoring servers, but also about recovering confidence in the proper functioning of the system, which can be extremely difficult.

The most dangerous scenario would be the combination of both forms of disruption. China could, for example, cause a limited physical incident in a submarine cable while launching cyberattacks against communication systems or data traffic management platforms (Loik, 2024). It could also increase maritime pressure near a port while interfering with customs or logistics systems, making the problem look like a combination of technical failures, congestion and operational tension. In the energy sector, physical pressure on supply routes could be combined with attacks against control systems or LNG unloading planning systems.

This combination would multiply the effect of the attack. The physical component would create the initial shock; the cyber component would make coordination more difficult and slow down recovery. For Taiwan, the problem would not be repairing the infrastructure but understanding which parts of the system remain reliable. For this reason, the most effective option for China would be to combine both components to make Taiwanese maritime infrastructure less reliable and more difficult to recover in a crisis (Su, 2026).

5. Implications

5.1. Strategic Implications for Taiwan

The analysis carried out in this thesis shows that Taiwan's critical maritime infrastructure is not only a logistical asset, but also a central element of its national security. Ports, LNG terminals, submarine cables, maritime routes and digital systems support external trade, electricity generation, connectivity, the technology industry and the country's ability to function in a crisis. Therefore, any disruption to these infrastructures would have economic, political and social consequences.

The first strategic implication is that Taiwan has a structural vulnerability. Its economic model depends on constant maritime flows and reliable digital systems. This dependence is an important weakness, because an actor such as China could use it as an instrument of pressure. From the perspective of exposure, Taiwan is in a difficult position. Many of its main ports, energy terminals and industrial areas are located on the western coast, facing

the Chinese coastline. In addition, submarine cables and maritime routes cannot be fully protected because they cross open spaces and depend on private companies and foreign governments, which are not always aligned with Taiwan's interests, as well as weather conditions, repair vessels and safe access to the affected areas (Huang, 2025). From the perspective of criticality, the potential impact is high. Taiwan's maritime infrastructure performs essential functions: energy, trade, communications, industrial activity and social stability. A problem in the ports would not only affect goods transport, but also the supply of basic goods to the population and exports. A disruption in LNG terminals could put pressure on electricity generation (Macías III & Jensen, 2025). A cut in submarine cables could affect civilian, business and government communications, including military communications. Recoverability is equally important. China would not need to destroy these infrastructures to create strategic effects. It is enough to delay operations, create uncertainty or reduce confidence in the normal functioning of the system. Some disruptions could be solved relatively quickly, but others could take longer to recover from and create internal political pressure.

For this reason, Taiwan faces a persistent hybrid threat. The most likely scenario does not necessarily have to be an invasion or a total blockade, but an accumulation of incidents: the presence of Chinese vessels, pressure on shipping companies and insurers, cyberattacks against logistics systems, damage to cables or disinformation campaigns against the Taiwanese government, or aimed at influencing election results (Min-Chen Lee, 2024). Each element may seem limited, but their accumulation can wear down Taiwanese resistance.

5.2. Resilience and Deterrence

A central conclusion of this thesis is that Taiwan cannot respond only through traditional military deterrence. If pressure is applied through cyberattacks, the grey zone, economic coercion or logistical interference, Taiwan needs a strategy that allows it to continue functioning during a crisis, while reducing the effects of attacks as much as possible (Byman et al., 2024).

The priority is redundancy. A system with a single critical path is easier to pressure. Taiwan should reinforce alternative routes, distributed port capacity, backup communication systems and continuity plans. Redundancy reduces the strategic value of

an attack because it prevents a single incident from paralysing a critical function (Huang, 2025).

The second priority is diversification. Taiwan cannot eliminate its maritime dependence, but it can reduce dependence on specific suppliers or routes. This is especially important in the energy sector. LNG represents a clear vulnerability because of its storage limitations. Increasing storage capacity to levels closer to those of oil or gas, diversifying suppliers and improving emergency supply agreements do not eliminate the risk, but they give Taiwan more room for manoeuvre in a crisis (Center for Strategic and International Studies, 2025).

The third priority is strengthening cybersecurity. The digitalisation of ports, energy terminals, AIS systems, customs and logistics platforms increases efficiency, but it also expands attack options. For this reason, cybersecurity is a key element of maritime security. It is not enough to physically protect a port if its cargo, logistics or coordination systems with shipping companies can be compromised (Bueger & Liebetrau, 2023).

Resilience also has a political and social dimension. This requires clear communication, coordination between agencies and emergency plans that are understandable to the population, which should carry out regular drills to know what to do in an emergency (Byman et al., 2024). In a hybrid crisis, public perception can be as important as the real impact of the attack. In this sense, resilience also acts as deterrence. If China perceives that a limited disruption does not manage to paralyse essential services or create panic, its usefulness decreases. The key is not only to prevent attacks, but also to prevent them from producing the desired political effects.

5.3. Policy Recommendations

The first recommendation is to prioritise infrastructure that combines high exposure, high criticality and low recoverability, as reviewed in this thesis. Not all infrastructures can be protected in the same way, so it is necessary to identify the most vulnerable assets (Cannon et al., 2026). Taiwan can also use its own strategic position as a source of leverage. Its role in semiconductor production, its democratic legitimacy and its importance for Indo-Pacific maritime stability allow Taipei to frame the protection of CMI as an international issue rather than a purely domestic one. This gives Taiwan room

to build coalitions around cable repair, port resilience, cyber defence, energy security and maritime domain awareness

It is essential to reinforce the physical and digital protection of these infrastructures. This includes maritime surveillance, sensors, protection of cable landing stations and monitoring of suspicious activity. Crisis exercises that combine several threats at the same time would also be useful, for example, a cyberattack against port systems together with the presence of Chinese Coast Guard vessels near a relevant route.

The third recommendation is to increase energy storage capacity, especially LNG storage capacity (Byman et al., 2024). This measure is costly, but fundamental in a crisis. Greater storage capacity would allow Taiwan to absorb temporary disruptions, reduce the psychological impact of a Chinese threat and avoid rushed decisions.

Externally, Taiwan should strengthen international cooperation to protect critical maritime infrastructure. Many necessary capabilities do not depend only on Taiwan: cable repair vessels, insurers, shipping companies, technology providers and energy partners are international actors. For this reason, Taiwan needs agreements with partners for technical assistance, intelligence sharing, cable repair and supply continuity (Abbondanza & Grgić, 2025). It is also important for Taiwan's allies to understand resilience as part of deterrence. Supporting Taiwan means helping the island remain connected, supplied and operational under pressure. If China perceives that its actions would trigger a coordinated response, the coercive value of attacking infrastructure decreases.

5.4. Implications for Indo-Pacific Security

The implications of this analysis go beyond Taiwan. A significant disruption of its critical maritime infrastructure would affect the whole Indo-Pacific and the global economy. Taiwan is in a key region for maritime trade, competition between China and the United States, and global technology production (Reinsch & Whitney, 2025). However, China would also face important risks in any campaign against Taiwan's critical maritime infrastructure. Even a limited disruption could generate regional escalation if Japan, the United States or other partners interpreted the action as the beginning of a broader coercive campaign. The risks would be particularly high if the disruption affected

commercial shipping, submarine cables or energy flows used by foreign companies. In that case, the crisis would no longer be limited to Taiwan, because private firms, regional governments and external navies could become involved in protecting access, restoring connectivity or deterring further disruption.

The main implication is the risk of geopolitical escalation. If China pressures Taiwan's maritime infrastructure and its allies try to support the island, the crisis could worsen. A limited incident could force Taiwan's allies to decide whether to provide technical support, maritime escort, sanctions or cyber assistance (Jestrab & Hadley, 2023). Each of these responses could be interpreted by China as aggression. An additional risk, in China`s case would be economic and reputational. Taiwan is not an isolated economy, but a central part of global semiconductor, logistics and technology networks. A serious disruption would therefore not only affect Taiwan. It could also disturb regional supply chains in which Chinese companies, even indirectly, have an interest. In addition, a coercive move against Taiwan could make other countries more willing to reduce their dependence on China, support Taiwan more openly and justify stronger countermeasures. This is why the tools analysed in this thesis may be useful for Beijing as long as they remain ambiguous. Their value would fall sharply if they were widely interpreted as clear and deliberate aggression.

The second implication is the impact on global supply chains. Taiwan is fundamental for semiconductor production, but this production depends on much more than factories. It needs stable electricity, machinery, maritime logistics and digital connectivity (Reinsch & Whitney, 2025). Therefore, pressure on ports, energy or communications could indirectly affect entire global industries, which could in turn trigger international intervention and escalate the conflict.

The third implication is that maritime security in the Indo-Pacific is changing. It is not only about protecting maritime routes with warships, but also about protecting cables, ports, energy terminals, logistics data and digital systems. Taiwan shows how an advanced economy can be vulnerable precisely because of its high level of integration. This lesson is relevant for all countries that depend on critical maritime infrastructure (Abbondanza & Grgić, 2025), but Taiwan is not only a passive target of Chinese pressure. Even if its maritime infrastructure is vulnerable, Taiwan can still reduce some of these risks through better preparation, stronger cybersecurity, cooperation with partners, public communication and emergency planning.

5.5. Limitations of the Study

This thesis has several limitations. The first is the available space. Taiwan's critical maritime infrastructure covers a wide range of components. Each of them could be studied separately in much greater depth, and some have already been addressed in the literature review. This thesis adopts an integrated view, which makes it possible to observe relations between vulnerabilities, but significantly reduces the level of technical detail.

The second limitation is uncertainty about future scenarios. China's behaviour will depend on multiple political, military and economic decisions, Taiwan's internal social and political situation, the position of the United States in particular, and the reaction of other regional and global allies. For this reason, this thesis does not try to predict a specific operation, but to identify mechanisms of pressure.

The third limitation is attribution. In cyber and grey-zone operations, many actions may appear accidental, ambiguous or difficult to prove. Damage to a cable, a digital disruption or the presence of civilian vessels can be interpreted in different ways. For this reason, the analysis does not treat every incident as proof of aggression, but as part of an environment in which ambiguity may be essential for Beijing.

6. Conclusions

6.1. Summary of Key Findings

This thesis has analysed how China could use Taiwan's critical maritime infrastructure as a tool of strategic pressure. The main conclusion is that Taiwan's vulnerability does not lie in one specific port, LNG terminal or submarine cable, but in the interdependence of the system. Ports, energy terminals, maritime routes, submarine cables and digital platforms function as components of a broader structure. For this reason, a limited attack can generate cascading effects on energy, trade, communications, industrial production and social stability. The analysis confirms the usefulness of the framework based on exposure, criticality and recoverability. Taiwan is exposed because of its island geography, the concentration of much of its infrastructure on the western coast, and its dependence on open maritime routes. Its infrastructure is critical because it supports

essential functions for the economy and society. Recoverability is uneven: some disruptions can be solved quickly, but others, such as damage to submarine cables, problems in energy terminals or cyberattacks against logistics systems, may require more time, specialised resources and external coordination. Another important conclusion is the relevance of hybrid and cyber threats. China does not need to launch an invasion or impose a blockade to pressure Taiwan. It can use more ambiguous tools, such as grey-zone operations, Coast Guard activity, maritime militia, economic coercion, pressure on private companies, disinformation and cyberattacks. These measures are useful because they remain below the threshold of open war and make it difficult for Taiwan and its allies to respond clearly.

6.2. Answer to Research Question

The main research question was: to what extent, and through which mechanisms, can China alter Taiwan's stability through its critical maritime infrastructure? The answer is that China could significantly affect Taiwan's stability, not necessarily by militarily attacking infrastructure, but by disrupting its functioning. This may happen by increasing maritime pressure around routes, ports and outer islands. It may also happen using Coast Guard and maritime militia forces to normalise China's presence in sensitive areas. China may also pressure shipping companies, insurers, energy suppliers or logistics operators so that operating with Taiwan becomes more costly or risky. Finally, it may use cyberattacks against port systems, logistics platforms, communications or energy networks.

The impact will depend on the combination of these instruments. An isolated incident may be manageable. However, a coordinated campaign combining maritime pressure, cyber disruption, economic coercion and psychological operations could have a much deeper effect. In that scenario, the Chinese objective would not be to paralyse Taiwan immediately, but to weaken its infrastructure so that it becomes less reliable and more difficult to recover in a crisis.

6.3. Academic Contribution

The main academic contribution of this thesis is to study Taiwan's critical maritime infrastructure as an integrated system. Much of the literature analyses submarine cables,

ports, energy or cybersecurity separately. However, this case shows that these dimensions are connected. The thesis also contributes by integrating the physical and cyber dimensions. The separation between them makes less sense. A cyberattack can cause physical effects, such as port delays or interruptions in energy operations. Similarly, a physical incident can multiply its impact if it is accompanied by data manipulation or digital interference. Therefore, the study of critical maritime infrastructure must analyse both physical assets and the digital systems that make them function.

6.4. Policy Relevance

From a policy point of view, this thesis shows that Taiwan must strengthen its resilience far beyond the military field. Conventional deterrence against the risk of invasion or blockade is important, but it is not enough against a Chinese strategy based on hybrid pressure. Taiwan needs to reduce the exposure of its infrastructure, protect its most critical assets and improve its recovery capacity. This means investing in port redundancy, greater energy storage capacity, submarine cable protection, cybersecurity, civil protection plans and public-private coordination. It also requires international cooperation, since many of the necessary resources come from other countries.

Finally, the lessons from the Taiwanese case are also relevant for other countries. Many advanced economies depend on ports, cables, energy terminals and digital platforms. Therefore, the protection of critical maritime infrastructure is not only a technical problem, but also a central issue for national security and international stability.

6.5. Future Research

This thesis opens several lines of future research. The first would be to develop quantitative disruption models. It would be useful to estimate, for example, the impact of a partial interruption in ports, a reduction in LNG deliveries, a submarine cable cut or a cyberattack against logistics systems. This would make it possible to measure more precisely the economic, energy and social costs of each scenario and compare them to prioritise resilience measures according to available resources. A second line would be to compare Taiwan with other regions exposed to similar risks, such as the Baltic Sea. These cases would help identify common patterns and regional differences.

Finally, it would be important to study in greater depth the relationship between real resilience capacity and public perception. In a hybrid crisis, it is not enough for infrastructure to continue functioning. It also matters that the population, companies and allies believe that the system remains reliable. This political and psychological dimension will become increasingly relevant in the study of critical maritime infrastructure.

7. References

Abbondanza, G., & Grgić, G. (2025). *Europe's Indo-Pacific pivot: Navigating new horizons*. Palgrave Macmillan. https://doi.org/10.1007/978-981-95-0273-8

Andrijauskas, K. (2022). *The Sino-Lithuanian crisis: Going beyond the Taiwanese representative office issue*. *IFRI: Institut français des relations internationales*, 1-9.

Asia-Pacific Economic Cooperation. (2012). *Economic impact of submarine cable disruptions*.

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context. *European Journal of International Relations, 11*(2), 171–201.

Bueger, C., & Liebetrau, T. (2023). *Critical maritime infrastructure protection: What's the trouble? Marine Policy*, *155*, 105772. https://doi.org/10.1016/j.marpol.2023.105772

Butler, Z. (2024, June 26). *Google disrupted over 10,000 instances of DRAGONBRIDGE activity in Q1 2024*. Google Threat Analysis Group https://blog.google/threat-analysis-group/google-disrupted-dragonbridge-activity-q1-2024/

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Byman, D., Jones, S. G., & Blanchette, J. (2024). *Strengthening resilience in Taiwan* . Center for Strategic and International Studies.

Cannon, B. J., Matsuo, K., & Matsuda, M. (2026). *Mapping undersea cable risk from bathymetry to geopolitics: Evidence-based rankings and tailored resilience strategies. Marine Policy*, *186*, 107012. https://doi.org/10.1016/j.marpol.2025.107012

Center for Strategic and International Studies. (2025). *Lights out? Wargaming a Chinese blockade of Taiwan*.

Chen, T.-C. (2025). *Undercurrent: Limits and prospects of submarine cable security for Taiwan*. Research Institute for Democracy, Society and Emerging Technology.

Cheng, E. (2026, May 16). *Why Taiwan became the defining issue in the Trump-Xi talks*. *CNBC*. https://www.cnbc.com/2026/05/16/trumps-meeting-with-chinas-xi-steers-the-us-away-from-taiwan-again.html

Fridbertsson, N. T. (2023). *Protecting critical maritime infrastructure - The role of technology*. NATO Parliamentary Assembly, Science and Technology Committee. General Report.

Germond, B. (2026, February 12). *Critical undersea infrastructures: A framework to address threats in a post-physical context. Georgetown Journal of International Affairs*.

Helmus, T. (2024). *Understanding and countering China's maritime gray zone operations*. RAND Corporation. https://doi.org/10.7249/RRA2954-1

Hoffman, F. G. (2007). *Conflict in the 21st Century: The rise of hybrid wars.* Potomac Institute for Policy Studies.

Huang, D. K. (2025). *Strengthening Taiwan's sea cable security*. The Hague Centre for Strategic Studies.

Insisa, A. (2026). *What lies beneath: Hybrid threats to Taiwan's submarine cables and the contest in the information domain*. Istituto Affari Internazionali.

Jestrab, M., & Hadley, S. J. (2023). *A maritime blockade of Taiwan by the People's Republic of China: A strategy to defeat fear and coercion*. Atlantic Council.

Kim, S. K. (2025). *Understanding the security of submarine cables in the East Asian context: Status and the way forward. The Korean Journal of International and Comparative Law*, 1-31. https://doi.org/10.1163/22134484-12341236

Lee, Y. (2026, January 5). *Chinese cyberattacks on Taiwan infrastructure averaged 2.6 million a day in 2025, report says*. Reuters. https://www.reuters.com/world/china/chinese-cyberattacks-taiwan-infrastructure-averaged-26-million-day-2025-report-2026-01-05/

Lewis, J. A. (2023). *Cyberattack on civilian critical infrastructures in a Taiwan scenario*. Center for Strategic and International Studies. https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario

Loik, R. (2024). *Undersea hybrid threats in strategic competition: The emerging domain of NATO–EU defense cooperation*. https://doi.org/10.57767/JOBS_2024_008

Macias, J. M., III, & Jensen, B. (2025). *Signals in the swarm: The data behind China's maritime gray zone campaign near Taiwan*. Center for Strategic and International Studies. https://www.csis.org/analysis/signals-swarm-data-behind-chinas-maritime-gray-zone-campaign-near-taiwan

Min-Chen Lee, L. (2024, December 11). *Decoding China's digital offensive: An analysis of information warfare tactics in Taiwan's 2024 presidential election. Yale Journal of International Affairs*. https://www.yalejournal.org/publications/decoding-chinas-digital-offensive-an-analysis-of-information-warfare-tactics-in-taiwans-2024-presidential-election

People's Liberation Army Eastern Theater Command. (2024a, May 23). *PLA conducts joint military drills surrounding Taiwan Island*. Ministry of National Defense of the People's Republic of China. https://eng.mod.gov.cn/xb/News_213114/TopStories/16310652.html

People's Liberation Army Eastern Theater Command. (2024b, October 14). *Chinese PLA Eastern Theater Command conducts "Joint Sword-2024B" drills*. Ministry of National Defense of the People's Republic of China. https://eng.mod.gov.cn/xb/News_213114/TopStories/16345116.html

Potcovaru, S.-D., & Mustață, M.-A. (2026). *Critical infrastructure through a securitization theory lens*. *Bulletin of Carol I National Defence University*, *14(4)*, 193-206. https://doi.org/10.53477/2284-9378-25-65

Reinsch, W., & Whitney, J. (2025). *Silicon island: Assessing Taiwan's importance to U.S. economic growth and security*. Center for Strategic and International Studies.

Reuters. (2024, June 17). *Cisco to establish cybersecurity centre in Taiwan. Reuters*. https://www.reuters.com/technology/cybersecurity/cisco-establish-cybersecurity-centre-taiwan-2024-06-17/

State Council Information Office of the People's Republic of China. (2019, July 24). *China's national defense in the new era*. The State Council of the People's Republic of China. https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html

State Council of the People's Republic of China. (2021, August 17). *Regulation to strengthen protection over critical information infrastructure*. https://english.www.gov.cn/policies/latestreleases/202108/17/content_WS611b8062c6d0df57f98de907.html

Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations, 13*(3), 357–383.

Su, W. M. (2026). *Protecting critical maritime infrastructure: a multi-domain approach to maritime security governance*. *RSIS Commentaries, 033-26*.

Taiwan Affairs Office of the State Council, & State Council Information Office of the People's Republic of China. (2022, August 10). *The Taiwan question and China's reunification in the new era*. The State Council of the People's Republic of China. https://english.www.gov.cn/archive/whitepaper/202208/10/content_WS62f34f46c6d02e533532f0ac.html

Taiwan National Security Bureau. (2026). *China's cyber threats to Taiwan's critical infrastructure in 2025*. National Security Bureau

Taiwan Semiconductor Manufacturing Company. (2025). *TSMC 2024 sustainability report*. https://esg.tsmc.com/en-US/articles/367

U.S. Cyber Command. (2024, February 7). *PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure* (AA24-038A).

U.S. Department of Defense. (2026). *2025 annual report to Congress: Military and security developments involving the People's Republic of China*.

U.S. Energy Information Administration. (2026). *Taiwan analysis brief*.

Vogt, J., Kollars, N., & Poznansky, M. (2025). *Preparedness wargaming for critical infrastructure resilience: Taiwan digital blockade wargame*. *The Cyber Defense Review*, *10*(2), 181-198. https://doi.org/10.55682/cdr/qgz7-pqvc

West, M. J., & Insisa, A. (2024). *Reunifying Taiwan with China through cross-strait lawfare. The China Quarterly*, *257*, 186-201. https://doi.org/10.1017/S0305741023000735

ANNEX: Declaration of Use of Generative AI Tools

Academic Year: _2025-2026____
Master's Programme: Master in International Security Management (MISM)
Student Name: Luis Alberto Moreno Martin-Portugués_

I declare that generative artificial intelligence tools have been used as support tools in the preparation of this Master's Final Thesis.

x YES ☐ NO

1. Ethical and Academic Use

Have you included sensitive or personal data when using AI tools? If yes, specify:
____No_____
_____

Have you used AI tools to replace your own work without critically reviewing the generated content? If yes, specify:

__No_____
_____

Have you followed the academic recommendations and guidelines regarding the use of AI tools?

__Yes_____
_____

2. Technical Use of AI Tools

Please indicate the AI tools used (e.g., ChatGPT, Copilot, Claude, Gemini):

ChatGPT

Please mark the applicable uses:

- ☐ Text generation
- ☐ Reformulation / editing
- X Translation / proofreading
- ☐ Structure suggestions
- ☐ Methodological support
- X Bibliographic search or citation support
- ☐ Audiovisual content generation
- ☐ Other uses (please specify)

I confirm that the final content of this thesis has been fully reviewed, corrected, and validated by me as the author. The use of AI has not replaced my own critical analysis, personal reflection, or intellectual work.

Signature: Luis Alberto Moreno Martin-Portugués