THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

# MAPPING CYBERSECURITY REGULATORY LANDSCAPES

## UNITARY VS. DISPARATE SYSTEMS

**RESEARCH FELLOWS**
Marquis G. Bullock
Nuqu Xiong
Yucheng Xue
Xinyi (Yolanda) Yang

**SENIOR RESEARCH FELLOWS**
Yelyzaveta Ismatullayeva

**FACULTY LEAD**
Jessica L. Beyer

**GLOBAL RESEARCH GROUP**
AUGUST 2022

This report is a product of the Global Research Group Program in the Henry M. Jackson School of International Studies at the University of Washington. The Global Research Groups match teams of top-achieving Jackson School students with private and public-sector organizations seeking dynamic, impactful, and internationally-minded analyses to support their strategic and operational objectives.

For more information about the Global Research Groups please visit our website at http://jsis.uw.edu/grg/

# Mapping Cybersecurity Regulatory Landscapes: Unitary vs. Disparate Systems

Global Research Group, Jackson School of International Studies

August 2022

**Synopsis**
In order to understand cybersecurity regulatory systems, we conducted a survey of 29 countries to identify countries with unitary, transitional, or disparate cybersecurity regulatory frameworks. From these 29 countries, we identified five country cases for in depth exploration: Brazil, Chile, France, Lithuania, and Singapore. Three of these countries – France, Lithuania and Singapore – have unitary models of cybersecurity governance and two of the cases – Brazil and Chile – have disparate models with plans to transition to a unitary system. The report analyzes each system in a series of country-based case studies. These case studies outline cybersecurity governing agencies, regulatory frameworks, international and public/private relationships, and general system effectiveness. Effectiveness is measured as a connection between the system model and streamlined communication networks.

**Research Fellows**
Marquis G. Bullock
Nuqu Xiong
Yucheng Xue
Xinyi (Yolanda) Yang

**Senior Research Fellow**
Yelyzaveta Ismatullayeva

**Faculty Lead**
Jessica L. Beyer

Contact: Jessica L. Beyer, jlbeyer@uw.edu

## *Table of Contents*

***Executive Summary*** ..... ***1***

***Research Findings*** ..... ***2***

***Brazil*** ..... ***10***

***Chile*** ..... ***21***

***France*** ..... ***35***

***Lithuania*** ..... ***49***

***Singapore*** ..... ***62***

***Bibliography*** ..... ***74***

# Executive Summary

While most countries recognize the need for cybersecurity regulation, there are differences in the form of regulatory framework they choose. In order to tackle cybersecurity threats, some countries establish a singular agency that has jurisdiction over cybersecurity and has the final word on the country's cybersecurity. This singular agency has the authority to speak with one voice to the private sector, providing effective guidance and a clear point of contact. In contrast, other countries employ a disparate system in which authority and responsibility is spread between organizations and actors. This report assesses the two cybersecurity regulatory systems with a particular focus on their effectiveness from the perspective of the private sector.

In order to understand cybersecurity regulatory systems, we conducted a survey of 29 countries to identify countries with unitary, transitional, or disparate cybersecurity regulatory frameworks. From these 29 countries, we identified five country cases for in depth exploration: Brazil, Chile, France, Lithuania, and Singapore. Three of these countries – France, Lithuania and Singapore – have unitary models of cybersecurity governance and two of the cases – Brazil and Chile – have disparate models with plans to transition to a unitary system.

The report analyzes each system in a series of country-based case studies. These case studies outline cybersecurity governing agencies, regulatory frameworks, international and public/private relationships, and general system effectiveness. Effectiveness is measured as a connection between the system model and streamlined communication networks.

While the purpose of the research was to create in-depth case studies, when we compared the five country cases, we also found the following:

- Unitary systems are more effective for productive engagement between government and the private sector. In the three unitary cases of France, Lithuania, and Singapore, a unitary approach is effective because it creates a clear legal framework, non-overlapping jurisdiction with established enforcement mechanisms, and collaborative partnerships with both international and private actors.
- Disparate systems are less effective and case studies of the disparate cases of Brazil and Chile reveal these limitations. The convoluted sector-specific regulations produce structural gaps and sometimes overlap, rendering the cybersecurity regulatory frameworks inefficacious for the private sector.
- There is a positive correlation between reactive policies and risk-based regulations and sector-specific regulations in disparate systems.
- The two disparate cases in this study recognize the ineffectiveness of their system and are transitioning to unitary systems for more effectiveness. Lithuania presents a successful case of transitioning from a disparate system to a unitary system in 2015, enhancing its overall effectiveness on cybersecurity.
- Finally, this report finds no interdependency between system styles and the public sector's ability to participate in a country's legislation on cybersecurity. Our research also finds no relationship between system styles and information sharing. Private participation in legislation and information sharing largely depend on each country's domestic political landscape.

# Research Findings

In order to understand cybersecurity regulatory systems, we conducted a survey of 29 countries to identify countries with unitary, transitional, or disparate cybersecurity regulatory frameworks. From these 29 countries, we identified five country cases for in depth exploration: Brazil, Chile, France, Lithuania, and Singapore. Three of these countries – France, Lithuania and Singapore – have unitary models of cybersecurity governance and two of the cases – Brazil and Chile – have disparate models with plans to transition to a unitary system.

The report analyzes each system in a series of country-based case studies. These case studies outline cybersecurity governing agencies, regulatory frameworks, international and public/private relationships, and general system effectiveness. Effectiveness is measured as a connection between the system model and streamlined communication networks.

## Case Selection

In order to identify case studies, our team created a list of 29 possible country cases and then gathered information about each country's system. This data is attached to the report as a spreadsheet. The criteria for potential cases included looking for cases in every region of the world, identifying cases with sufficient economic resources for a robust cybersecurity policy environment, and looking for cases that presented varied styles of cybersecurity governance from unitary to disparate. Figure 1 illustrates a geographic map of our five country cases.

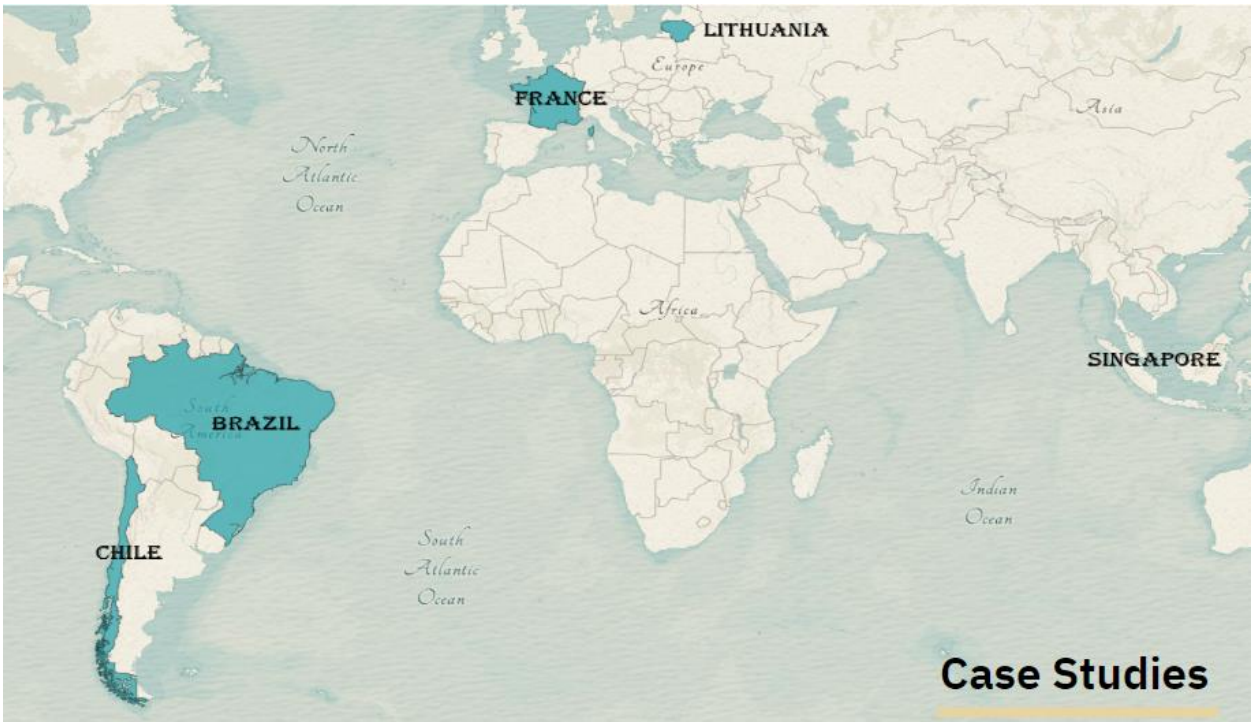


Figure 1: Map of Case Studies

Based on a review of government reports, official websites, legislative decrees, academic sources, feedback from Microsoft, and other materials, researchers selected five country cases. Of these five cases, France, Lithuania, and Singapore constitute examples of a unitary system, while Brazil and Chile are in the transition from a disparate system to a unitary system as illustrated in Figure 2.

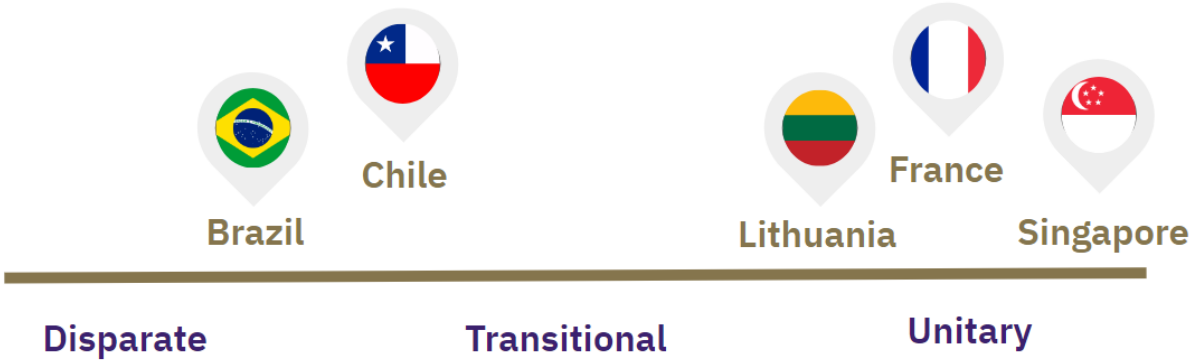


Figure 2: Distribution of System Styles

## Findings

While most countries recognize the need for cybersecurity regulation, there are differences in the forms of regulatory framework they choose. In order to tackle cybersecurity threats and regulate the cybersecurity system, some countries establish a singular agency that has jurisdiction over cyberspace and has the final word on the country's cybersecurity. This singular agency has the authority to speak with one voice to the private sector, providing effective guidance and clear points of contact. In contrast, other countries employ a disparate system in which authority and responsibility is spread between organizations and actors. Disparate systems may create overlapping and contradictory regulations.

In order to develop a comprehensive understanding of the cybersecurity governance of each country, we analyzed cybersecurity agencies, regulatory frameworks, enforcement mechanisms, international cooperation, and relationships with the private sector within each case to evaluate the effectiveness of the five countries' cybersecurity regulatory models. Table 1 illustrates the high-level findings from the report.

Table 1: Cross Case Comparison

| | **Brazil** | **Chile** | **France** | **Lithuania** | **Singapore** |
|---|---|---|---|---|---|
| **Overall system effectiveness** | Moderate | Moderate | Effective | Effective | Effective |
| **System style** | Transitional | Transitional | Unitary | Unitary | Unitary |
| **National strategy and framework** | Initial stage | Initial stage | Established | Established | Established |
| **NCSI index rating** | 46.75 | 59.41 | 84.42 | 93.81 | 71.43 |

As illustrated in Table 1, the report assesses each country's overall system effectiveness and ranks each case from *ineffective* to *moderately effective* to *effective*. The ranking is based on the following three categories: legal frameworks, regulation and enforcement, and relationships. The assessment of each category is based on a holistic assessment of data gathered in that category–with similar data having been gathered about each of the cases.

An overall system is considered *effective* if the cybersecurity framework in the country produces an engaging environment for the private sector to navigate and execute businesses in the cyber-related fields. In our cases, France, Lithuania and Singapore are effective. Under this rubric, a country with an effective system has the following characteristics:

- A clear legal framework;
- Non-overlapping jurisdiction with established enforcement mechanisms;
- Collaborative with both international and private actors.

In contrast, a country has a *moderately* effective system if it fits most of the criteria of an effective system but is lacking in certain aspects, such as having no lobbying pathways, that would impede private businesses' executions and future business progressions. Brazil and Chile are considered to be moderately effective under this rubric. Finally, an *ineffective* system lacks most of the above aspects.

This report categorizes a country's cybersecurity regulatory system from *disparate* to *transitional* to *unitary*. We consider a country that does not have a unitary regulatory agency to have a *disparate* system style. A country that currently has a disparate system and is in the process of creating a unitary agency, such as Brazil and Chile, has a *transitional* system style. And a country that has an established unitary agency, such as France, Lithuania and Singapore, has a *unitary* system.

Our national strategy and framework category considers whether the country has a national plan of actions for the overall environment and security. Country is considered to be at the *initial stage* if it has no national plan but aims at establishing one in the foreseeable future. For the two disparate cases, Brazil and Chile's national strategies are both in an initial stage. An *established* stage is a country that has a national plan in effect. The unitary cases France, Lithuania and Singapore have established national strategies. A *mature* stage is a country that has a fully functional plan that has yielded many successes.

In addition, the report uses the National Cyber Security Index (NCSI) produced by e-Governance Academy Foundation as a parameter to provide a basic sense of the preparedness of countries to prevent cyber threats and manage cyber incidents. Each country is given a NCSI

score out of 100. This report builds on NCSI's criteria and operates on the specific guidelines provided by Microsoft in assessing the effectiveness of cybersecurity of each case study. It is worth noting that a high NCSI score does not necessarily guarantee a high effectiveness in our cases.

## Comparing Unitary Cases

We determined that the overall system effectiveness of France, Lithuania, and Singapore are effective based on the criteria mentioned above. All three countries have a clear legal framework, non-overlapping jurisdiction with established enforcement mechanisms, and collaborative partnerships with both international and private actors. The three countries have unitary systems with singular cybersecurity authorities, and their national strategies and frameworks have all been established.

In all three countries, the cybersecurity regulatory framework is parsimonious, which means the structure is simple or not overly complex. Furthermore, in all three countries with a singular cybersecurity authority, the jurisdiction is clear. While there are overlaps and gaps in the authority and regulations in all three cases, they are not significant enough to make the system overly complicated. France and Singapore are also identified as technology neutral, which means their cybersecurity strategies and regulatory approaches can accommodate new and changing technologies; while Lithuania is considered to have risk-based regulations, which means that their cybersecurity rules are based on risks and are functional and practical across sectors. Other than that, all three countries are identified as outcome focused, which means their strategies and approaches can evolve with the changing threat landscape. Table 2 summarizes these findings.

Table 2: Legal Framework and Effectiveness of Unitary Cases

| | **France** | **Lithuania** | **Singapore** |
|---|---|---|---|
| Is the framework parsimonious? | Yes | Yes | Yes |
| Is jurisdiction clear? | Yes | Yes | Yes |
| Are there gaps in the framework? | Yes | Yes | Yes |
| Is regulation: outcome focused, technology neutral, risk-based? | Outcome focused, technology neutral | Outcome focused, risk-based | Outcome focused, technology neutral |

In France, Lithuania, and Singapore, cybersecurity regulation and enforcement are all somewhat sector specific. This means that there are regulations and enforcement mechanisms in critical sectors, but not in every sector. We consider a country to have an enforcement agency if there is a specific government entity responsible for the enforcement of cybersecurity regulations. In all three countries, France, Lithuania, and Singapore, there are enforcement agencies in place. Table 3 summarizes these findings.

Table 3: Regulation and Enforcement of Unitary Cases

| | **France** | **Lithuania** | **Singapore** |
|---|---|---|---|
| Are regulation/enforcement sector-specific? | Somewhat | Somewhat | Somewhat |
| Is there an enforcement agency? | Yes | Yes | Yes |

Finally, each country illustrates active and robust relationships between domestic and international partners. The relationships here include international coordination, public and private partnerships, and information sharing between national agencies. France, Lithuania, and Singapore all actively cooperate with international institutions. France and Lithuania partner the European Union (EU) and NATO, while Singapore cooperates with the Association of Southeast Asian Nations. In France and Singapore, there are clear pathways for the private sector to comment on the legislative process or to lobby the government. While in Lithuania, public-private relationships are still in development. Specifically, private businesses in Lithuania can submit comments on draft cybersecurity policies, but it is unclear whether these comments are taken into serious consideration by legislators. Finally, the country's information sharing is characterized as sufficient if there are specific and thorough requirements for information sharing between different government entities. In all three countries, we identify that there are sufficient information sharing mechanisms. Table 4 illustrates the findings related to relationships.

Table 4: Relationships Of Unitary Cases

| | **France** | **Lithuania** | **Singapore** |
|---|---|---|---|
| Are there international relationships? | Yes | Yes | Yes |
| Can the private sector weigh in? | Yes | Somewhat | Yes |
| What characterizes information sharing? | Sufficient | Sufficient | Sufficient |

## Comparing Disparate Cases

We identify the overall system effectiveness of Brazil and Chile as moderately effective based on our analysis of the cybersecurity agencies, regulatory frameworks, enforcement mechanisms, international cooperation, and relationships with the private sector. Both Brazil and Chile are in transition from disparate models to unitary models, and their national strategies and frameworks are both in an initial stage.

In the two disparate cases, Brazil and Chile both have risk-based regulations, which is consistent with their reactive policies on cybersecurity. The sector specific cybersecurity regulations in Brazil and Chile result in many structural gaps in their respective legal regulatory frameworks, and unclear jurisdictions in the case of Chile. Our research shows that the frameworks of two disparate cases are not parsimonious. These sectoral regulations are convoluted and discursive, making it inaccessible for the private businesses to gain a clear understanding of the regulatory frameworks and the enforcement mechanisms when conducting

businesses in the cyber-related fields. Both countries, however, recognize the gaps and overlaps within their frameworks and the impediments these inconsistencies present for private businesses. Hence, both countries are currently working toward more centralized systems with unitary agencies. Table 5 illustrates these findings.

Table 5: Legal Framework and Effectiveness of Disparate Cases

| | **Brazil** | **Chile** |
|---|---|---|
| Is the framework parsimonious? | No | No |
| Is jurisdiction clear? | Yes | In development |
| Are there gaps in the framework? | Yes | Yes |
| Is regulation: outcome focused, technology neutral, risk-based? | Risk-based | Risk-based, technology neutral |

One commonality between Brazil and Chile is their sector-specific regulations on cybersecurity. Both countries are reactive in forming their cybersecurity policies, wherein they do not establish laws until concerns over particular cybersecurity issues become urgent and prevalent. Because of this reactive policymaking and enforcement are developed individually by sectors. The regulatory frameworks in both countries are constantly evolving as more regulations are created to address cyber-threats specific for each sector. As a result, due to the ad-hoc nature of regulations, it is not surprising that there is no single enforcement agency in the two case studies that is responsible for the enforcement of all cybersecurity regulations. Table 6 summarizes these findings.

Table 6: Regulation and Enforcement of Disparate Cases

| | **Brazil** | **Chile** |
|---|---|---|
| Are regulation/enforcement sector-specific? | Yes | Yes |
| Is there an enforcement agency? | No | No |

The two disparate cases have different focuses on their governments' relationships. Whereas Brazil places more emphasis on its international relationships, Chile emphasizes both the private sector and international actors. Both countries invested extensively in the Budapest Convention of the Council of Europe, transforming their cybersecurity policies to align with international standards. In terms of the relationship between the governments and the private sector as related to public consultation on legislation, both have some channels for the private sector to input on legislation – Brazil through private sector forums, Chile through civil society councils—although the efficacy of these inputs differs. Table 7 summarizes these findings.

Table 7: Relationships of Disparate Cases

| | **Brazil** | **Chile** |
|---|---|---|
| Are there international relationships? | Yes | Yes |
| Can the private sector weigh in? | Somewhat | Yes |
| What characterizes information sharing? | Minimal | Sufficient |

In both cases, the move towards toward unitary systems and the potential of these efforts depends on the progression of their domestic politics. The outcome of the 2022 presidential election in Brazil may influence the direction of future national strategy on cybersecurity. It is anticipated that this national strategy will sustain if President Bolsonaro remains in power. Yet, if his main opposition defeats him, it may change the course of Brazil's cybersecurity regulatory system. In the case of Chile, as it proposed a new constitution replacing the one passed under Pinochet's dictatorship in July 8, 2022, it is possible that the lobby pathway underwritten in the past constitution and laws could be altered because the new constitution envisions a stronger government role.

## Cross-case Comparison

Cybersecurity regulations and enforcement mechanisms are the essential parts of the larger regulatory system. Their presence or the lack thereof influences the legal framework's practicality. When comparing both unitary and disparate cases, it is clear that the unitary system is more effective in creating an fruitful environment for the private sector. The three unitary cases, France, Lithuania and Singapore, fit our evaluation criteria for effective systems, in which their unitary systems create clear legal frameworks, have non-overlapping jurisdictions with established enforcement mechanisms, and are collaborative with both international and private actors. In contrast, the disparate systems are less effective. The Brazil and Chile case studies reveal that their disparate systems are complex and discursive, with structural gaps and overlaps. As a result, disparate systems are ineffective, according to our evaluation criteria, for the private sector to navigate and operate.

Additionally, our research shows that there is a trend for disparate cases to address the ineffectiveness of their system by transitioning to unitary systems. For example, both Brazil and Chile acknowledge the deficiencies in their systems and are working to refine their disparate systems by restructuring toward unitary governance. One of the case studies, Lithuania, presents a successful case of such transition. Lithuania did not have an organized system on cybersecurity regulation between the period when it became independent in 1990 to before it joined the EU in 2004. Lithuania managed to reorganize its cybersecurity legal framework to be in line with Budapest Convention as well as with the EU requirements when it joined the EU. The changes in the legal framework were followed by structural changes. The unitary system style and the National Cyber Security Centre came into existence in 2015 and the National Cyber Strategy was updated shortly to reflect the private sector interests and to strengthen the trust in the cybersecurity authorities.

Furthermore, in regard to private sectors' ability to weigh in on cybersecurity legislation, this report finds no interdependency between system style and the private sector's ability to

participate in a country's legislation on cybersecurity or system style and information sharing. In democracies, the private sector can weigh in on the legislative process if there is a clear lobbying pathway and proposals from private enterprises are taken into account. Two of the cases, Brazil and Lithuania, were identified as lacking pathways for the private sector to provide feedback. In the case of Brazil, clear avenues for private sector input are not defined. Instead, sectoral agencies have at times have hosted forums for input, but forums are not legally mandated. Lithuania, on the other hand, has been improving public-private interaction. Because its transition is fairly recent, Lithuania still has some residual transformation "symptoms" in its private-public relationships, such as mistrust in the authorities and fear of bureaucratic corruption. Ultimately, our findings cannot conclude that system style in a democracy influences private sectors' ability to weigh in cybersecurity legislations and information sharing. The variations we observed across cases on private participation in legislation and information sharing largely depend on each country's domestic political landscape, rather than the style of their regulatory systems.

# Brazil

Brazil has a disparate governance model with an effective cybersecurity governance system in place, based on its developing national cybersecurity framework and growing international cooperation. Brazil has low development of public-private partnerships, as demonstrated by the insufficient ability for the private sector and other stakeholders to provide feedback on legislation through diverse communication methods, such as meetings or conventions. Brazil acts as an interesting case study that demonstrates the attempt to transition from a disparate governance model to a more unitary approach. Table 8 summarizes finding on Brazil's cybersecurity framework.

Table 8: Findings on Brazil's Cybersecurity Framework

| **Overall Cybersecurity Assessment** | |
|---|---|
| Overall system effectiveness | Moderate |
| System style | Transitional |
| National strategy and framework | Initial stage |
| NCSI index rating | 46.75 |
| **Legal Framework and Effectiveness** | |
| Is the framework parsimonious? | No |
| Is jurisdiction clear? | Yes |
| Are there gaps in the framework? | Yes |
| Is regulation: outcome focused, technology neutral, risk-based? | Risk-based |
| **Regulation and Enforcement** | |
| Are regulation/enforcement sector-specific? | Yes |
| Is there an enforcement agency? | No |
| **Relationships** | |
| Are there international relationships? | Yes |
| Can the private sector weigh in? | Somewhat |
| What characterizes information sharing? | Minimal |

## Country Background

Brazil is a democracy as it holds regular national elections in which power transfers from one party to another with minimal disruptions. As of this writing Brazil's gross domestic product (GDP) is 1.6 trillion. While economically smaller than other Western countries (such as Germany) regionally, Brazil maintains the highest GDP in Latin America (World Bank, 2022). In 2022, Brazil increased its overall security spending by one billion USD, a bulk of which is directed at cloud security and protection against cyberattacks.

Brazil earned a score of 46.75 out of 100 on the NCSI Index in which Brazil ranked 18th globally (NCSI, Brazil). An early adopter of online banking, Brazil experienced a substantial increase in cybercrime during the mid-2010's. In 2015, more than half of all cyberattacks reported to Brazilian officials originated within Brazil's borders (CERT.br, 2015). The adoption of digital banking has resulted in a mostly cashless economy which has led to Brazil being one of the top five countries in which cyberattacks originate globally (Security Today, 2017). In order to combat its cybercrime problem, Brazil increased cybercrime investigations and criminal penalties. This approach has been flagged by civil liberty organizations as an encroachment into basic digital freedoms (Council on Foreign Relations, 2016).

In 2020, the Brazilian government approved its new cybersecurity strategy, E-Cyber. While there are many aspects of this strategy that aim to protect user data, there is also an overarching directive of creating a centralized or unitary governance model. Among numerous initiatives present in the strategy, the following are most relevant. The strategy seeks to promote international coordination with "actors related to cybersecurity, beyond the federal sphere to promote joint analysis of the challenges faced in the fight against cybercrime." It looks to assist in the formulation of public policies and create a national cybersecurity council. It aims to create groups in different sectors, under the coordination of the Institutional Security Office, to promote discussion on the topic, through informal participation mechanisms and further establish a routine of cybersecurity compliance checks, internally, in public agencies and in private entities. And finally, to allow the convergence of efforts and initiative, and act in a complementary way to receive complaints, investigate incidents and promote society's awareness and education on the subject.

In addition to this national strategy which focuses on the period between 2020 and 2023, there are other relevant federal structures that should be noted. The Office of Institutional Security of Brazil is responsible for coordinating cybersecurity at the national level. The office's work is to allow for broad, cooperative, and participatory action that matches with cyber defense actions related to the Ministry of Defense. In addition to the national strategy for cybersecurity, there are several regulations that govern Brazilian cybersecurity. In December 2018, Decree 9637 instituted the National Policy for Information Security, Decree 10222 approved the National Security Strategy, and Instruction No. 4 of the Institutional Security Office of the Presidency, set the minimum cybersecurity requirement for 5G telephone networks (Azevedo Sette Advogados, 2021).

In October 2022, Brazil will hold its next Presidential election, which may change the Brazilian cybersecurity landscape and future national security related objectives. In an echo of President Trump's rejection of the US election in 2020, Brazilian President Bolsonaro stated in 2021 that he may not accept Brazil's election results (Reuters, 2021). This statement alarmed international officials, including the US, which sent the National Security Advisor-Jake Sullivan to warn Bolsonaro against interfering with the Brazilian election results (Choi, 2021). Recently,

Bolsonaro has maintained that he is not seeking a coup and that he is not afraid of an election loss. And yet, Bolsonaro and his supporters have flooded digital media platforms with disinformation and outright falsehoods (Freedom House, 2021). At the moment it is unclear whether Bolsonaro will accept or reject the election results, but it is clear that the campaign does not have a problem producing information designed to mislead or confuse Brazilian voters. The outcome of this election could have serious implications for the future of Brazilian cybersecurity regulation creating significant uncertainty.

## Cybersecurity Agencies

At this time there is no central cybersecurity authority in Brazil; however, the national cybersecurity strategy E-Cyber aims to create a more centralized system. For the most part, cybersecurity in Brazil is sector oriented, with four different regulatory agencies establishing sector specific requirements. These regulatory agencies are – the Central Bank (Banco Central do Brasil, BACEN), the Securities and Exchange Commission (Comissão de Valores, CVM), the National Telecommunications Agency (Agência Nacional de Telecomunicações, ANATEL), and the Private Insurance Authority (Superintendência de Seguros Privados, SUSEP). Each regulatory agency governs a unique aspect of cybersecurity from financial transactions to public interest telecoms.

In 2018, the Brazilian National Monetary Council issued resolution 4.658 which set new cybersecurity requirements for institutions that fall under the regulation of the central bank. The Brazilian National Monetary Council is a major institution of the Brazilian Financial system, tasked with creating monetary and credit policies in the interest of Brazilian monetary stability and economic development (Banco Central Do Brasil). The National Monetary Council is made of three members who meet at least once a month. The members are the Minister of Finance, the Minister of Planning, Development and Management, and the Governor of the Banco Central do Brasil. While the council formulates monetary and credit policies, the Banco Central is the agency that actively regulates financial institutions. Institutions that fall under the Banco Centrals authority are banks institutions authorized to operate within Brazil, those that operate in foreign exchange markets, and those which transfer national or foreign currency of interest entities headquartered in Brazil (Circular 3.689). As such, the Banco Central set cybersecurity requirements for all entities that fall within its scope of regulation.

Under Instruction No.505/2011, the Securities and Exchange Commission is tasked with setting rules and procedures for operations in regulated securities markets. Although there is some overlap between regulation by the Banco Central and the Securities and Exchange Commission, the latter focuses on the regulation of market participants and licensed financial intermediaries. In addition to setting rules and procedures related to the implementation of cybersecurity measures, CVM sets rules related to third-party services notification process in the event of a breach. Under the authority of the National Monetary Council, the CVM is a monetary agency whose cybersecurity initiatives focus on data protection.

In addition to the monetary sector, the third sectoral regulator of cybersecurity is the National Telecommunications Agency which is tasked with identifying any failures or vulnerabilities that may compromise the safety of users or the country's telecommunications networks. Resolution No. 740/2020 sets out to apply cybersecurity regulation in the telecommunications sectors. As such, the National Telecommunications Agency is tasked with establishing conduct and procedures that aid in the promotion of telecommunication security and

the protection of critical telecommunication infrastructure. While the primary focus of the cybersecurity in this sector is the protection of data, ANATEL aims to protect telecommunication operations from malicious attacks. With the exception of providers that qualify as small sized (PPP, Prestadores de Pequeno Porte) resolution 740/2020 focuses on all telecommunication service providers. An independent agency with governing authority over telecommunications entities in Brazil, ANATEL operates outside the scope of any government ministry and its ruling can only be appealed through the Brazilian judicial system.

The fourth major cybersecurity sectoral regulator is the Private Insurance Authority. Constituted by the National Council of Private Insurance, the Superintendence of Private Insurances, the Reinsurance Companies, the Insurance Companies, and the Insurance Brokers, the Private Insurance Authority supervises and regulates the insurance, open private pension funds, and capitalization markets of Brazil (Superintendência de Seguros Privados). Directly linked to the Ministry of Finance, SUSEP acts as the executive agency that acts as the governing body for the Brazilian insurance market. In addition to this direct link, SUSEP is managed by a managing council, comprised of the Ministry of Finance appointed Superintendent and four directors. The council is responsible for enacting compliance regulation. Under Circular No. 638/2021, SUSEP set guiding principles for internal cybersecurity policies, guidelines for identifying risks, and the measures necessary to limit said risks. Furthermore, under the Circular, SUSEP establishes when regulated entities are liable for cyber incidents. Here two we have another example of a cybersecurity agency linked to monetary policy.

While each of the four sectors comprise the bulk of cybersecurity regulatory frameworks and the national strategy is an attempt by the President to remedy gaps that result from response focused sectoral measures, it was the Brazilian Internet Act of 2014 which set cybersecurity standards for the public. The law sets the basic principles, guarantees, rights and obligations for the use of internet in Brazil, as well as addressing the protection of data and privacy, and network neutrality. Although it is not necessarily a direct cybersecurity measure, it did govern some security aspects for internet application.

Moreover, the Brazilian Data Protection Law which went into effect in 2020, established a legal framework for personal data and processing operation. It also details the rights of personal data subjects, sets data processing, and reporting requirements in the event of data breaches. A major development of the Data Protection Law was the creation of the National Data Protection Authority (ANPD). The ANPD is a full-scale data protection regulation that coincides with the EU General Data Protection Act (Hogan Lovells, 2019). A portion of the ANPD's authority was implement through Executive Order no. 869/18, where the ANDP gained authority over the issuance of rules and regulation, information requests, development of domestic and international data protection and privacy practices to name a few.

In a similar fashion, Decree no. 9637/2018 established the National Policy for Information Security. Issued by President Bolsonaro, the decree amends a 1997 Decree that regulated the provisions of art. The updated decree sets guidelines to guarantee the authenticity, confidentiality and integrity of information contained in federal administration networks (EU Cyber Direct, 2018). It should be noted, that while sectoral regulation comprises the bulk of cybersecurity framework, these laws and decree updates are attempts to close cybersecurity gaps that result from its disparate framework.

Another example of this gap closure framework is how the National Health Surveillance Agency (ANVISA) set cybersecurity guidelines governing medical devices under ANVISA Guide No. 38/2020. The Federal Health Councils Resolution No. 1.821/2007 and 467/2020

regulated cybersecurity related to medical records. And the Brazilian Electricity Regulatory Agency established cybersecurity regulation for energy. Though these Agencies make up a portion of cybersecurity governance policy, they further highlight the disparate nature of the Brazilian system.

To elaborate, federal decrees should be viewed as a part of the Brazilian government's goal of providing guidelines on matters of cybersecurity and critical infrastructure. Where Decree No. 9.573/2018 defines the National *Policy* for Critical Infrastructure Security, Decree No. 10.569/2020 looks to set the National *Strategy* for Critical Infrastructure Security. This National Strategy for Critical Infrastructure Security lays out the road map by which the national policy implements its guidelines. Places such as, facilities, services, and assets, where any disruption would create political, social, and economic turmoil are the target of these decrees.

Finally, the National Authority of Data Protection (ANPD) sets obligations and processing requirements with which data processors must comply. Data Processors and Data Controllers are required to protect personal data from unauthorized access and protect personal data against nefarious or accidental incidents that lead to loss, alteration, and destruction. Additionally, ANPD sets notification requirements in the event of a security breach. ANPD further protects data subjects right to access, correct erroneous data, and revoke consent to access among others (Data Protection, 2018). Outside of the sectoral regulatory agencies, there are a number of targeted decrees and strategies that have been implemented in order to reduce the pitfalls of a disparate system.

## Summarization and Evaluation

As a result of sector specific cybersecurity regulation, there are gaps in public sector related cybersecurity. Until the implementation of E-Cyber, cybersecurity was highly sector oriented with piecemeal regulations and laws that attempted to address specific cybersecurity problems. As a result, cybersecurity governance in Brazil is not only disparate but disconnected. Apart from the Monetary Councils influence over regulation in the Banco Central and the Securities and Exchange Commission, there is not a central point in which cybersecurity measures are discussed. The current national strategy, aware of these gaps, looks to begin the process of moving toward a more centralized model. However, the implementation of E-Cyber initiatives must contend with an established piecemeal system with multiple laws and regulations.

It is apparent that early adoption of digital banking revealed the necessity of cybersecurity in financial institutions. As such, a bulk of sector regulations target not only data but financial activity. Moreover, rather than designing a national model for cybersecurity as it adopted digital technologies, Brazil responded to cybersecurity concerns after they became a problem. As a result, Brazil is attempting to redesign its cybersecurity structure within a system that was not designed intentionally but rather developed responsively. For this reason, it is important to note that while E-Cyber is a move toward a unitary model, cybersecurity governance is sectoral, and any top-level initiatives must contend with a web of sector specific regulation. E-Cyber is thus simply the initial step toward a future unitary model.

While there is some concern with the president's unclear position on the upcoming presidential election, it is clear that his cybersecurity agenda aims to create a more unitary cybersecurity structure. Through the noted decrees and the updated national cybersecurity strategy, his administration has taken a proactive role in updating cybersecurity policy while also defining guidelines and protections for digital spaces. However, while Bolsonaro's policy favors

the creation of a better-defined cybersecurity governance model, politically he has been accused of spreading disinformation and his campaign supporters have been accused of intimidating political opponents (Reuters, 2020).

# Regulatory Framework

An early adopter of internet banking, much of the legislative framework in Brazil is a scattered and decentralized system with very limited overlap. For this reason and in response to constant cyberattacks which places Brazil behind only the US, China, Germany and the UK, the Brazilian legislative framework is aimed at the protection data and limiting private sector security exposures.

## National Framework

A major point of concern within the Brazilian cybersecurity framework is protection against cybercrime. Federal Law No. 14.155/21 addresses unauthorized access or what is commonly known as hacking. Article 2 of Federal Law No. 13.260/16 is directed at addressing Denial of service attacks, or attacks which intend to shut down a machine or system. Similarly, Federal Laws No. 14.155/21, Federal Laws No. 9.296/96, address phishing, and malware infection respectively. Identity theft, electronic theft and system exploitation are all addressed in the federal penal code.

Beyond these laws that target the various ways in which cybercrime takes place the following are the primary legislative measures make up cybersecurity in Brazil. The 2018 Brazilian Data Protection Law sets the legal framework for personal data rights and protections. The Brazilian Internet Act and Decree No. 8.771/16 set standards for online applications. From here the bulk of legislation is governed within each sector, which is noted in the previous section.

## Enforcement Mechanisms

Similar to Brazil's sector specific regulatory agencies, enforcement of its national cybersecurity regulatory framework is disparate. Each sector agency is tasked with establishing and enforcing the guidelines and regulations within its regulatory scope. Though there are similar approaches to how each agency regulates its sector, enforcement is targeted at the type of entity being regulated.

The Central Bank has the power to discipline and apply administrative punishment to companies linked to the sector. Under the Brazilian Financial System (Law 134.506/2017) the Central bank can issue fines, prohibit activities or operations, remove persons allegedly involved in irregularities among other actions. In the realm of cybersecurity, BACEN has the authority to require a plan of action for incident responses in the event of a systems breach. A major focus of cybersecurity action revolves around data protection and disclosure.

The Securities and Exchange Commission is responsible for analyzing the securities market and imposing penalties for offenders. In addition to imposing cost related penalties, it can take legal action. Under the Provisional Executive Order No. 784/2017 any convictions made by the Securities and Exchange Commission, such as prohibition to trade and or act on the securities market, suspension or disqualification are enacted immediately. If an entity were to appeal the Commission's ruling, it would have to request penalty suspension from the Commission until the final trail.

The Telecommunication Agency can issue regulations and directives, grant, or revoke certifications and monitor the integrity telecommunications service providers. As a major agency within the domestic authority, the Telecommunications Agency also represents the Brazilian government in international telecommunications agreements. Under resolution 740, which targets procedures for security in telecommunications services and critical telecommunications infrastructure, ANATEL seeks to reduce infrastructural susceptibility to attacks and frauds.

The Private Insurance Authority (SUSEP) under Resolution CNSP # 060/2001 has the authority to issue administrative sanctions. This is the primary way that SUSEP enforces its authority on regulated entities within its regulatory scope. Moreover, in matters related to insurance SUSEP has the authority to issue judgments and monetary fines for rule violations.

## Information Sharing

There are no requirements within the national cybersecurity framework that mandate information sharing between sector regulators. However, due to the severity of cybercrime the government created through presidential decree the Federal Cyber Incident Management Network. The goal of the network is to coordinate response to cyber security incidents. In the event of a cybersecurity breach, the government makes itself available to network members and strongly encourages contact and coordination with the most specific CSIRT or security team (RFC 2350, 2021). Network members are made of public businesses, enterprises, and other subsidiaries who choose to coordinate willingly (Dascalu, 2021).

## Summarization and Evaluation

Due to the disparate structure of domestic cyber governance, regulation and enforcement take place on a sector-by-sector basis. As stated earlier, there is some overlap in the type of authority that each agency has with regard to its regulated sector, but there are also unique penalties that each may employ. What is apparent however it the absence of a central authority in the lack of cross sector regulation and enforcement.

As it is, the way in which each sector has attempted to standardize cybersecurity policy has been to implement similar sectoral requirements. All sectors require the protection of data and set breach notification mandates. Each sector uses a mixture of financial penalties, license suspensions and what I would call an accountability officer. That is, an executive tasked with overseeing cybersecurity policies and is responsible for managing cybersecurity incidents (Kujawski et al, 2021). It is clear, that in the absence of a national strategy regulatory sectors attempted to develop coherence in the system through the implementation of similar sectoral guidelines and penalties. However, now that there is national strategy, one that looks to unify a web of regulation based on targeted sector regulation and based on consumer protection should be seen as barriers to transition. Within this regulatory framework there is a divide between the system that was born out of necessity and the target system. The responsive system resulted in different sectors with a variety of measures aimed at filling systemic gaps. Whereas, the target system, outlined in the National Strategy looks to the future and aims to develop into a unitary system. Indeed, the National Strategy is not merely an outline for the future, but also a type of bridge between the two systems.

And yet, where the National Strategy aims to be a bridge between to national cybersecurity systems, it fails to have significant influence in any one sector. In truth, the strategy is a broad list of national goal without much enforcement power. It aims to promote a

unitary model without carving out the pathway toward success. As such, it should be considered a soft power approach to cybersecurity governance. Put another way, the national strategy is not a forceful overhaul of cyber governance, but rather a light touch that uses federal influence in order to transition cybersecurity from a disparate system to a unitary one.

# Relationships

Under the new National Strategy for cybersecurity there is a renewed focus on strengthening international cyber governance cooperation. A major regional power, Brazil has participated in a number of different international discussion on cyber governance policy. What follows is an overview of the two major avenues in cyber governance, international institutional relationships, and private sector relationships.

## International Cooperation

In terms of cybersecurity Brazil has acted to meet global standards, while also protecting its sovereign interests. Although it did not publish its first national cybersecurity policy until 2020, which was after roughly 100 other countries, Brazil has been a major international actor in international internet governance and cybersecurity discussions (Mueller & Kuerbis, 2018). The fragmented and at times extempore system that has been created at times adopts international guidelines, while mostly addressing internal necessity. In the case of medical devices, the National Health Services Authority developed its cybersecurity practices based on the International Medical Devices Regulators Forum. Other than this, cybersecurity guidelines do not directly follow international standards, sectoral regulators do however acknowledge need to comply with international law. Especially, laws that govern human rights and humanitarian law (International Cyber Law, 2021). In the same vein, Brazil actively advocates for the protection of state sovereignty including digital spaces. In short, the Brazilian position is one of international cooperation without direct interference with state sovereignty. Under the national cybersecurity strategy E-Cyber there is a focus on entering international cyber governance discussions with the intent of sharing information and developing cyber partnerships.

In 2020 the European Union hosted Brazil for Cyber Dialogue in Brussel (Council on Foreign Relations, 2020). This comes a few years after a UN Vote on Russia's 'New' Cybercrime Resolution at the UN (2018), in which questions of censorship, traffic throttling, and internet regulation were being considered. At the time there were three governance positions which some have characterized as the "global and open" the "sovereign and controlled" and the "digital deciders camp." At this vote Brazil voted in favor of the Russian Cybercrime Resolution, which situated them on the side of independent cybercrime control or the "sovereign and controlled" (Sherman & Morgus, 2018).

Apart from disagreements on the line between international cooperation and sovereignty in cybersecurity, Brazil participates in EU cyber governance discussions. Actively engaged in the UN's Open-Ended Working Group and the Group of Governmental Experts, Brazil continues to work with the EU to establish agreed up measures which govern international cyberspace. In a statement made to the United Nations Group of Governmental Experts, Brazil maintains that it "firmly believes that in their use of information and communications technologies, States must comply with international law, including the United Nations Charter, international human rights law and international humanitarian law." (International Cyber Law, 2021). The ongoing dialogue

between Brazil and the EU began in the early 2010's when both worked together to establish research agendas, develop digital infrastructure projects and the construction of cross continental submarine fiber cable (Council on Foreign Relations, 2020).

Earlier this year Brazil accessioned to the Budapest Convention after a period as an official observer, joining South Africa as one of only two BRICS members. A clear step toward national framework harmonization, the accession may have major national and international consequences (Belli, 2022). For that matter, the entrance of Brazil into the convention will lead not only to greater cooperation, but to the adaptation of international cooperation mechanisms. In effect, this is a major step toward not only acknowledging international cyber governance frameworks, but rather a commitment to implement similar frameworks domestically. Furthermore, as a priority country it has capacity building and technical assistance activities to enhance the ability of criminal justice authorities (Strasbourg, 2021).

As was the case with many of the U.S. relationships with other countries, the Snowden Leak, damaged US-Brazil relations. The former Brazilian president went so far as to publicly denounce the U.S espionage. Under President Obama, however, the previously paused U.S.-Brazil cyber working groups were resumed. Through the US-Brazil Internet and Information and Communication Technology Working Group, the two countries were able to strengthen a joint commitment to a secure cyberspace. The Working Group was focused on what the US deems are key cyber and internet policy topics, such as, cybersecurity, data protection, data free flow (U.S. Department of State, 2018). At the moment the US-Brazil relationship is one of discussion. Both countries agreed after the Working Group to "explore a series of technical exchanges."

## Private Sector

The relationship between the private sector and federal government is characterized by cooperation. Especially under the current administration, which values free markets and prioritizes private sector growth, the relationship has become a major political talking point. Until recently, President Bolsonaro maintained significant support in the business community, but comments on election result rejection have frayed support (Pooler, 2021). Indeed, much of national cybersecurity regulation is directed at the protection of private sector data. As the largest and wealthiest country in Latin America, Brazil is the target substantial cyberattack. Behind only the US, Germany and the UK in ransomware attacks, a major focus of private sector regulation centers on the protection of data. In 2017 Brazil accounted for 6% of all cyber threats globally with over 300,000 attacks originating domestically. In that context, it is not surprising that cybercrime and user protection is a state initiative directed at private entities. As was noted the five sectoral agencies have made data protection a top priority for market actors.

The connection and the flow of information between the private sector and the Brazilian government is not explicitly designed. The best avenue for private sector entities to participate in the creation of cyber policy is through participation in public forums. For example, in 2017 the Central Bank proposed sectoral regulatory changes in the interest of cybersecurity. Before implementing the change, the Central Bank made itself available to commentary by regulated entities (Legal Intelligence Center, 2017).

## Summarization and Evaluation

In truth, the relationships between international institutions and private sector entities are not explicitly defined. Instead, Brazilian cooperation is centered on protection of sovereign

authority. As such, Brazil's approach to international cooperation historically has not looked to fully accept international guidelines, but rather protect its cyber governance sovereignty. That is not to say that Brazil is on an island, nor that it does not interact or implement international guidelines. Indeed, the accession to the Budapest Convention marks a shift from international discussion observer to commitment in international guideline implementation. Furthermore, this shift is also an acknowledgment of the severity and borderless nature of cybercrime. Aware that monitoring digital spaces requires international cooperation, the joining of the information exchange focused Budapest Convention is an acknowledgment of cybercrime gaps within the disparate Brazilian system.

Alternately, the relationship between the Brazilian government and the private sector is one of support. Under the current administration, the aim toward governance is not active regulation, but rather cooperative protection of private sector customer data. Indeed, regulations typically focus on the implementation of mechanisms that increase private sector security and private sector cooperation. Still, one of the major pitfalls of the disparate system model is apparent in public/private relations. Without a clear central cybersecurity authority that governs national cybersecurity regulation, a communication gap has developed. This gap not only impedes communication between the major sector regulators, but it also limits how the private sector can interact with and impact the creation of cybersecurity regulation. Instead, different sectors allow different levels of input via public forums at irregular points in the creation of sectoral cybersecurity policy.

## Overall Effectiveness

It is apparent that the disparate cybersecurity model that developed in Brazil has been reactionary. Early adoption of internet banking placed national cyber governance policy behind new technological adoption. As a result, overall effectiveness of the system should be characterized as moderate. That is to say, the system is effective in its sectoral regulation, but sectoral focus has resulted in cybersecurity gaps. Moreover, these gaps are mainly addressed in the event of a breach. Rather than a system designed to limit exposure, the disparate system in Brazil was developed in *response* to exposure. These gaps and the responsive nature of cybersecurity Brazil becomes more apparent in the NCSI index.

According to the NCSI index, the Brazilian cybersecurity environment is not secure. With a rating of 46.75, the index notes the gaps in cybersecurity standards in both public and private sectors. The NCSI highlights the absence of any cybersecurity responsibility for digital service providers, the lack of a standard for the public sector and lack of a supervisory authority. However, the global cybersecurity ranking has increased drastically over the last couple of years, having moved from the 74$^{th}$ to 18$^{th}$. This change comes as a result of the new national cybersecurity strategy and more comprehensive international cooperation.

The current disparate model has resulted in fragmented cybersecurity policy and unclear cybersecurity jurisdiction. In cases directly related to sectoral agencies, cybersecurity guidelines are clear. Whereas, in instances where a case is not directly related to any one sector, there is unclear regulator application. As previously stated, the sectoral nature of cybersecurity policy has left numerous gaps in private sector coverage. To the degree that the impact of cybercrime private sector actors has forced significant invest in their private entity cybersecurity.

And yet, cybersecurity authority within the disparate Brazilian governance model is not completely devoid of overlap. While both the Central Bank and the Securities and Exchange

Commission have substantial regulatory authority within their sector, the Monetary Council maintains influence over cybersecurity policies in each sector in the interest of securing economic stability in Brazil.

Apart from this, there is not a clear public-private partnership in Brazil. The responsive nature of cybersecurity policy has resulted in a lack of direction from a central authority in cyber governance policy creation. Indeed, there is no central authority and the most recent attempt at developing a more unitary system with a type of central authority is severely lacking in enforcement. The implementation of a national cybersecurity council without legislative regulatory authority is half measure that does not offer a solution but a suggestion for shifting cybersecurity governance to a more unitary system. As a result, the cybersecurity model present in Brazil is a scattered collection of responsive measures, that does not favor long term strategy, but rather aims at reducing the severity of system exposure. Finally, the risk-based nature of the Brazilian disparate model has resulted in a collection of sectoral focused, and agency independent decrees and regulations that create a system of roadblocks in the effort to transition to unitary model.

# Chile

The Republic of Chile has a disparate governance model with a relatively effective cybersecurity governance system in place, based on its developing national cybersecurity framework and robust international cooperation. Chile's cybersecurity regulatory landscape primarily focuses on telecommunication, Critical Information Infrastructure (CTI), and banking sectors. Chile has highly developed public-private partnerships, as demonstrated by the ability of the private sector and other stakeholders to provide feedback on legislation. Chile is an interesting case study because it is transitioning from a disparate system toward a unitary one due to the recent legislative proposal on establishing the National Cybersecurity Agency. Table 9 summarizes this case study's high-level findings about Chile's cybersecurity framework.

Table 9: Findings on Chile's Cybersecurity Framework

| **Overall Cybersecurity Assessment** | |
|---|---|
| Overall system effectiveness | Moderate |
| System style | Transitional |
| National strategy and framework | Initial stage |
| NCSI index rating | 59.41 |
| **Legal Framework and Its Effectiveness** | |
| Is the framework parsimonious? | No |
| Is jurisdiction clear? | In development |
| Are there gaps in the framework? | Yes |
| Is regulation: outcome focused, technology neutral, risk-based? | Risk based, technology neutral |
| **Regulation and Enforcement** | |
| Are regulation/enforcement sector-specific? | Yes |
| Is there an enforcement agency? | No |
| **Relationships** | |
| Are there international relationships? | Yes |
| Can the private sector weigh in? | Yes |
| What characterizes information sharing? | Sufficient |

## Country Background

Chile is a democracy with an annual GDP of 317.06 billion U.S. dollars and a population of 19.12 million people (The World Bank, 2022). It earned a score of 59.41 on the NCSI Index, ranking 47 globally, and is one of the best performers on cybersecurity in South America (NCSI: Chile, 2021). Politically, the executive power of Chile is entrusted to the president, and the legislative power to the bicameral National Congress (Congreso Nacional), which consists of the Senate and the Chamber of Deputies (Central Intelligence Agency, 2022). Since its return to democracy in 1989, Chile has followed a market-friendly neoliberal economic model, spurring a continued rise in economic growth (O'Neil, 2022). Private businesses have long enjoyed access to policy processes under Pinochet's dictatorship in 1984 and after Chile's return to democracy. The Coalition of Parties for Democracy (Concertación de Partidos por la Democracia) largely maintained the participation of business elites under Pinochet's dictatorship, allowing the leadership of the business to participate in policy formulation regarding major economic-policy issues even prior to democratization (Silva, 1997, p. 173). The private sector's participation in policy formation benefitted both the policymakers and the private sector, addressing the needs of the national economy in general while building confidence in the various economic sectors that those policies would not be at the expense of their interests (Silva, 1997, p. 155). In Chile, the consultation of the private sector in policy formation has contributed to the implementation of workable policies (Silva, 1997, p. 155). Today, similar public-private sector cooperation will come to serve an important role in the forming of national cybersecurity policies (Carlos & Pablo, 2016, p. 13).

Cybersecurity has been a top political agenda through several of the last Chilean administrations, particularly that of the former President Sebastián Piñera, who had served two non-consecutive terms of presidency in 2010 and 2018, respectively. Built upon the Digital Agenda of 2020 (La Agenda Digital 2020) of former President Michelle Jeria's administration, Piñera signed a series of presidential decrees in 2019 covering a range of cybersecurity-related issues, introducing a Digital Transformation (La Transformación Digital) that includes the normalization the use of digital technologies (Ministry General Secretariat of the Presidency of Chile, 2014). Chile has also been a keen participant in the international conventions for cybersecurity, such as the Budapest Convention on Cybercrime of the Council of Europe (the "Budapest Convention") while structuring its policies for cybersecurity in compliance with international standards.

Although Chile does not have a singular agency that has jurisdiction over cybersecurity and has the final word on a nation's cybersecurity, Chile presents an interesting case study because it is currently on its way to establishing a Framework Law on Cybersecurity and CTI. To create a special authority agency that oversees the nation's cybersecurity, the National Cybersecurity Agency, the proposed bill was introduced under the Piñera administration and aims to:

> Establish the institutions, principles and general regulations that allow structuring, regulating and coordinating the cybersecurity actions of the State Administration bodies and between them and individuals; to establish the minimum requirements for the prevention, containment, resolution and response to cybersecurity incidents; to establish the attributions and obligations of the State bodies as well as the duties of private institutions that possess information infrastructure qualified as critical and, in both cases, the mechanisms of control, supervision,

and responsibility for the infringement of the regulations (Carey & Mercado, 2022; To the Law Project, 2022).

## Cybersecurity Agencies

In Chile, there is no unitary authority overseeing the regulations on cybersecurity. The current institutional structure requires the strategic coordination of different government bodies because regulations on cybersecurity and offenses related to information and computer systems are dispersed. The regulations on cybersecurity are divided among three major government ministries and entities, the Ministry of the Interior and Public Security; the Ministry of Telecommunications; and the Ministry of Economy, Development, and Tourism. Because the regulations on cybersecurity are separated among different agencies, it inevitably creates structural overlaps and gaps in their jurisdictions.

The main body for cybersecurity in Chile is the Interministerial Committee on Cybersecurity under the Ministry of Interior and Public Security created under the Supreme Decree Nº 579/2019, which is made up of the Undersecretariats of Interior, Foreign Affairs, Defense, Finance; General Secretariats of the Presidency, Economy, Justice, Telecommunications; and the National Intelligence Agency. The Supreme Decree Nº 533/2015 first established a Cybersecurity Interministerial Committee (CICS), which was later modified into the current Interministerial Committee on Cybersecurity (Comité Interministerial sobre Ciberseguridad, the "Committee") of the Ministry of the Interior and Public Security under the 2019 amendment. Because of Chile's dispersed system, the Interministerial Committee on Cybersecurity's main function is to advise the President of the Republic in the analysis and definition of a national cybersecurity policy, establishing a leadership role in coordinating the operations of those ministries involved and developing a proposal for the National Cybersecurity Policy (Amends Supreme, 2020). Under Article 8 of Nº 579/2019, the Advisory Commission of the Interministerial Cybersecurity Committee (the "Commission") is created under the Committee to provide technical assistance for the operation of the Committee, in which its tasks include responding to computer incidents or other multidisciplinary work groups in matters of cybersecurity (Amends Supreme, 2020).

The Ministry of the Interior and Public Security (Ministerio del Interior y Seguridad Pública, MISP) is the principal agency that provides preventive and investigative public policy design regarding cybersecurity. Under Article 1 of Law No. 20.502, the MISP is established as the main body responsible for the coordination, evaluation, and monitoring of plans and programs developed by the other ministries and public services in matters of crime prevention control (Creates the Ministry, 2011). Built upon its inter-sectoral coordination role, MISP assumes similar responsibilities regarding cybersecurity, including preparing the regulations and setting out safe mechanisms for exchanging information within the government bodies, and coordinating between high-level officers and other officials. In addition, MISP is responsible for investigative public policy, especially in collaboration with the Office of the Prosecutor. For example, under Exempt Resolution No. 10.168, 3/12/2013, the MISP creates the Organized Crime Department responsible for developing strategies for combating cybercrime (The Government, 2016, p. 34). And the Carabiniers of Chile's (Carabineros de Chile) OS9 Department is in charge of investigating cybercrimes (The Government, 2016, p. 34). Under Article 8, Section C, Law 19.974 establishes the State Intelligence System and creates the National Intelligence Agency, delegating the Investigations Police of Chile (Policía de

Investigaciones de Chile, PDI)'s Criminal Investigation Brigades (Brigadas de Investigación Criminal, BICRIM) to propose rules and procedures for the protection of the state's critical information systems (About the State, 2011; The Government, 2016, p. 34). Externally, MISP is the first point for disseminating information to citizens based on the different digital channels and social networks enabled by the internet. It works closely with the Ministry of Foreign Affairs to update the national cybersecurity regulations and implements them in adherence to the Budapest Convention (The Government, 2016, p. 34).

The Computer Security Incident Response Team (CSIRT) under MISP is in charge of responding to cybersecurity incidents. It is responsible for collecting information from other countries' and international CSIRTs. The national CSIRT's goal is to create a platform for information about cybersecurity incidents and implement a standardized template for cybersecurity incident reports and it is also responsible for identifying potential risks for CIT (Computer Security Incident Response Teams, 2021). CSIRT is also the primary agency for exercises related to cybersecurity incidents with different stakeholders to examine the vulnerabilities and improve and research ways of mitigation in the national systems (The Government, 2016, p. 36; Computer Security Incident Response Teams, 2021).

The Ministry of National Defense (Ministerio de Defensa Nacional, MINDEF) is responsible for the preventive and reactive response to cybersecurity challenges related to national defense. It collaborates with other government bodies, namely MISP, to advise on cybersecurity bills for the National Congress, in which it mainly oversees the planning of cybersecurity policies in the area of national defense (The Government, 2016, p. 34). Additionally, it is the regulatory agency in the defense sector. Under MINDEF, the Armed Forces are responsible for protecting their own information infrastructure by cooperating with the national intelligence systems in tasks related to national cybersecurity. For cybersecurity challenges for the National Defense, the Armed Forces are also responsible for executing the relevant institutional and operational plans (The Government, 2016, p. 26).

The Ministry of Transport and Telecommunications (Ministerio de Transportes y Telecomunicaciones, MTT) designs policies and monitors compliance with cybersecurity policies in the area of telecommunications. It is exclusively responsible for the implementation and enforcement of cybersecurity laws in the telecommunication sector, particularly Law 18.168 "General Telecommunications Law" and Law 20.478, "On Business Recovery and Continuity under Critical and Emergency Situation of the System of Public Telecommunications (General Telecommunications, 1982; On Recovery, 2010)." Article 39, Section C of Law 18.168 states that the MTT is responsible for the development of a backup plan for the country's critical telecommunications infrastructure to ensure the continuity of communications in emergency situations and for coordination with the various government agencies and institutions and with private agents for regulating and providing the protection of critical telecommunications infrastructures (General Telecommunications, 1982). Additionally, the MTT evaluates the resilience of telecommunication networks in Chile, proposing measures to improve it in both the public and private sectors. Moreover, in collaboration with the Interministerial Committee on Cyber Security, MTT is the main body responsible for coordinating the creation of the updated requirements for regulated economic sectors (The Government, 2016, p. 25).

The Ministry of Education (Ministerio de Educación, MINEDUC) is primarily responsible for promoting cybersecurity in the educational field. Its objective is to educate the general public about cybersecurity matters. This educational effort is mainly achieved through the creation of the Center for Education and Technology of the Ministry of Education of Chile

(Centro de Educación y Tecnología del Ministerio de Educación de Chile, Enlaces), which is one of the products of this information awareness process that trains school teachers in ICT use and integrates educational informatics in the school system to fulfill the needs of the information society of today (Ministry of Education, 2016). MINEDUC often collaborates with other institutions to raise cybersecurity awareness targeting different populations, particularly with the Ministry of Economy, Development, and Tourism (The Government, 2016, p. 34).

The Ministry of Economy, Development, and Tourism (Ministerio de Economía, Fomento y Turismo, MINECON) is responsible for overseeing the production of cybersecurity infrastructures and typically serves an auxiliary role in facilitating other ministries to increase productivity and further innovation in the cybersecurity awareness agenda. The National Standards Institute (Instituto Nacional de Normalización, INN) was created by the Production Development Corporation (Corporación de Fomento de la Producción, CORFO) in 1973 as a technical body in charge of overseeing quality infrastructure in the cybersecurity fields (National Standards Institute, 2016). The CORFO is a government agency dependent on the MINECON and supports entrepreneurship and innovation, particularly for promoting the development of advanced human capital regarding cybersecurity in the different technical- professional or vocational areas. On the other hand, MINECON promotes the modernization and competitiveness of the country's productive structure, private initiative, and market efficiency (On Recovery, 2010) and facilitates MINEDUC in promoting the Enlaces initiative and the Finance Ministry (Ministerio de Hacienda, MINHACIENDA) in processing the Cybersecurity Framework Act on personal data. Additionally, the Human Capital Committee under MINECON collaborates with the National Service for Older Persons (Servicio Nacional del Adulto Mayor, SENAMA) under the Ministry of Social Development (Ministerio de Desarrollo Social y Familia, MDS) to design and implement a cybersecurity campaign aimed at the elderly population, including training and dissemination (The Government, 2016, p. 34; National Service for Older Persons, 2021).

The Ministry of Justice and Human Rights (Ministerio de Justicia y Derechos Humanos, MINJUSTICIA) is responsible for updating legislation on the challenges posed by technological development, especially in charge of the task of updating the regulation on computer-related crimes and the national regulation on cybersecurity in adherence to the Budapest Convention (The Government, 2016, p. 34).

The Ministry of Foreign Affairs (Ministerio de Relaciones Exteriores, MINREL) serves as the central government body to oversee the international coordination of the national cybersecurity policy. Under MINREL, the Department for International and Human Security (Dirección de Seguridad Internacional y Humana, DISIN) is responsible for identifying, coordinating, and promoting Chile's cybersecurity position and interests within the international community (Ministry of Foreign Affairs, 2022). Similar to the role of MISP for inter-ministerial coordination, MINREL coordinates and promotes Chile's involvement in specialized international bodies and forums such as Meridian, Octopus, Organization of American States(OAS), Union of South American Nations, International Telecommunication Union, Internet Governance Forum, and United Nation expert groups (The Government, 2016, p. 24). Its tasks involve advancing the creation of bilateral work mechanisms, developing agendas and implementing cross-cutting political consultation instances with partner countries, and promoting the exchange of experiences with other countries in the field of cybersecurity, with emphasis on the implementation and evaluation of strategies and policies (Ministry of Foreign Affairs, 2022). Additionally, it works closely with MISP to advise the National Congress on cybersecurity

policy, ensuring that the regulations adhere to and implement the Budapest Convention. On the other hand, the ProChile, an institution of the Ministry of Foreign Affairs, oversees the export of national products and services in the field of cybersecurity (ProChile, n.d.).

The University of Chile is the main academic body and the contact point with international Computer Emergency Response Teams. One of the organizations under the University of Chile is the NIC Chile, which is responsible for maintaining and securing all names containing the ".CL" domain (NIC Chile, 2020).

### Summarization and Evaluation

Compared to other countries with unitary cybersecurity systems, Chile's cybersecurity authorities are less effective. Several different government agencies collectively are responsible for the regulation and implementation of cybersecurity policies in Chile, with the Interministerial Committee on Cybersecurity serving as the main committee for inter-ministerial coordination. Because jurisdiction over cybersecurity policy is dispersed among several agencies, as listed above, many ministries do not have a clear assignment but serve many individual roles when applicable. Consequently, this blurry distribution of jurisdiction results in overlapping of responsibility of some agencies while some gaps in others. For example, the jurisdiction for raising public cybersecurity awareness is shared among the Ministry of Education, Ministry of Social Development, and the Ministry of Economy, Development, and Tourism.

As a result of these complex coordination efforts among agencies, it sometimes fails to encapsulate all areas of regulation, blurring the jurisdiction. For example, there is currently no agency responsible for enforcing personal data protection regulations because the personal data protection bill was first introduced by the Minister of Economy, Development, and Tourism but later transferred to the Ministry of Finance for revisions (Carlos & Pablo, 2016, p. 10).

Additionally, this form of dispersed system requires a high degree of cross-agency information sharing to ensure the flow of information and the effectiveness of communication. However, Chile has no official programs for sharing cybersecurity assets within the public sector. Because of the number of agencies involved and the overlapping of jurisdictions, it does not seem that the information sharing among government agencies is sufficient. Nevertheless, in light of the forthcoming Cybersecurity Framework Act, establishing a singular regulatory body should significantly reduce the obscurities for jurisdictions.

## Regulatory Framework

In Chile, there is no single Cybersecurity Framework Act but a list of laws, supreme decrees, and presidential instructions (instructivo presidencial) function individually to regulate each sector. This is the result of the ad hoc nature of the cybersecurity policies, where the sector regulators only establish regulations within the sector on cybersecurity when they face prominent and serious cyberthreats. However, the Chilean government appeared to have recognized the ineffectiveness of their system and are transitioning to unitary systems for more effectiveness. As a result, it is currently in the process of creating a new Cybersecurity Framework Act, which aims at establishing a unitary system. This convoluted disparate regulatory system has inevitably created gaps and overlaps between each agency's jurisdiction, impeding the private businesses' ability to navigate.

## National Framework

Currently, Chile is on its way to enacting the new Cybersecurity Framework Act, which not only establishes a series of definitions and principles but also has a strong institutional focus on creating a unitary agency, the National Cybersecurity Agency, which will establish its duties and its basic institutional form under Article 8 (Carey & Mercado, 2022). Additionally, it envisions a division of the work of both the Technical Council of the National Cybersecurity Agency and the CSIRTs, which are organized by areas that could be sectoral constituted by sectoral overseers or regulators in their respective areas or could be related to the public sector such as national, government and defense CSIRTs (Carey & Mercado, 2022).

Two major laws, Law No. 19.223/1993 and Law No. 21.459/2022, broadly regulate the criminal behaviors and offenses related to information technology. Law No. 19.223/1993 established criminal offenses relating to information technology. Specifically, Law No. 19.223/1993 defined a sub-category in cybercrime, such as malicious destruction of an information processing system, hindrance of its operation, unduly seizing and using information, damages to data, and the dissemination of data contained in an information system. This law was repealed in June 2022 and replaced by Law No. 21.459/2022, which establishes rules on cybercrimes in adherence to the Budapest Convention regulations (Establishes Rules, 2022). Law No. 21.459/2022 is the current law that regulates the criminal behaviors related to cybersecurity and practices promulgated on June 9, 2022 (Establishes Rules, 2022). This law modernizes cyber-related criminal offenses and adapts Chilean legislation to the Budapest Convention (Aldoney et al., 2022). The law allows the prosecution of criminal offenses such as the attack on the integrity of a computer system, illegal access and disruption of computer systems, unlawful interception and interference with the non-public transmission of information in a computer system, computer forgery, and improper alteration and damage of computer data, and various forms of computer fraud. The enforcement of this law is entrusted to MISP through the National Prosecutor, which MISP has the power to initiate complaints about the crimes provided for in this law.

Chile currently has a national CSIRT that is organized in relation to the public sector. The Government and the Ministry of Defense have their own CSIRTs that play a vital part in the coordination of Chile's Army, Navy, Air Force, and other armed forces (Carey & Mercado, 2022). Currently, the private sector is integrated into the CSIRT's coverage if it belongs to strategic sectors or a public-private collaboration agreement has been established (Computer Security Incident Response Teams, 2021). All public institutions are required to report all cyber incidents that they detect in their networks, equipment and systems to CSIRT. There are three stages of report: the initial stage is a mandatory report that only contains the information known at the time, the interim report needs to update the information(this stage is also mandatory whether or not there are new developments), and the final report confirms all information and follows the template (CSIRT, 2021). The initial report should be completed within an hour of the incident and the time frames for other two stages vary by the hazard level defined by CSIRT (CSIRT, 2021). Under the proposed Cybersecurity Framework Act, it discusses the creation of sectoral CSIRTs, which will play a key role in reporting and managing cybersecurity incidents, including existing, known, or detected vulnerabilities, and suggesting action plans to address such cybersecurity gaps (Carey & Mercado, 2022). The Cybersecurity Framework Act also regulates that reportings of cyber incidents should be no later than one hour after verifying the existence of a cybersecurity incident when it has had a significant impact on the security of the

computer system of an institution with information infrastructure classified as critical or on the continuity of an essential service (Carey & Mercado, 2022).

## Sector Framework

Within the public sector, supreme Decree No. 533/2015 creates a Cybersecurity Inter-Ministerial Committee, and this decree is later amended in the Supreme Decree Nº 579/2019, which creates an Inter-Ministerial Committee responsible for inter-ministerial coordination. There is a list of decrees that regulate cybersecurity within the public sector. Supreme Decree No. 1299/2005 establishes rules regulating the State Connectivity Network, which is managed by MISP and sets the procedures, requirements, and technological standards for incorporating public institutions into the said network. Supreme Decrees No. 83/2005 approves technical standards for state administration bodies on the security and confidentiality of electronic documents. Supreme Decree No. 93/2006 approves technical standards for adopting measures to minimize the harmful effects of unsolicited massive electronic messages received in the electronic mailboxes of the State administration bodies and their officials. Supreme Decree No. 14/2014 modifies Decree No. 181/002, which approves the regulations of Law 19.799 on electronic documents, electronic signature, and the certification of said signature, and repeals the decrees indicated. Supreme Decree No. 1/2015 approves technical regulations on systems and websites of the State administration bodies (The Government, 2016; CSIRT, n.d.). Law No. 20.285/2008 is about the access to public information, particularly on the transparency of the public function and access to information of the State Administration (The Government, 2016; On Access, 2020). This piece of legislation creates a transparency scheme for the state's activities, with active transparency obligations, which must be carried out through the website of each relevant public body; and passive obligations, which consist in providing the data that any person may require from these bodies, provided that this does not affect other rights and interests set out in the law, such as the state's security and third party's privacy, so that the confidentiality of the relevant is not affected (The Government, 2016; On Access, 2020).

Furthermore, a series of laws and Supreme Decrees establish the legal framework of the regulations in cybersecurity, with each focusing on its respective sector. Several major sectoral laws and regulations include: Law 19.628/1999, "Personal Data Protection Law," which is the primary body of rules on the processing of personal data; Decree with the force of law N° 3/19.978, "General Law of Banks," and Law 20.575/2012 regulates the processing of personal data for financial, economic, banking or commercial information, Law 18.168/1982, the "General Telecommunications Law," regulates the telecommunication industry, Law 19.223/1993 regulates certain computer crimes, and Law 20.584/2012 regulates individual medical data.

In regards to personal data protection, Chile has two laws regulating this area, yet it has no special data protection authority for the enforcement of the abovementioned laws on personal data. Law No. 19.628/1999, commonly referred to as "Personal Data Protection Law (PDPL)," creates regulations for the protection of private life, which sets out a series of principles and rights relative to general application rules for the management of personal data by the public and private sectors (On Protection, 1999). The law also provides data subjects the right to access, process, delete, and of personal data, with the appropriate authorizations required to process personal data. For example, it is mandatory to have written authorizations for processing personal data to store personal data and possible communication to the public (The Government, 2016; On Access, 2020). Moreover, Law No. 20.575/2012 establishes the "purpose principle" for

the processing of personal data in the economic, financial, banking, or commercial areas, in which the communication of this kind of data may only be made to the established business, for the credit process, and to the entities that participate in the evaluation of commercial risk and for that sole purpose (The Government, 2016; Establishes the Principle, 2012). It also specifies that such data could not be required for other purposes, such as in the processes of personal selection, pre-school, school or higher education admission, emergency medical care, or application for public office. Additionally, the law delineates the right of data subjects to request access to their commercial information every four months and free of charge. In regards to the health industry, Law 20.584/2012 establishes that both information from the clinical record and from the studies and other documents where procedures and treatments to which people were subjected are recorded are considered sensitive data (Establishes the Principle, 2012). Thus, they follow the regulation of Law 19.628/1999, which states that sensitive data may not be subject to treatment except when the law authorizes it, and the consent of the owner of this data is required for the determination or granting of health benefits that correspond to their owners (On Protection, 1999).

For the banking and financial sector, Decree with Force of Law N° 3/19.978, also known as the "General Law of Banks," establishes the data protection and confidentiality of an individual's transactions with and through banks (Article 154) (Established Consolidated, 1997). The primary enforcement agency is the Financial Market Commission (FMC), which establishes that it is mandatory for banks to report all cyber incidents that occurred in the current month (Established Consolidated, 1997). The reporting requirement under this sector mandates banks to report all cyber incidents that have occurred in the current month (Magliona & Araya, 2022). Law N° 3/19.978 distinguishes transactions covered by secrecy, which are prohibited for any disclosure, and transactions covered by reserve, which could only be disclosed where a legitimate interest exists and there is no evidence that revealing such information would cause financial damage to the customer (Established Consolidated, 1997; The Government, 2016). Law No. 20.009/2005 regulates the loss, theft, or robbery of Credit and Debit Cards in electronic transactions that are issued and operated by entities subject to the control of the Commission for the Financial Market and the regulation of the Central Bank of Chile and those that are not operated by these entities (Establishes a Regime, 2020). The issuers of the payments are subjected to the regulation of this law, stating that "the issuers, operators, businesses and other establishments affiliated with a payment card system, as well as other entities that intervene or provide services associated with payments and electronic transactions must adopt the measures of security necessary to prevent the commission of the illicit acts (Article 6) (Establishes a Regime, 2020)." Law No. 19.913/2003 creates the financial analysis unit and modifies a series of provisions in the field of money laundering. This law creates the Financial Analysis Unit (UAF) to prevent and prevent the use of the financial system and other sectors of economic activity for the commission of any crimes (Creates the Financial, 2003).

Regarding the telecommunication sector, Law No. 18.168/1982, known as the "General Telecommunications Law," regulates the telecommunication industry, which provides key physical and logical infrastructure for national cybersecurity. It establishes that all the installation, operation, and exploitation of telecommunications services located in the national territory are governed by this law (General Telecommunications, 1982). Two recent modifications to this law are especially relevant for the country's cybersecurity: Law No. 20.478/2010 and Law No. 20.453/2010. The former law regulates the public telecommunication system and business recovery and continuity when the public telecommunications system is

affected by critical and emergency situations, allowing the maintenance and continuity of the country's telecommunications and the availability of information contained in cyberspace (On Recovery, 2010). Law No. 20.453/2010 ensures the principle of network neutrality for internet consumers and users, regulating network management measures that may be adopted by internet service providers and ensuring confidentiality (Principle of network, 2010; The Government, 2016). Law 20.478, Article 7 sets requirements for the telecommunication industry; in disaster situations, concessionaires (concesionarios) of public and intermediate telecommunications services are mandatory to provide the Undersecretariat with information on significant failures in their telecommunications systems that may affect their regular operation (On Recovery, 2010). Additionally, resolution No. 1318 establishes a mandatory duty to report cyberthreats in the context of telecommunication services for companies that provide such services (Approves Technical, 2020).

Presidential Instruction No.8/2018 establishes a technological infrastructure of state administrative bodies: the Coordination Center of Government Entities (CCEG), which is responsible for verifying compliance with current cybersecurity standards (Magliona & Araya, 2022). It requires a compulsory report of incidents in the state administration bodies to the CCEG, as soon as they become aware of them, in which the Ministry of the Interior, through the CCEG, arranges the necessary actions to ensure the continuity and proper maintenance and functioning of the networks (Silva, 2018). For other sectors, there are individual regulations on the reporting process. For example, the updated Supreme Decree No. 5.996 and Supreme Decree No. 1.299, in line with the amendments to Supreme Decree No. 83, altogether set out the obligation to report incidents by public bodies (Magliona & Araya, 2022).

## Summarization and Evaluation

Overall, the effectiveness of enforcing cybersecurity regulation is relatively sufficient in certain critical sectors but to a less degree in others. Because of such dispersed regulations and the absence of centralized agency, many entities have jurisdiction yet lack authority for enforcement. For example, because Chile currently has no special data protection authority, the enforcement of cybersecurity-related offenses such as data protection violations in the Law No. 19.628 must be challenged with a "Constitutional Protective Action" based on the possible violation of the constitutionally guaranteed right to protection of personal data, or challenged with an action before the ordinary civil courts (On Protection, 1999; Magliona & Araya, 2022). However, as the Pro-Consumer Law came into force and created the consumer protection agency SERNAC, consumers now are able to make complaints alleging the violation of the data protection law to this authority (Consumers International, 2022; Magliona & Araya, 2022). Although the SERNAC does not possess the legal authority to impose fines, it has the ability to initiate and participate in judicial proceedings and collective voluntary proceedings to enforce data protection legislation (Magliona & Araya, 2022). On the other hand, because Chile relies on sectoral regulations, it does not have a strict enforcement mechanism requiring mandatory reporting from digital service providers and operators of cyber security incidents, this mandatory reporting largely varies by sector.

# Relationships

Chile has been an active participant in the international cooperation on cybersecurity insofar that it took the initiative to change its current policies in adherence to international standards. Domestically, the government has formed extensive partnerships with the private sector and encouraged the participation of the private sector in the cybersecurity legislation process through established lobbying channels, albeit this public consultation is only accessible to big corporations.

## International Cooperation

Internationally, Chile is involved and committed to international cybersecurity agreements taking a multistakeholder approach to international cybersecurity. It acceded to the protocol of accession to the Budapest Convention of the Council of Europe in 2017. In 2010, Chile became a member of the Organization for Economic Co-operation and Development (OECD) countries, committing to adapt data protection regulations and regularizing the cross-border data flow. Chile modified its laws based on the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') standards and created a data protection agency.

Chile was officially invited by the Council of Europe to accede to the protocol of accession to the Budapest Convention in 2009, and in 2017 the government deposited the instrument of accession to the treaty through Decree No. 83/2017 (Convention on Cybercrime, 2022; Enacts the Convention, 2017). The MINREL claims that Chile is committed to adhering to the international standards on cybercrime through the measures of its national cybersecurity policy (Ministry of Foreign Affairs, 2017). As a result, it replaced the previous law with Law No. 21.459/2022 in order to comply with the regulations of the Budapest Convention. For example, Law No. 21.016/2017 legalizes information sharing with other countries, including the exchange of personal data, but specifies that this delivery of information will not imply the transfer of national databases or access directly to them by another state (Rodriguez-Ferrand, 2017; Facilitates the Reciprocal, 2017).

In terms of the intra-state corporation, Chile is also regularly represented in other international cooperation forums dedicated to international cybersecurity. For instance, Chile is an active member of the Forum of Incident Response and Security Teams (FIRST), which aims for strong global coordination and a more conducive environment for all relevant stakeholders. Regionally, Chile participates in the Organization of American States (OAS), mainly through the CSIRT Americas Network, a cybersecurity program under the Inter-American Committee against Terrorism (CICTE) of OAS. Through this robust international engagement, Chile strengthens its CSIRTs capacities and enhances Chile’s response to cyber incidents. Additionally, Chile is a part of the G8 24x7 Contact Network, which is designed for intra-state information exchange on cross-border criminal investigations (Velasco, 2016). However, it is necessary to acknowledge that due to the level of cybersecurity system development in Chile, it primarily does not play a leading role in international conversations. For this reason, Chile is not currently hosting any international cybersecurity organizations.

## Private Sector

Domestically, public-private partnerships (PPPs) are a crucial component of Chile's cybersecurity policy, especially in major areas of cybersecurity agendas, as private companies

are encouraged by the government also to provide incident management-related services. The Chilean government has a record of PPPs in cyber-related areas. For example, in 2015, the Chilean government joined Microsoft's Government Security Program to reduce potential vulnerabilities in information systems and develop services and "GSP for Cloud" capability using Microsoft products (Bnamericas, 2015). Recently, in 2020, 16 organizations formalized the cybersecurity collaboration agreement with the Ministry of Interior and Public Security, including major corporations such as Sercor, Deloitte, CenturyLink, and IBM. The primary collaboration area focuses on the voluntary exchange of technical information, practical training, beneficial practices, and the development of cybersecurity activities. One aim is voluntary information sharing in computer security threats and incidents, prevention of cyber risks, and technological innovations in the field of cybersecurity to minimize the impact of cyberthreat on critical infrastructures and essential services (Cybersecurity in Chile, 2020). MIPS and IBM also had "signed a collaboration agreement to enable the Chilean government to use IBM X-Force threat information through the free IBM X-Force Exchange platform." Recently, the government collaborated with multiple private businesses to streamline cybercrime and electronic evidence in the national training strategies for judges and prosecutors through the Joint Project GLACY+ (GLACY+: Chile, 2020).

With regards to the private sector's participation in policymaking, Law No. 20.500/2011 establishes citizen participation in public management. Article 70 states that the mandatory establishment of formal and specific modalities of participation for individuals and organizations within the framework, and Article 74 details that each body of the State Administration must establish advisory civil society councils, which should be made up of a diverse, representative and pluralistic manner by members of non-profit associations that are related to the competence of the respective body (On Associations, 2011). The enactment of Law No. 20.500/2011 prior to the creation of the new Cybersecurity Framework Act led to an increase in civil society councils on cyber-related issues, with 31 civil society councils active through 2016, and 20% of these councils' members related to a business association (Carlos & Pablo, 2016, p. 11). Additionally, during the formation of national cybersecurity policies like Digital Agenda 2020 and later the Cybersecurity Framework Act, the public consultation was open to the private sector, albeit with high barriers to entry. Many stakeholders in the private sector had submitted their comments and inputs on the drafts for the first National Cybersecurity Policy, which the Interministerial Cybersecurity Committee reviewed (Carlos & Pablo, 2016, p. 13). The Chilean mining association Sonami and the country's mining council actively participated in the forming of a cybersecurity plan in the mining industry (Bnamericas, 2020). Because Chile is the world's top copper producer, it needs to create a sectoral cybersecurity policy for early warning and response to the attacks. In 2021, the mining ministry arranged PPPs with many private companies such as the London-based Anglo American, Australia's BHP, Vancouver-based Teck, Chile's Antofagasta Minerals, and copper miner Collahuasi in creating a cybersecurity plan for the mining industry (Bnamericas, 2021).

## Summarization and Evaluation

Chile is involved in robust intra-state cooperation efforts with nations across the world to facilitate the sharing of cybersecurity information and assets. Although its current state renders it unable to host any international cybersecurity organization, it is an active participant in international collaborations such as the Budapest Convention, FIRST, and OAS. Furthermore, the Chilean government places a key role on public-private partnerships in the areas of

cybersecurity, signing many agreements with industry leaders for voluntary information sharing. These collaborations, both internationally and domestically, have been proven effective. On the other hand, even though there are communicable channels for the private sector to weigh in the legislation process, the results are mixed. Some industries have more success, as the mining industry attests, and others do not. For example, in developing Digital Agenda 2020, the process through which dozens of private entities and groups participated was not shared outside the Ministry of Economy before its publication. Therefore, although communication avenues exist for the private sector to participate in the legislative process, the effectiveness of their lobbying efforts is unknown.

## Overall Effectiveness

In general, Chile has relatively robust mechanisms for cybersecurity, as indicated by its NCSI index score of 59.41. Cybersecurity has been one of the top priorities for each administration, and the country has established clear legislation against cybercrimes, especially for military cyber operations. Although Chile might seem to have a relatively complete regulatory system on cybersecurity, the normative bodies concerned with this matter have been somewhat too complicated for day-to-day operations and sometimes obsolete, leaving many laws and regulations unused.

Chilean regulations on cybersecurity are reactive, because it does not establish laws until concerns over the certain cybersecurity issues in a sector become urgent and prevalent. In essence, Chile’s regulations are ad hoc in nature, resulting in the disparate system that our research observed. The currently dispersed cybersecurity system presents an impediment to the effectiveness of cybersecurity policies. Since many ministries do not have a straightforward assignment, the jurisdiction of each agency does not align perfectly, leaving gaps in personal data protection and creating overlaps between authorities in public cybersecurity awareness campaigns. Although exact information on inter-ministerial collaboration is limited, the confusions among agencies indicate that there does not seem to have clear pathways for cross-government agencies' information sharing on vulnerability information and crisis management. Nevertheless, there are avenues for private businesses to communicate with legislation and to comment on draft cybersecurity policies. Common communication channels include civil society councils and participation in sector-specific legislation processes through public consultations.

With the current dispersed cybersecurity system and the lack of national cybersecurity strategies, it creates a risk-based and technology neutral, where the lack of institutional stability inadvertently allows more flexibility for the cybersecurity policies in Chile to evolve with changing threat landscape and to accommodate new and changing technologies, albeit in a less effective way in terms of implementation and enforcement. It is also necessary to note that the principal agency responsible for coordination on cybersecurity regulation, the Interministerial Committee, is transitory. Although the establishment of a unitary agency is forthcoming, it is expected that Chile's cybersecurity regulatory landscape will remain discursive, requiring additional efforts from the private businesses to navigate through all the structural inconsistencies. Furthermore, the domestic political uncertainties might change Chilean cybersecurity regulatory landscape. On July 8, 2022, Chile proposed a new constitution replacing the one passed under Pinochet’s dictatorship (Osborn, 2022). The old constitution provided a favorable environment for private business, allowing the private sector to participate in policy formation. With the new constitution in place, it envisions a stronger government role, which

might alter the private sector's lobbying pathway underwritten in the past constitution and laws (Osborn, 2022). Nevertheless, it is anticipated that the cybersecurity regulatory landscape will be dominated by the transitional agency the Interministerial Committee, with an aim to reorganize the structure towards a more unitary approach.

# France

France has a unitary cybersecurity governance model with an effective cybersecurity governance system in place, based on its established national cybersecurity framework and robust international cooperation. The French cybersecurity landscape is based on cooperation with the European Union (EU) and the North Atlantic Treaty Organization (NATO) as well as the protection of critical infrastructure. France has high development of public-private partnerships, as demonstrated by the presence of the critical infrastructures information protection (CIIP) regulatory framework and the ability of the private sector and other stakeholders to influence legislation. France demonstrates the effectiveness of unitary governance models and public-private partnerships. Table 10: Findings on France's Cybersecurity Framework summarizes findings on France's cybersecurity framework.

Table 10: Findings on France's Cybersecurity Framework

| **Overall Cybersecurity Assessment** | |
|---|---|
| Overall system effectiveness | Effective |
| System style | Unitary |
| National strategy and framework | Established |
| NCSI index rating | 84.42 |
| **Legal Framework and Its Effectiveness** | |
| Is the framework parsimonious? | Yes |
| Is jurisdiction clear? | Yes |
| Are there gaps in the framework? | Yes |
| Is regulation: outcome focused, technology neutral, risk-based? | Outcome focused, technology neutral |
| **Regulation and Enforcement** | |
| Are regulation/enforcement sector-specific? | Somewhat |
| Is there an enforcement agency? | Yes |
| **Relationships** | |
| Are there international relationships? | Yes |
| Can the private sector weigh in? | Yes |
| What characterizes information sharing? | Sufficient |

## Country Background

France, officially the French Republic, is a democracy with a gross domestic product (GDP) of 2937.47 billion US dollars in 2021, ranked 7th in 2021world GDP and (World Bank, 2022). In 2013 and 2014, the French government launched €150 million ($153.11 million) investments in cybersecurity research and development (R&D) to boost national digital security (Calcara and Marchetti, 2021). By 2021, the French government has attributed €1 billion ($1.02 billion) of investment to accelerate the development of cybersecurity in the country and increase protection levels for public institutions (Hentzen, 2021).

France earned a score of 84.42 out of 100 on the national cybersecurity index (NCSI) in which France ranked 11th globally. The NCSI Index considers these following categories in determining their scores: cybersecurity policy development, cyberthreat analysis and information, education and professional development, contribution to global cybersecurity, protection of digital services, protection of essential services, E-identification and trust services, protection of personal data, cyber incidents response, cyber crisis management, fight against cybercrime, and military cyber operations. We adopt this score for a measure of how prepared countries are in preventing cyberthreats and managing cyber incidents.

In a 2008 White Paper on Defense and National Security, President Nicolas Sarkozy underscored the risk of cyberattacks on national infrastructures for the first time (Baumard, 2017). Based on the 2008 White Paper, the French National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information, ANSSI) was created as a national cybersecurity authority to coordinate the responsibilities of different cybersecurity bodies. France is highly engaged in international cooperation regarding the security of information systems, committing to the European Union (EU) and the North Atlantic Treaty Organization (NATO). France also features vigorous public-private partnerships in the field of critical infrastructures information protection (CIIP), making it worthwhile to conduct a case study on the French cybersecurity strategy and structure.

## Cybersecurity Agencies

France has a unitary cybersecurity regulatory system, as there is a unique national authority for cyber defense and network and information security (NIS): National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information, ANSSI). Nevertheless, cybersecurity responsibilities are shared among various actors. While ANSSI coordinates the work of different agencies and organizes standards for critical infrastructures, the Ministry of Interior prevents and investigates cybercrime, and the Ministry of Armed Forces performs cyberdefense activities. On the strategic side, the Cybersecurity Group of the High Council for Strategic Education and Research conducts research. The National Commission on Informatics and Liberty independently protects personal data.

The General Secretary for Defense and National Security (Secrétariat général de la défense et de la sécurité nationale, SGDSN) is the host of ANSSI. Placed at the heart of the executive, the SGDSN assists the Prime Minister in fulfilling his responsibilities in terms of national defense and security (ANSSI, n.d.). Its scope of intervention covers all strategic defense and security issues in the field of military programming, deterrence policy, and internal security, including national security, economic and energy security, crisis response planning, and the fight against terrorism (SGDSN, n.d.). The SGDSN has three main missions: to monitor and warn of

threats and risks, to advise and draft decisions of defense and national security taken by the executive, and to act as an operator through the classified inter-ministerial information systems operator (OSIIC). The ANSSI, which reports to SGDSN, is responsible for the last mission (SGDSN, n.d.).

The ANSSI is the sole cybersecurity authority in France. ANSSI was created by Decree No. 2009-834 on July 7, 2009 (Official Journal of 8 July 2009). By imparting its expertise and assisting government departments and operators of vital importance, ANSSI acts as an inter-ministerial organization in charge of coordinating the national effort regarding the security of information systems (ANSSI, n.d.; Décret n° 2009-834, 2009). ANSSI hosts the Operational Center for Information Systems Security (Centre opérationnel de la sécurité des systèmes d'information, COSSI), responsible for the detection and mitigation of cyberattacks directed at French Government information systems. Within COSSI, CERT-FR provides incident management support to ministries, institutions, jurisdictions, independent authorities, local authorities and OIV (operators of vital importance) to assist government agencies to implement the necessary protection measures and respond to incidents or computer attacks (CERT-FR, n.d.).

The Ministry of the Interior (Ministère de l'Intérieur) administers the territory and guarantees the security of citizens and property. Its missions include fighting against all forms of cybercrime targeting institutions, national interests, economic actors, public authorities, as well as individuals. The Ministry hosts the General Directorate of Internal Security (Direction Générale de la Sécurité Intérieure, DGSI). DGSI closely partners ANSSI to combine their dual expertise in intelligence and high technology, anticipating and attempting to thwart cyberattacks alongside the targeted companies and institutions (Ministry of the Interior, n.d.). In the cybersecurity regulatory framework, the Ministry of the Interior serves to prevent cybercrime.

The Ministry of Armed Forces (Ministère des Armées) takes the responsibility to combat cyberattacks and cybercrime. The role of the Ministry of Armed Forces is to ensure the protection of French territory, population, and interests. It also carries out other missions within the framework of international (NATO) or regional (European defense) agreements and treaties (Ministry of Armed Forces, n.d.). Within the Ministry, the Analysis Center for Cyber Defensive Operations (Centre d'analyse en lutte informatique défensive, CALID) provides detection, analysis, and response to cyberattack (Brangetto, 2015). Since 2013, CALID and COSSI have been co-located to enhance information sharing and coordination between the two bodies (ANSSI, n.d.).

Cybersecurity Group of the High Council for Strategic Education and Research (Conseil supérieur de la formation et de la recherche stratégiques, CSFRS) is a national security strategic council and a public interest group that supports strategic research and training and organizes colloquia and conferences on strategic research (République Française, 2014). Created in November 2009 by the President of the Republic, the council aims at gathering a broad range of expertise — civilian and military, industrial and governmental, scientific and academic — to conduct a "strategizing" function for France Prime Minister (Geostrategia, n.d.; Baumard, 2017). To be more specific, the CSFRS is essentially the tool designed and utilized by the private sector to admonish the government to impose policies that are favorable to the dominant private enterprises in the cybersecurity market. The CSFRS bridges between the major private companies and the ministries and communicates the needs of the private sector to the government. In November 2019, the CSFRS was dissolved by decree of the Prime Minister, who then entrusted the Security Defense Research Team - Intelligence, Criminology, Crises,

Cyberthreats (Équipe de recherche Sécurité Défense – Renseignement, Criminologie, Crises, Cybermenaces, ESD-R3C) to take over and accomplish the same missions (Geostrategia, n.d.).

The National Commission on Informatics and Liberty (Commission nationale de l'informatique et des libertés, CNIL) is an independent administrative regulatory body (autorité administrative indépendante, AAI) to ensure the application of data protection laws and the collection, storage, and use of personal data. The CNIL was created by the French Data Protection Act of 6 January 1978 (Loi Informatique et Libertés N°78-17, FDPA) as an enforcement agency of the FDPA to ensure the protection of public and private data privacy, public and individual freedoms, and human rights (CNIL, n.d.). Without being placed under the authority of the government or any ministry, the commission acts on behalf of the state (CNIL, n.d.).

### Summarization and Evaluation

Compared to other countries, French cybersecurity governance is based on a high degree of institutional centralization, as ANSSI is the sole cybersecurity authority and the coordinator (Calcara and Marchetti, 2021, p.9). However, the cybersecurity responsibilities are shared among various actors. ANSSI is responsible for assisting the state's institutions on cybersecurity and for organizing standards of industries and critical infrastructure; the Minister of Interior is responsible for anticipating, forestalling, and investigating cybercrime and cyberterrorism; the Ministry of Defense is responsible for conducting cyber-defense activities; the CSFRS gathers a broad range of expertise for research; and CNIL independently enforces personal data protection (Calcara and Marchetti, 2021). The jurisdiction over cybersecurity policy is clear, and the assignment of responsibilities to each ministry and public body is also coherent. Overall, the unitary cybersecurity system in France is rather effective.

The plentitude of cybersecurity actors and the decentralization of cybersecurity responsibilities inevitably engender overlapping between different agencies. For instance, the CALID in the Minister of Armed Forces and the CERT-FR in the COSSI both engage in incident response. Nonetheless, the close cooperation between the CALID and the COSSI is in fact salutary for the system, as the two organizations reinforce and supplement each other. In this way, the structure of a unique authority and shared responsibilities empowers France in the field of cybersecurity.

We do not detect major gaps in France's well-organized jurisdictional hierarchy. However, there is an absence of an agency for international coordination. The lack of a centralized point to interact with the international community is adverse for France, a country actively participating in international cooperation.

## Regulatory Framework

To enforce the national cybersecurity regulatory framework, there are two main laws and three national strategy documents in France. The two laws, for data protection and critical infrastructure protection, respectively, integrated France more into the EU cybersecurity framework, and each of the three national strategy documents further polished the French cybersecurity system. To enforce the two laws, France has established an enforcement framework equipped with enforcement agencies and rigorous penalties. In the regulatory

framework, sectors regulate themselves to compose national regulations and are subject to national regulations.

The regulatory framework begins from the prevention of intended cybercrime and incorporates both mandatory and voluntary information sharing mechanisms. According to Article 57 of the FDPA, data controllers, the entity that determines why to and how to process data, and data processors, the entity that performs the data processing on the controllers' behalf, should take all necessary precautions regarding all risks to preserve the security of the data and to prevent it from "being distorted, damaged, or accessed by unauthorized third parties" (EU GDPR, 2016; Lecomte, 2021). Within the NIS Directive and the CIIP framework, operators of vital importance and trust service providers are required to carry out and maintain a list of networks and information systems necessary for the provision of the services, identify the risks threatening the security of the information systems, guarantee an appropriate level of security by implementing technical and organizational measures necessary and proportionate to prevent, manage, and reduce the risks, avoid incidents and minimize their impact, and identify the information technology (IT) security risks that may affect their activities (Lecomte, 2021). The DGSI in the Ministry of Interior also takes actions to anticipate and prevent cyberattacks.

## National Framework: Cybersecurity Legislation

Today, the two main pieces of legislation in the French cybersecurity governance are the General Data Protection Regulation (GDPR) and the Network and Information System Security Directive (NIS Directive). GDPR focuses on data protection, while NIS Directive concentrates on critical infrastructures. Both laws derive from the EU cybersecurity framework, as France aims to enhance the cybersecurity cooperation networks in the region.

Since January 6, 1978, the French Data Protection Act (Loi Informatique et Libertés N°78-17, FDPA) on information technology, data files, and civil liberties has been in force. On May 25, 2018, the European Union General Data Protection Regulation (GDPR), a single cybersecurity legal framework across the EU, took effect and applied directly in every EU member state. Rather than repealing or replacing the FDPA, France enacted Law n°2018-493 of June 20, 2018 (French GDPR Law) to modify it. The French GDPR Law extended the FDPA, aligned French data protection with the EU, and provided for specific rules on certain topics.

The publication of the European Cybersecurity Strategy First proposal of the Network and Information System Security Directive (NIS Directive) was in February 2013. After three years of negotiations, the Council of the European Union and the European Parliament adopted the NIS Directive on July 6, 2016. As the first European legislation dedicated to cybersecurity, the NIS Directive aims at strengthening national cybersecurity capabilities, establishing a framework for cooperation among EU Member States, and strengthening the cybersecurity of "operators of essential services" and "digital service providers" (ANSSI, n.d.). On February 15, 2018, the French Parliament voted in favor of the legislation proposal of the transposition of the NIS directive into France's national law. On May 22, 2018, Décret n° 2018-384 du 23 mai 2018 was published to pursue the implementation of the French law. ANSSI transposed the NIS Directive to the French framework of the implementation of the CIIP law.

In addition to these two regulations, there are also the law on daily security (LSQ n°2001-1062), the law on internal security (n°2003-239), the law strengthening the provisions on the fight against terrorism (n°2014-1353), and the law strengthening the fight against organized crime and terrorism (n°2016-731) (Lecomte, 2021). These decrees together form France's cybersecurity legislative framework.

## National Framework: Strategies

In 2008, 2013, and 2015, the French government published three national strategies, and each of them was a turning point in terms of French cyberdefense. In the 2008 White Paper, cyberattacks were, for the first time, introduced as a component of the French national defense and security policy; in the 2013 White Paper, the CIIP law was established; and in the 2015 national digital security strategy, the government strongly supports the digitalization of French society and promote digitalization in Europe.

The 2008 White Paper on Defense and National Security marked an important turning point in the French history of cybersecurity. This informational document highlighted the potentially enormous threats of cyberattacks and identified cybersecurity as an integral component of the French national defense and security policy for the first time (Baumard, 2017). Specifically, in the field of cyber defense, it stressed the need for an early detection capability for cyberattacks, and for an organization to counter attacks ranging from the most subtle to the most far-reaching. In the field of prevention, it advocated greater use of high-security products and networks, and the establishment of a pool of skills serving government departments and operators of vital importance. ANSSI was created in line with the proposals of this White Paper on Defense and National Security (ANSSI, n.d.).

According to ANSSI, the 2013 White Paper on Defense and National Security was in response to the increasing number and sophistication of cyberattacks against the network and information systems of numerous French businesses and public sector enterprises (ANSSI, n.d.). This is another turning point in terms of French cybersecurity regulations: the state provided not only its own cybersecurity requirements, but also for operators of vital importance, defined as "operator[s] whose unavailability could strongly threaten the economic or military potential, the security or the resilience of the Nation" (ANSSI, n.d.).

Following the guidelines set by the 2013 White Paper on Defense and National Security, the Critical Infrastructures Information Protection (CIIP) law was established as a dedicated CIIP regulatory framework in December 2013. The law applies to more than 200 public and private operators (called "operators of vital importance") from 12 sectors defined in France's framework for the security of activities of vital importance established in 1998 (ANSSI, n.d.). In addition, as ANSSI was incapable to handle all CIIP challenges alone, ANSSI established an evaluation process to qualify private cybersecurity trust service providers and products.

The Military Programming Law (LOI n° 2013-1168 du 18 décembre 2013), adopted on December 19, 2013, furthered the 2013 White Paper on Defense and National Security. According to ANSSI, "this legislative mechanism enabled national public and private sector operators of vital importance to better protect themselves and ANSSI" from cyberattacks (ANSSI, n.d.).

On October 16, 2015, French Prime Minister Manuel Valls announced the French national digital security strategy to support the digitalization of French society. The development of cyberspace brings in innovation and growth, but it also exposes the state, economic stakeholders, and citizens to greater cyberthreats (ANSSI, n.d.). To deal with the emerging risks in the digital age, France proclaimed the 2015 digital strategy to strengthen the security of information systems and critical infrastructures, emphasized privacy and awareness raising, fostered the environment of digital technology businesses. This digital security strategy also placed France "as a leader in promoting a road map for European digital strategic autonomy", underlying France's commitment to promote the EU cybersecurity sovereignty in the 2022 French presidency of the European Union (ANSSI, n.d.).

## Enforcement Mechanisms

To ensure the effectiveness of the cybersecurity framework and to underscore the authority of laws, France has established a relevant enforcement and penalty environment. The ANSSI takes the responsibility for the enforcement of the critical infrastructure information protection framework set by the NIS Directive. While ANSSI itself cannot perform sanctions, it can udit information systems as a trust provider, investigate information systems of operators of vital importance (OVI) and bring the violations of applicable cybersecurity requirements to the attention of the judicial authorities (Navarro et al., 2022). Executives of operators of essential services (OES), stakeholders who provide an essential service whose interruption would have a significant impact on the functioning of the economy or the society, can be sanctioned by a fine of €100,000 ($100,376.40) for failing to comply with the security measures specific to them, €75,000 ($75,282.30) for failing to comply with the obligation to report an incident, and €125,000 ($125,470.50) for obstructing the inspection operations (Navarro et al., 2022). Electronic communications operators, their agents, or operators of vital importance (OVI) can be sanctioned by a fine of €150,000 ($150,564.60) for obstructing the implementation of the technical markers for the detection of events likely to affect the security of information systems (Navarro et al., 2022).

The CNIL, equipped with sanction abilities, is responsible for the enforcement of the data protection framework set by the FDPA and the GDPR. Infringements of the provisions in the two legal documents with respect to cybersecurity are subject to administrative fines up to €10 million ($10.04 million) or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Navarro et al., 2022). Besides, in Article 323-1 of the French Penal Code (Code Pénal, 1992), fraudulent access to or fraudulent remaining in all or part of an automated data processing system is punishable by two years' imprisonment and a fine of €60,000 ($60247.80); where this results in the deletion or modification of data contained in the system or in the alteration of the functioning of the system, the penalty is three years' imprisonment and a fine of €100,000 ($100,376.40); and when it involved the national public system, the punishment increases to five years' imprisonment and a fine of €150,000 ($150,564.60) (French Penal Code, 1992). In Article 323-2, obstructing or distorting the operation of an automated data processing system is punishable by five years' imprisonment and a fine of €150,000 ($150,564.60), increasing to seven years' imprisonment and a fine of €300,000 ($301170.00) (French Penal Code, 1992).

## Sector Framework

In the French cybersecurity framework, national regulations and sectoral regulations of critical sectors support one another. The 2013 CIIP law adopted more than 200 operators in 12 critical sectors named by the national authority ANSSI, including Food, Health, Water, Telecom & Broadcasting, Space & Research, Industry, Energy, Transport, Finance, Civilian Administration, Military Activities, and Justice (ANSSI, n.d.). The law set a common minimum level of cybersecurity for critical operators in the 12 sectors, required the appointment of a representative in each sector to be the point of contact of the ANSSI, and reinforced the ANSSI to assist the sectors in event of cyberattacks (ANSSI, n.d.; Lecomte, 2021).

There are also some individual cybersecurity requirements for specific critical sectors. For example, healthcare institutions, bodies, and services carrying out prevention, diagnosis, or care activities, pursuant to article 1111-8-2 of the French Public Health Code, “shall report

without delay serious information system security incidents to the regional health agency" (Lecomte, 2021). The financial services sector must comply with requirements including auditing IT systems, strengthening resistance to cyber risks, developing defenses adapted to the complexity of cyberattacks, and reporting to the ANSSI by ministerial orders of November 28, 2016 (Lecomte, 2021). Also, the Financial and Monetary Code stipulates cooperation between ANSSI and the Financial Markets (Authority Autorité des marchés financiers, AMF), the stock market regulator in France, to provide each other with information relevant to the performance of their respective missions in the area of information systems security (Navarro et al., 2022). Another example is in the telecommunication sector. According to article L.33-1 of the French Post and Electronic Communications Code, telecom enterprises must comply with rules and regulations regarding "the conditions of permanence, quality, availability, security, and integrity of the network and service", including the obligation to notify data breaches to the competent authorities (Lecomte, 2021). Public and private firms in the 12 critical sectors may join the working groups voluntarily to work with different sectors for tailored security rules and cross-sectoral security rules. However, for the sectors not listed as critical sectors by ANSSI, there is a lack of specific sectoral regulations.

## Information Sharing

To ensure the availability of intelligence and the security of the information system, France has set clear requirements regarding information sharing. In France's cybersecurity framework, information sharing is mandatory in some cases, but to protect the privacy and integrity of different sectors, some information sharing is anonymous or voluntary.

For public and private data, Article 33 of the GDPR requires all data controllers to notify any incidents to the data competent controlling body, the CNIL. The notification must contain a description of the incident and its potential consequences, an indication of the category of the affected data, the concerned data subjects, a detailed description of the measures taken to remedy or to mitigate negative effects, as well as the name and contact details of the data protection officer (Lecomte, 2021). Article 58 of the FDPA and Article 34 of the GDPR provide an obligation for data controllers to inform each affected individual of the incident if the breach may be a risk to their rights and freedoms (Lecomte, 2021).

For critical infrastructure data, Article 22 of the Military Programming Law makes it mandatory for victim critical operators to send a form to report the incidents on their systems to ANSSI. ANSSI should share anonymized information on the incident with other critical operators to prevent potential attacks and incident information with sectoral ministers; in turn, sector ministers share incident feedback with ANSSI. Victim critical operators and other critical operators may exchange information voluntarily.

## Summarization and Evaluation

Overall, France's cybersecurity regulatory system is clear and effective. The two main regulations in France's cybersecurity framework, the GDPR and the NIS Directive, both follow the EU cybersecurity guidance. The GDPR amended the FDPA to secure data privacy and data protection, and the NIS Directive has been fit into France's CIIP framework. The French cybersecurity structure is, thus, intertwined with the EU one to enhance the cybersecurity capacities of the region.

The three national strategy documents have guided the development of France's cybersecurity framework. The 2008 White Paper on Defense and National Security listed cyberattacks as major threats and called to develop cyber-defense capacities; the 2013 White Paper on Defense and National Security provided guidance for sector regulations of operators of vital importance and established the CIIP framework; the 2015 French national digital security strategy further supported the digital transition of French society and promoted its position in the EU digital strategy. France continues to renew the national cybersecurity strategies to adapt to the new threats and new needs.

A mature system of enforcement mechanisms has been established in France's cyberspace. With the ANSSI enforcing critical infrastructure protection and the CNIL enforcing public and private data protection, specific penalties apply to various forms of violation. The relatively exhaustive enforcement mechanisms effectively ensure the operation of the cybersecurity framework.

While the 12 critical sectors in France are responsible for their own incident regulations, they report to the ANSSI and seek help from the ANSSI. Also, they are subject to their corresponding sectoral regulations set by the nation. The sectors may cooperate with the working groups to establish custom-made security rules and cross-sectoral security rules. Other than the 12 critical sectors, there is a potential oversight of noncritical sectors.

The regulations in the French cybersecurity framework starts from intent cyberattacks with detection and prevention mechanisms, rather than already committed cybercrimes. Such boosts French cybersecurity by adding one more layer of protection to the system.

France also has a clear structure of information sharing. Data controllers are supposed to report to CNIL, and victim critical operators are supposed to report to ANSSI of incidents. Such mandatory mechanisms ensure the promptness of incident report and information sharing, facilitating the security of digital products and services. The anonymity information sharing between ANSSI and other critical operators also ensures the data confidentiality of the victim critical operators. Nevertheless, such an information sharing mechanism is only obligatory when the incident poses major risks to other data controllers and operators, and the definition for the risk level remains obscure.

# Relationships

France interacts with international actors and actively participates in international cooperation in terms of cybersecurity, taking a multistakeholder approach to international cooperation. France's most vital partners are the EU and NATO. However, the private sector constitutes a crucial part of the French cybersecurity framework as well. The private companies' robust lobbying influence on the government's decision and salient presence in the CIIP framework, the working groups, and the cybersecurity industry and market underlie a close public-private partnership.

## International Cooperation

France' collaborations with the European Union (EU) and the North Atlantic Treaty Organization (NATO) have different focuses. When it comes to economic and industrial cybersecurity standards, Paris prefers to discuss cybersecurity within the European context and

to promote a European approach to cybersecurity industry issues (Terpan & Saurugger, 2021). When it comes to military and intelligence cyber defense, France cooperates with NATO.

France aligns closely with the EU in terms of the development of cybersecurity capacities. French cybersecurity legislation has been strongly influenced by the EU agenda. As introduced above, both the GDPR and the NIS Directive adapt to the EU regulations. According to the press release on September 8, 2021, ANSSI defends the future of a common and shared cybersecurity framework in Europe based on cooperation and solidarity. To be more specific, France acts as the coordinator of the European Secure Software Defined Radio (ESSOR) that aims to develop common cybersecurity technologies for European military radios; French cybersecurity companies are engaged in the Integrated Unmanned Ground System (UGS) to develop cyber secure autonomous navigation capability for route and mission planning; some French companies receive considerable funding from the European Investment Bank (EIB) that promotes innovation and supports innovative companies (Calcara and Marchetti, 2021). However, there are also circumstances in which the interests of the EU contradict those of the France nation. For instance, in the Cybersecurity Act, the EU pushed the member states to adopt an EU-based cybersecurity certification process without specific criteria to define security levels. The French government worried about the possibility of foreign cybersecurity penetration and the threats to French national industrial autonomy.

The 2013 White Paper on Defense and National Security clarifies that "NATO and the European Union are not in competition; the two organizations are complementary". In the field of military and intelligence, France closely aligns with NATO, and one major initiative is the CIS3 C&I Partnership. The Communication and Information Systems Security Standards (CIS3) Communications and Information (C&I) Partnership (CIS3 Partnership) is a Smart Defense Initiative that focuses on the development and maintenance of security standards for interoperability in the area of Consultation, Command and Control (C3) (NCI Agency, n.d.). It is one of NATO's multinational projects and partnerships. The project embarked on October 24, 2016, with participation of 12 nations: Canada, Czech Republic, France, Germany, Italy, The Netherlands, Norway, Poland, Spain, Turkey, The United Kingdom, and The United States of America. The CIS3 Partnership helps to set common standards that ensure the effective cooperation between member states and the efficiency of conducting missions while guaranteeing the autonomy of their own systems. According to the NCI website, the partnership "rings together nations who want to maintain and influence the further development of selected CIS security standards for use in Nations and NATO, achieving interoperability across the Alliance, as well as internally in the Nations between devices from different manufacturers" (NCI Agency, n.d.).

## Private Sector

The private sector has a huge role to play in the French cybersecurity structure. In the CIIP framework, private companies constitute the operators of vital importance and the critical infrastructure sectors. Some private companies are also on the list of Trusted Services Providers to "facilitate access of administration and national critical operators to highly efficient and trust cybersecurity and cyberdefence services." The cybersecurity industry and market are both dominated by five major private companies with strong capacity to influence the government's decision on cybersecurity governance. While this market structure ensures the quality of cybersecurity products and services, it also hinders development and innovation to some extent.

The French government largely incorporates the private sector into the critical infrastructure information protection framework. In December 2013, ANSSI promulgated a regulatory framework, the CIIP Law. The Law applies to more than 200 public and private operators from 12 sectors already defined as critical (operators of vital importance, defined as "operator[s] whose unavailability could strongly threaten the economic or military potential, the security or the resilience of the Nation") by France's framework for the security of activities of vital importance established in 1998. The CIIP Law requires operators to identify their critical information systems supporting vital functions of the operators and "whose unavailability could strongly threaten the economic or military potential, the security or the resilience of the Nation" and submit a list of their critical information systems to ANSSI (ANSSI, n.d.). ANSSI and the operators collectively published security rules to reduce the risks of cyberattacks.

In order to better facilitate the implementation of the CIIP law and promote public-private partnership, ANSSI allows the qualification of private Trusted Service Providers. The list of qualified products and services contains 4 categories: cybersecurity audit service providers (PASSI), incident detection service providers (PDIS), integration response services providers (PRIS), and integration/architecture service providers (planned) (ANSSI, n.d.). In this way, ANSSI involves the private sector to support operators in raising their level of cybersecurity.

In November 2014, ANSSI started setting up working groups (WG) with voluntary public and private operators to construct a Public and Private Partnership (PPP) on CIIP (ANSSI, n.d.). WGs managed to develop a critical information systems typology, cross-sectoral security rules, and a security incidents framework. Operators also benefit from the participation in WGs. On a multistakeholder basis, the WGs co-draft with the operators tailoring the provisions to meet the sectors' expectations and constraints and avoid unnecessary burden for the operators. In case of an incident, ANSSI would provide direct assistance to the operators in the working groups, constituting a fairly strong incentive for the operators to join the WGs (ANSSI, n.d.).

The cybersecurity market in France is also led by private enterprises. The French cybersecurity industry sector is a mature market with around 700 companies (Calcara and Marchetti, 2021). The market has been led by 5 major companies: Airbus, Thales, Atos, Orange, and Sogeti. From traditional network protection solutions to network surveillance devices, the 5 companies "provide the full range of cybersecurity products" (Calcara and Marchetti, 2021). The French cybersecurity industry has been able to influence Paris' cybersecurity governance strategy significantly. The High Council for Strategic Education and Research (CSFRS) created in 2010 gathered a broad range of civilian, military, industrial, and governmental expertise to offer strategic suggestions to the government. The council suggested investing massively in the cyber security industry, promoting a centralization of cybersecurity governance, and establishing a privileged relationship between the state and the industry in the cybersecurity market (Calcara and Marchetti, 2021). Therefore, French cybersecurity governance has been constantly driven by the private sector's desire to strengthen the Public and Private Partnership (PPP).

While the cybersecurity responsibilities in France are dispersed among different bodies, there is a sole cybersecurity authority; namely, French cybersecurity regulations embody a high degree of centralization. The centralized institutional framework, shaped by the interpenetrating PPP, provides the private sector with an advantageous channel to lobby.

In order to build a reliable network of government suppliers for the cybersecurity supply chain, ANSSI issues Common Criteria Certification (or "IT Security Certification") to ensure the compliance of a product with a specifications document or technical specifications through the intervention of an independent, competent, and supervised professional certification body

(ANSSI, n.d.). Enacted on April 18, 200, decree 2002-535 pinpoints French certification framework for security products and systems. ANSSI takes the responsibility to examine certifications according to "specifications or standards specified by the ANSSI" and based on evaluation studies conducted by Information Technology Security Evaluation Facilities (ITSEF) "licensed by the French Prime minister and accredited by the French accreditation committee (COFRAC) according to the standard NF EN ISO/CEI 17025". The certification requirements impose high costs, which are way above the costs of similar product certifications in the US or Germany, for private cybersecurity companies to enter the market (Baumard, 2017).

### Summarization and Evaluation

As a member state in both the European Union and the North Atlantic Treaty Organization, France actively interacts with the two organizations on an international scale. French cooperation with the EU focuses more on the economy and the industry, while France leans towards NATO in terms of military and intelligence. It is worth mentioning that France's ties with the European allies are stronger than those with the NATO allies. While France does differentiate its engagement with EU and NATO, there could be potential overlaps or even conflicts as France incorporates both EU and NATO cybersecurity agenda and interoperability into its cybersecurity framework.

The private sector in the French cybersecurity framework is mature and vibrant. Private cybersecurity companies constitute operators of vital importance and trust services providers to bolster French cybersecurity, and they are well equipped for lobbying and influencing the government's decision on the cybersecurity market given the advantageous institutional structure. Private firms may also participate in the working groups to confer on the sectoral and cross-sectoral security rules.

Yet, there are also overt issues regarding the French cybersecurity market. The market is essentially composed of five major corporations and more than 600 small and medium enterprises (SMEs) with fewer than 20 employees, while the 5 major companies with potent lobbying power cover the full range of cybersecurity products. Moreover, while the certification requirements improve the quality of French cybersecurity products and services and effectively protect the market from potential external competitors, they also lead to high entry barriers in the cybersecurity market. Therefore, French small and medium companies have raised concerns about the overwhelming regulation of the cybersecurity market. The high entry barriers might cause market inefficiency and discourage the development of young, R&D intensive, innovative cybersecurity start-ups.

## Overall Effectiveness

In general, France has an effective unitary cybersecurity system with clear jurisdiction, robust regulatory system, and vigorous international cooperation as well as public-private partnerships. France earned a score of 84.42 out of 100 on the national cybersecurity index (NCSI) in 2022, and the score has been fairly stable in the last three years. France ranks 11th in National Cyber Security Index, 9$^{th}$ in Global Cybersecurity Index, 15$^{th}$ in Information and Communication Technology (ICT) Index, and 14th in Networked Readiness Index (NCSI, n.d.). According to the NCSI, France is particularly equipped in the protection of essential services, protection of personal data, fight against cybercrime, and military cyber operations; although

France has not reached an ultimate level, the country is also strong in cybersecurity policy development, cybersecurity education and professional development, and e-identification and trust services, (NCSI, n.d.). Notwithstanding, the lack of a single point of contact for international coordination and the lack of national-level cyber crisis management exercises also manifest the need for continuous development and improvement. But overall, the cybersecurity environment in France is safe.

The cybersecurity jurisdiction is fairly clear in France. The sole national cybersecurity authority, ANSSI, assists and coordinates government departments and operators of vital importance; Ministry of Interior anticipate, detect and counter cyber threats; Ministry of Armed Forces ensures the protection of French territory, population and interests; the High Council for Strategic Education and Research (CSFRS) serves as the research agency that the private sector used to lobby the government; the National Commission on Informatics and Liberty (CNIL) works independently to secure citizens' data rights and freedom. Although the functions of the Analysis Center for Cyber Defensive Operations in the Minister of Armed Forces and CERT-FR in the ANSSI overlap, these two departments co-locate and cooperate with each other. While some missions within the international framework, specifically, the EU and NATO, are carried out by the ANSSI and the Ministry of Armed Forces, there is, however, no specific agency responsible for international coordination. This is potentially hazardous for France, a country deeply involved in the international cybersecurity framework.

While the private sector, dominated by the five major companies, cannot manipulate the government's decisions, they are able to influence the cybersecurity legislation effectively by lobbying. The highly centralized institutional framework shaped by the private companies put the private sector in an advantageous position to lobby the administration for favorable policies and legislation. Though there are no formal conventions or organizations to bring different stakeholders together, the CSFRS gathers civilian, military, industrial, and governmental expertise to provide strategic suggestions for the government. Also, private companies in the 12 critical sectors may join the working groups to confer on the security rules applied to their sectors. However, the lobbying channel is largely ruled by the five large enterprises, and the lobbying power of the small and medium companies is limited.

The information sharing mechanisms are mostly clear in the French cybersecurity framework. All data controllers are required to report any incidents to the CNIL and all victim critical operators are required to report any incidents to the ANSSI. Data controllers should inform other entities in risk and the ANSSI would share anonymized information on the incident with other critical operators in risk. Victim critical operators may inform other operators on a voluntary basis. The ambiguity here is that there is no absolute standard to define the necessity of voluntary information sharing.

The French strategies are outcome focused and technology neutral. The White Papers and national strategy documents continue to renew the direction of cybersecurity development and adjust to the constantly changing landscape. The sector and cross-sector security rules are also flexible for the evolving technologies, as they are tailored to fit the specific sectors. The only concern is that the oligopolistic cybersecurity market and the high entry barriers of IT Security Certification might decelerate the emergence of new technologies.

Cybersecurity defenses remain a critical field in national governance and the cybersecurity industry remains vigorous, as President Emmanuel Macron announced the embankment of €500 million (around $600 million) to help private companies and public authorities boost their cyber defenses (Nussbaum, 2021). According to Bloomberg, Macron's

goal is to triple the annual sales of French cybersecurity companies to 25 billion euros in 2025 from 7.3 billion euros in 2019, and double the number of jobs in the sector by 2025 (Nussbaum, 2021).

In the 2021 International Cybersecurity Forum, the ANSSI defends the future of European cybersecurity, based on cooperation and solidarity (ANSSI, 2021). Given the French presidency in the EU in 2022, France commits to strengthen European sovereignty in cybersecurity, revise the NIS Directive, bolster the cybersecurity of EU institutions, develop a trusted industrial base and European solidarity in case of a major crisis (ANSSI, 2021). Both French cybersecurity and EU cybersecurity continue to thrive.

# Lithuania

Republic of Lithuania has a unitary governance model with an effective cybersecurity governance system in place, based on its established national cybersecurity framework and robust level of international cooperation. The Lithuanian cybersecurity regulatory landscape is primarily focused on enhancing regulations around critical infrastructure, creating a data transfer network suitable for use during a crisis, and cooperation with the EU and NATO. Lithuania has a moderate level of development of public-private partnerships, as demonstrated by the insufficient ability of the private sector to provide feedback on legislation. Lithuania is a good case study for understanding the effectiveness of a unitary cybersecurity governance model. Table 11 summarizes findings on Lithuania's cybersecurity framework.

Table 11: Findings on Lithuania's Cybersecurity Framework

| **Overall Cybersecurity Assessment** | |
|---|---|
| Overall system effectiveness | Effective |
| System style | Unitary |
| National Strategy and Framework | Established |
| NCSI index rating | 93.81 |
| **Legal Framework and Effectiveness** | |
| Is the framework parsimonious? | Yes |
| Is jurisdiction clear? | Yes |
| Are there gaps in the framework? | Yes |
| Is regulation: outcome-focused, technology-neutral, and risk-based? | Outcome-focused, risk-based |
| **Regulation and Enforcement** | |
| Are regulation/enforcement sector-specific? | Somewhat |
| Is there an enforcement agency? | Yes |
| **Relationships** | |
| Are there international relationships? | Yes |
| Can the private sector weigh in? | Somewhat |
| What characterizes information sharing? | Sufficient |

## Country Background

The Republic of Lithuania is a democracy with a GDP of $65.5 billion (World Bank, 2022). Lithuania earned a score of 93.81 on the NCSI Index in which it ranked second globally (NCSI : Lithuania, 2021). Lithuania has made significant investments in cybersecurity in recent years, and as a result, it has received the highest assessment in the areas of legal regulation and the development of cybersecurity facilities according to external evaluators such as the Global Cybersecurity Capacity Centre (Bada & Weisser Harris, 2017, pp. 5–7). Lithuania is an excellent example of a unitary governance approach to national cybersecurity. It also has a strong cybersecurity industry, with many companies specializing in providing security services to businesses and government agencies. In recent years, the country has become a victim of the world's biggest cyberattacks, including disinformation campaigns (Judson, 2019). As a result, Lithuania has gained a wealth of experience in dealing with cyber-threats. This experience is now being used to help other businesses and corporations around the world improve their cybersecurity practices.

## Cybersecurity Agencies

The main characteristics of Lithuania's structural organization are: a unitary approach to governance, clearly defined lines of responsibilities, and an adherence to the international cybersecurity generally recognized regulations. In Lithuania, the structure of the national cybersecurity authorities and regulatory agencies is unitary, with the Ministry of National Defense (MoND) playing the central coordinating and organizational role. Few organizations work directly under the MoND to manage national cybersecurity agendas: the National Cyber Security Centre (NCSC) embodies the regulatory function of the MoND and the Cyber Security Council acts as an advisory body to the MoND. Other national entities such as the Lithuanian Armed Forces, the Lithuanian Police, and the General State Security Department are also providing support and performing defense functions. In addition, several other agencies and organizations are international initiatives. Some originated from the EU and are aligned with the EU regulations that take precedents over the national regulations. Others are national institutions that are following universal models of the established cybersecurity organizations. Examples include the Computer Emergency Response Teams (CERTs), the Cybersecurity Information Network (CSIN), and the State Data Protection Inspectorate (VDAI).

MoND's obligations as a central cybersecurity authority are prescribed by the Republic of Lithuania Law on Cyber Security No. XII-1428 (2014) stipulates that MoND is responsible for ensuring the effectiveness of the country's Cybersecurity Strategy and for coordinating repair work in case of an incident. It is also responsible for submitting organizational and technical requirements for approval to the government, as well as approving typical plans for incident management and cyber defense. Furthermore, the MoND establishes procedures for responding to incidents and for implementing technical measures for security. It also participates in crisis management for cybersecurity. Lastly, the Ministry is responsible for developing recommendations and proposals for improvement in the legal regulation of cybersecurity, as well as other functions entrusted by the government (Republic of Lithuania Law on Cyber Security; No. XII-1428, 2014). Consequently, Lithuania's cybersecurity policymaking, regulation, assessments, and response are largely resting on the shoulders of the Ministry of National Defense, as this authority is a hub of all decisions regarding cybersecurity.

The Republic of Lithuania Law on Cyber Security No. XII-1428 also defined the National Cyber Security Centre (NCSC) as the primary cybersecurity institution in Lithuania (2014). The Law further dictates that the NCSC is responsible for ensuring the cybersecurity of the country's information resources and critical infrastructure, and for managing cyber incidents on a national level. The NCSC also works with businesses, research and education institutions, and other cybersecurity entities to develop projects that strengthen national cybersecurity. In addition, the NCSC processes personal data necessary for the fulfillment of its functions and cooperates with international organizations, foreign authorities, and services in the field of cybersecurity. Finally, the NCSC fulfills the functions outlined in Lithuanian legislation in the area of cybersecurity assurance (Republic of Lithuania Law on Cyber Security; No. XII-1428, 2014). Thus, NCSC may be considered an institutionalized representation of the MoND in the cybersecurity area with a direct link to the government.

To fulfill the scope of its responsibilities, in 2015 the NCSC established the Regional Cyber Defense Centre (RCDC) with the main objective of strengthening Lithuania's cyber-defense posture by providing expert analysis and advice on cybersecurity issues, as well as training and research in this field (Petkevičius, 2021). The key operational objectives of the RCDC are to strengthen cooperation with the United States of America, Ukraine, Georgia, and other strategic partners of Lithuania in the field of cybersecurity, and to contribute to the development of a comprehensive national approach to cyber-defense (*About RCDC*, 2022). Thus, RCDC, being a part of NCSC, falls under the jurisdiction of MoND.

The Cyber Security Council was set up following the approval of Resolution No. 422 and is headed by a representative of the Ministry of National Defense and falls directly under its jurisdiction (Skvernelis & Karoblis, 2018, p. 12) as well as NCSC. The Cyber Security Council is a permanent collegial independent advisory body that analyzes cybersecurity in Lithuania and is comprised of twenty-four experts from across the industries and the Lithuanian government (Cyber Security Council of Lithuania Convened for the First Time, 2015). The functions and scope of practice of the Cyber Security Council are defined by the Republic of Lithuania Law on Cyber Security No. XII-1428 (2014). According to it, the Cyber Security Council puts forward proposals to institutions that develop and implement cybersecurity policy, cybersecurity entities, research and educational institutions, and business entities. It also can submit suggestions to the cybersecurity actors about cybersecurity priorities, development directions, target results, and ways the objectives are to be pursued. Lastly, its functions include identifying opportunities for cooperation between the public sector, business, and research in the field of cybersecurity assurance (Republic of Lithuania Law on Cyber Security; No. XII-1428, 2014). To achieve these goals, the Council has access to all relevant information related to Lithuanian national cybersecurity and participates in joint projects with other state institutions and private businesses in order to carry out activities that improve cyber hygiene awareness and practices (Skvernelis & Karoblis, 2018, pp. 12–13). Thus, the Cyber Security Council is essentially the main link between the private sector and the cybersecurity authorities in Lithuania.

The Cybersecurity Capacity Review Republic of Lithuania defines Lithuania’s Computer Emergency Response Team (CERT-LT) as a responsible agency for investigating incidents involving electronic communications networks and information security (2017). According to the review’s assessment, the CERT-LT team coordinates its actions with similar organizations at the sub-national, sectoral, and international levels and reports its findings to the appropriate authorities. Its functions include compiling yearly statistics and reports on network and information security incidents. CERT-LT also plays a role in coordinating the response to cross-

border incidents in collaboration with other EU-level teams (Bada & Weisser Harris, 2017, p. 6). As such, it ensures the continuity and security of electronic communications networks within Lithuania and outside its borders. However, some of the functions are overlapping with the national agencies such as NCSC and the Cyber Security Council.

As of July 2016, according to the Directive (EU) 2016/1148 of the European Parliament and of the Council the State Data Protection Inspectorate (VDAI) became an agency tasked with protecting the personal data of Lithuanian citizens and enforcing the country's laws on data protection (OJ 2016 L 194, p. 1). The Directive 2016/1148 defines VDAI as a responsible party for ensuring that data processing is carried out in compliance with Lithuanian and European Union law and is an active member of the European Data Protection Board (EDPB), which is responsible for overseeing the application of data protection law across the EU (OJ 2016 L 194, p. 1). The Inspectorate monitors compliance with electronic communications laws in Lithuania. In addition to its supervisory role, the EDPB also coordinates enforcement activities and provides guidance on data protection issues (Andrijauskas, 2020). The VDAI is also responsible for supervising the activities of controllers and processors of personal data in line with the EU's General Data Protection Regulation (GDPR). Controllers must comply with the requirements of the GDPR, as well as ensuring the security of personal data processed by them (Hassan, 2018). In recent years, the VDAI has taken an active role in promoting cybersecurity in the private sector. For example, in the Annual Report for 2021 stated that the agency launched a campaign to raise awareness of phishing attacks and distributed educational materials to businesses and individuals (2021). The VDAI has also published guidance on cybersecurity best practices and helped to develop a national cybersecurity strategy (*Annual Report of Personal Data Protection Supervision in Lithuania in 2021*, 2021, pp. 8–9). As a result of these efforts, the private sector in Lithuania has become more aware of the importance of cybersecurity and has made significant progress in protecting its data. The VDAI's work is therefore essential for ensuring the cybersecurity of the private sector in Lithuania.

The Cybersecurity Information Network (CSIN) is a European Union initiative that was established to improve coordination and information sharing among member states on cybersecurity matters (Skvernelis & Karoblis, 2018, p. 13). Article 13 of the Republic of Lithuania Law on Cyber Security No. XII-1428 prescribes CSIN to build communication between public and private sectors (2014). Thus, CSIN typically shares information on potential or past cyber incidents, as well as recommendations, orders, technical solutions, and other measures which help assure cybersecurity and cooperation among the members of the network. To use the CSIN, entities must meet certain requirements set forth in the CSIN regulations. They must also have someone assigned who is responsible for the organization of cybersecurity and management of cyber incidents (Republic of Lithuania Law on Cyber Security; No. XII-1428, 2014). The purpose of these requirements is to ensure that only those who are serious about cybersecurity have access to the wealth of information available through the network. Thus, Lithuania through CSIN collaboration and testing exercises manages to implement additional cybersecurity measures (Key Trends and Statistics of the National Cyber Security Status of Lithuania, 2022, pp. 12–13). In this way, the CSIN is another link that helps to improve communication and collaboration between private, public, and administrative sectors.

## Summarization and Evaluation

Lithuania's cybersecurity authorities are considered effective because they are well-organized and have a clear hierarchy, which allows for efficient decision-making. Additionally,

they have strong ties to the EU, which helps to ensure that they are up to date on best practices and trends. However, there are some gaps and overlaps in their functionality. Also, the same reliance on the European Union for its cybersecurity structure and resources can lead to a slowdown in response time or lack of coordination in the event of a major cyber incident. There is also room for improvement in communication and coordination between different agencies since the structure and the relationships are fairly new. Overall, however, the Lithuanian cybersecurity authorities are generally effective in their roles and functions. The responsibility division and strong will for cooperation between the actors are the indicators that this system has great potential and with time the gaps and overlaps will reduce.

# Regulatory Framework

Cybersecurity is an important issue for any country, but it is especially important for Lithuania, considering its proximity to Russia and its geopolitical situation. To protect itself from cybercrime and nation-state attacks, Lithuania has enacted a number of laws and regulations related to cybersecurity. Lithuania's National Cyber Security Strategy is part of its wider efforts to ensure a high level of security. In recent years, Lithuania has invested heavily in upgrading its cyber regulatory mechanisms and has taken part in several international initiatives to enhance cooperation on cybersecurity, improving its cybersecurity potential.

## National Framework

According to Štitilis et al., one of the first pieces of cybersecurity legislation in Lithuania, the Republic of Lithuania Law on Cyber Security, was enacted in 2003 and was focused on ensuring the confidentiality of electronic communications (2017, p. 362). This Law was later updated in 2006 to include provisions on data security and integrity. In 2009, Lithuania became one of the first countries in the European Union to pass a comprehensive law on cybersecurity, which established a national cybersecurity strategy and created several institutions and mechanisms for implementing it. The law also criminalized many activities related to cybercrime, such as unauthorized access to computer systems and data, and the distribution of malicious software (Štitilis et al., 2017, pp. 362–363). Since then, Lithuania has continued to update its cybersecurity legislation in line with international standards and best practices. The Republic of Lithuania Law on Cyber Security No. XII-1428 was updated to require all electronic communications providers to ensure the security of their networks and customers' data and to create some new offenses related to cyber-crime, such as identity theft and fraud (Republic of Lithuania Law on Cyber Security, 2014).

The Republic of Lithuania Law on Cyber Security No XII-1428 outlines six principles for ensuring the country's cybersecurity (2014). The first principle is that cybersecurity is a shared responsibility. This means that everyone has a role to play in keeping Lithuania's cyberspace safe, from individuals to businesses to government agencies. The second principle is that cybersecurity must be proportionate. This means that the measures taken to ensure cybersecurity must be appropriate to the risks involved. The third principle is that cybersecurity must be risk-based. This means that the threats and vulnerabilities must be identified and prioritized so that the most effective countermeasures can be put in place. The fourth principle is that cybersecurity systems must be resilient. This means that systems and networks must be designed to withstand and recover from attacks. The fifth principle is that cybersecurity must be

constantly evolving. This means that organizations must continuously monitor and update their security measures to keep up with the latest threats. The sixth and final principle is that cybersecurity must be global. This means that cooperation between different countries is essential in order to effectively tackle cross-border cyber threats (Republic of Lithuania Law on Cyber Security; No. XII-1428, 2014).

Lithuania's National Cyber Security Strategy, approved by the government in November 2016, sets out the main objectives and priorities for ensuring a high level of cybersecurity in the country (2016). The strategy is based on the principles of international law, respect for human rights and fundamental freedoms, and the rule of law. It also takes into account the need to ensure an adequate level of security for critical infrastructure and essential services (*National Cybersecurity Strategy of Lithuania*, 2016). According to Skvernelis & Karoblis, to achieve this, the strategy sets forth a number of measures to be taken at the national, government, and EU levels (2018). At the national level, the measures include strengthening Lithuania's Cyber Security Centre, developing a national cybersecurity strategy, and improving cooperation between government agencies and the private sector. At the government level, the measures include establishing a cross-sectoral task force on cybersecurity, drawing up contingency plans for dealing with major cyber incidents, and enhancing information sharing between EU member states. At the EU level, the measures include contributing to the work of the European Union Agency for Network and Information Security (ENISA) and participating in EU-wide exercises such as Cyber Europe (Skvernelis & Karoblis, 2018).

## Enforcement Mechanisms

In Lithuania, several reporting mechanisms have been established and are regularly used, such as an online platform of the e-police, the EU reporting agency CERT-LT, and the National Cyber Security Center (NCSC). A detailed audit of critical infrastructure is performed every two years or so depending on governmental needs (Bada & Weisser Harris, 2017, p. 6). Lithuania’s Law on Electronic Communication of the most important enforcement regulations that oblige entities in both public and private sectors to certain standards (Republic of Lithuania Law on Electronic Communications; No IX-2135, 2014). Under this law, cyber incidents the entities from the public sector and the critical infrastructure must be reported to the National Cyber Security Centre within one hour of becoming aware of the incident.

According to the National Cyber Incident Management Plan decree No. 1209, public and private cybersecurity entities are required to provide the National Cyber Security Centre with telephone numbers, e-mail addresses, and other contact information of the responsible persons who can be contacted on a 24-hour basis, so that the contact information was always available during the cyber incident management (2018). Depending on the danger level of the threat the governmental entities would report differently. For high-impact cyber incidents, the threats must be reported immediately, no later than one hour after detection. For moderate impact cyber incidents, the report must be submitted no later than four hours after detection. In case of minor cyber incidents, governmental entities may report them periodically, for example, on the first working day of each calendar month (National Cyber Incident Management Plan; Decree No. 1209, 2018).

To protect digital information and thwart potential cybercrime, service providers are required by the National Cyber Incident Management Plan decree No. 1209 to report high-impact incidents to the NCSC (2018). This includes, but is not limited to, critical infrastructure that may be disrupted as a result of the incident. Reporting must be done within one hour of

learning of the incident. Persons who are not legally obliged to report are encouraged to do so to maintain the safety and security of digital information. When the NCSC receives information about a potential cyber incident from sources who are not required to report such incidents, the center will categorize and investigate the incident in the same manner as incidents that are officially reported (National Cyber Incident Management Plan, 2018). This allows the center to more effectively track and respond to potential threats, as well as to identify patterns and trends that may be indicative of larger problems.

It is important to note that upon receiving a report of a potential cybersecurity incident, NCSC has the right to request additional information for either avoiding or managing the incident according to the National Cyber Incident Management Plan (2018). In cases where it is necessary to inform the public, the NCSC will consult with the entity who reported the incident before issuing a statement in order to provide accurate information and avoid panic. However, if the situation is deemed urgent, the NCSC may insist that the entity itself inform the public to manage the incident effectively (National Cyber Incident Management Plan, 2018). The NCSC itself is also obliged to report non-classified information on the cyber-incident within 30 working days (Incident Management, 2018). By making this information available the NCSC opens the pathways for communication with the private sector which is an essential part of the National Cyber Security Strategy of Lithuania.

Failure to comply with the cybersecurity requirements in Lithuania may result in administrative liabilities for the public administration bodies (the private sector's responsibilities are not strictly imposed unless they are identified as critical infrastructure). According to the Code of Administrative Offences, there is a fine (€1,448) for such violations that are imposed on the chief executive officer (Beržanskiene, 2017). However, failure to comply with the requirements and committing a cybercrime are falling under different jurisdiction categories and are punishable differently. The criminal law of Lithuania contains substantive provisions that relate to cybercrime. The country has ratified regional and international treaties to combat cyber threats. The Criminal Code of Lithuania includes an article about crimes committed with electronic devices, but there are no punishments for identity theft in both electronic and non-electronic spaces (Bada & Weisser Harris, 2017, p. 8). However, if the term 'cybercrime' is deemed as a crime against the security of electronic data and information systems, it can result in criminal liability and penalize with a fine, community service, arrest, or even imprisonment for up to three years (Beržanskiene, 2017). Thus, the understanding of the difference between the legal requirements and recommendations, administrative violations, and crimes is crucial in order to establish any business relations in Lithuania.

It is important to note that The State Data Protection Inspectorate (VDAI) is also entitled to take remedial actions and impose sanctions depending on the circumstances of a particular case (Andrijauskas, 2020). Following Regulation (EU) 2016/679, VDAI may "warn, make a reprimand, provide instructions, restrict or prohibit the processing of data, impose an administrative penalty which, depending on the breach, may be up to 2 or 4 percent of the total annual global turnover of the previous financial year or up to EUR 10 million or 20 million" (OJ 2016 L 119, p. 1). In 2021 alone, VDAI imposed 2 warnings, issued 8 recommendations, imposed 26 administrative penalties, drew up 30 records of administrative offenses, and issued 101 instructions and 101 reprimands on the organizations (*Key Trends and Statistics of the National Cyber Security Status of Lithuania*, 2022). Although it may vary from region to region, in the EU and Lithuania specifically, personal data protection is of high priority based on its comprehensive legal coverage.

## Sector Framework

Lithuania has only recently shifted toward sector-specific cybersecurity regulations, with its laws initially applying to a wide range of industries, from energy and healthcare to banking to telecommunications. Under Lithuanian Law on Electronic Communications No IX-2135 certain actors are required to report cyber incidents: internet service providers, banks, e-money institutions, payment service providers, electronic communications providers, electricity and gas providers, transport operators, and e-commerce companies (2015). The types of incidents that must be reported include those that result in a loss of service or degradation of service quality, as well as those that compromise the security of networks and information systems (Republic of Lithuania Law on Electronic Communications, 2014). The release of these regulations followed a number of high-profile cyberattacks in Lithuania, including a ransomware attack on the country's largest hospital and a data breach at the country's tax authority (*Key Trends and Statistics of the National Cyber Security Status of Lithuania*, 2022). The new regulations required companies to take several steps to improve their cybersecurity, including appointing a dedicated cybersecurity officer, implementing risk management processes, and conducting regular cybersecurity audits (*National Cyber Incident Management Plan*, 2018).

The reporting requirements are laid out in Article 15 of the Lithuanian Law on Electronic Communications No IX-2135 (Republic of Lithuania Law on Electronic Communications, 2014). The Order on the Approval of the Rules on the Insurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services regulates all the rights and responsibilities of public communication networks as well as service providers (Bada & Weisser Harris, 2017, p. 7). Additionally, the Law on Electronic Communications No IX-2135 covers a wide range of topics related to electronic communications, including infrastructure, services, user rights, and obligations, and safety requirements (2014). Lithuania's Law on Electronic Communications No IX-2135 sets a requirement on providers of electronic communications services to implement appropriate technical and organizational measures to safeguard the security and integrity of their services. These include measures to prevent and detect unauthorized access to networks and facilities, as well as measures to protect against distributed-denial-of-service attacks. In addition, providers must take steps to ensure the confidentiality of communications, including the use of encryption. Furthermore, the law requires providers to take into account the risks posed by new technologies and to take steps to mitigate those risks (Republic of Lithuania Law on Electronic Communications, 2014). Before the adoption of the National Cyber Security Strategy, the laws did not mention the private sector; however, in the most recent revisions, the role of the private sector, especially in the critical infrastructure, is articulated.

Complex cyberattacks target public, state, and municipal institutions, organizations of the member states, and critical infrastructure. According to the 2022 Key Trends and Statistics report on cybersecurity, as the legal framework in Lithuania only recently specifically included its critical infrastructure in the cybersecurity regulatory process, only 77% of them completed the process of agreement on their cybersecurity documentation with the NCSC (2022). The goal was announced by the end of 2022 for the majority of Lithuania's critical infrastructure managers to complete their security documentation with NCSC. To speed up this process, in 2021 NCSC made the process mandatory for applicable entities. The instructions and penalties were issued under the Administrative Code of the Republic of Lithuania. Also, as the number of cybersecurity attacks increased due to the conflict in Ukraine, the NCSC provided detailed instructions for critical infrastructure managers. Preventive measures such as surveys and

inspections to determine the status of cyber security stakeholders, both scheduled and non-scheduled, were conducted promptly (*Key Trends and Statistics of the National Cyber Security Status of Lithuania*, 2022, p. 14). Also, in 2021 a new draft on cybersecurity regulation for critical infrastructure in Lithuania was published by MoND and is going through the revision process at the moment (*Key Trends and Statistics of the National Cybersecurity Status of Lithuania*, 2022, p. 15). The details of the said draft are still subject to change and will require closer consideration once the revision is published.

Lastly, the VDAI is also tightly involved with sector-specific regulations. The agency is actively monitoring activities of the Compliance, eHealth and Government Expert Subgroup (CEH), the International Transfer Subgroup (ITS), the Coordinated Enforcement Framework (CEF) working group, the Communication Network, the network of the Data Protection Officers (Andrijauskas, 2020). In 2021, VDAI even took part in the assessment of 16 prior binding corporate rules and co-authored 14 opinions of the EDPB on the binding corporate rules (*Annual Report of Personal Data Protection Supervision in Lithuania in 2021*, 2021). Thus, when it comes to sector-specific regulations, one needs to take into account the impact of VDAI on the specific business as it has more enforcement ability than its international equivalents.

One could also argue that Lithuanian cybersecurity authorities are more inclined to cooperate with different sectors via mutual assistance instead of implementing regulation. This can be seen in the 2022 Key Trends and Statistics report on cybersecurity in Lithuania (2022). The active cooperation with the Ministry of Health, the Police Department, the Ministry of Justice, and the State Data Protection Inspectorate were reported. The cooperation with the military sector was launched in 2021 to enhance cybersecurity within the National Defense Network (*Key Trends and Statistics of the National Cyber Security Status of Lithuania*, 2022, p. 12). These cooperation tactics aimed to create more approachable pathways for raising cybersecurity awareness and improving the trust in the authorities.

## Summarization and Evaluation

To conclude, despite a transition period, Lithuania's regulatory framework vigorously expands its potential: from sectional cooperation and encouragement in the private sector to strict reporting guidelines and administrative sanctions in the public and critical infrastructure sector. In general, the provisions of the cybersecurity laws and regulations efficiently cover the functions of the government and other state institutions responsible for cybersecurity. Despite several gaps, the jurisdiction of the agencies is clear. Although there is an overlap within the regulatory framework, it is not extensive. The legal framework has only recently begun to move toward regulating the private sector on par with the public sector. And although the critical infrastructure receives a lot of attention, there are still very few specific mechanisms in place to see its effectiveness except for VDAI which carries out the EU personal data protection regulations. Lithuania’s adherence to international standards, such as the EU's directives on cybersecurity, allows it to constantly be updated to keep pace with the latest changes in technology. Thus, both outcome-focused (strategies and reports) and risk-based (scheduled/non-scheduled inspections and cross-agencies cooperation programs) regulations are represented in the governing framework of Lithuania, with a prevalence of the risk-based approaches.

# Relationships

Lithuania is deeply embedded in international relationships and institutions as well as serving as a voice for deeper international cooperation in the area of cybersecurity. Domestically, its relationship with the private sector is still in flux. While there are attempts to integrate private sector voices into legislative processes, it is not clear that feedback on legislation is taken into consideration and government actors remain the dominant voice in cybersecurity legislation.

## International Cooperation

Lithuania is engaged in significant international cooperation and cybersecurity and has a multistakeholder orientation to international internet governance. It has signed the Budapest Convention on Cybercrime and the Paris Call for Trust and Security in Cyberspace and is also a member of the Global Partnership on AI and the European Union's High-level Expert Group on Artificial Intelligence (*NCSI: Lithuania*, 2022). In addition, Lithuania focuses on cooperation with NATO, the EU, and other countries which adhere to democratic principles. Through these efforts, Lithuania seeks to ensure that international legal regulation of cyberspace is based on compliance with the provisions of international law, principles applied to activities in this space, security of the open internet, and protection of human rights and freedoms in cyberspace. Specifically, following the decision adopted in NATO Warsaw Summit 2016 (*NATO*, 2022) that recognized cyberspace as the fifth warfare domain, the Lithuanian Armed Forces were designated as the main cyberspace defense body.

Lithuania has been coordinating various EU cybersecurity projects since 2018, one of which is PESCO (Permanent Structured Cooperation). This project includes representatives from six different EU Member States: Estonia, Croatia, Poland, Lithuania, the Netherlands, and Romania (Judson, 2019). A bilateral program on cybersecurity was launched with support from Israel (*Prime Minister: Lithuania leads the world in cybersecurity*, 2019). The CERTs associated with these programs reached and tested their full operational capacity during the Alarmex exercise in Vilnius and Warsaw in May 2021 (*Key Trends and Statistics of the National Cybersecurity Status of Lithuania*, 2022, p. 17). To understand Lithuania's approach to cybersecurity management it is important to follow its international cooperation trajectory. At the moment, these trends include strengthening European ties and close cooperation with the countries that also support democratic principles.

## Private Sector

The Lithuanian government has been working on increasing the level of cybersecurity in the country by cooperating with the private sector. One of the initiatives is the sharing of information on cybersecurity threats between the government and private companies. There are several ways in which the Lithuanian government has sought to cooperate with private companies on cybersecurity matters. In 2016, the Ministry of Defence launched a voluntary Cybersecurity Information Sharing Platform (CISP), which allows companies to share information about cybersecurity threats with the government (Bada & Weisser Harris, 2017). The government has also sought to engage private companies in its Cyber Emergency Response Team (CERT-LT) (*National Cybersecurity Strategy of Lithuania*, 2019). This team is responsible for coordinating responses to major incidents, and members include representatives from both the public and private sectors.

Critical information infrastructure is often represented by the private sector and is not always capable of containing cyber incidents. Thus, cooperation between public and private sectors became inevitable to ensure full cybersecurity. A shift toward cooperation with the private sector came to the realization in 2015 when the Cyber Security Council approved the Resolution No. 422 “On the Approval of Establishment of a cybersecurity Council and its Rules of Procedure” (2015). Cyber Security Council includes representatives from the private sector and makes it possible for the private sector to be able to advise on various cybersecurity issues (Bada & Weisser Harris, 2017, p. 42). It made it possible to share information on cyber incidents, exchange recommendations and technical solutions that is essential step for building cooperation between the private sector and the regulatory authorities.

The government has also established a number of initiatives specifically for small- and medium-sized enterprises (SMEs). According to the National Cyber Security Strategy of Lithuania, in 2017, the Ministry of Economy launched a Cybersecurity Basics for SMEs project, which provides training on basic cybersecurity measures for SME employees (2019). The Ministry has also developed a Cybersecurity Self-Assessment Tool for SMEs, which helps businesses to identify potential risks and vulnerabilities. The main purpose was to enhance the communication and to establish the trust between the actors (*National Cybresecurity Strategy of Lithuania*, 2019, pp. 17–18). Thus, the private sector's delineation in legislation has led to a wider scope of regulation that applies to all business sizes.

Overall, the private sector remains one of the main targets of cyberattacks in Lithuania. While the private-sector importance has just emerged in the regulatory system of Lithuania, there is a response that the country has been resorting to for some time now. Lithuania’s ongoing participation in cross-sector cybersecurity exercises is seem as an effective way to build the resilience capacity of the private sector in times of crisis (*Cybersecurity and Defence Exercise Underway in Lithuania | The Baltic Word*, 2018). The limitation to this approach is its narrow scope: given that the basic scenario is aimed to raise awareness of a specific threat, and, thus, it might be rendered ineffective in case of the future changes in technologies (Luiijf et al., 2019, pp. 174–175). Another limitation lies in the sector-specific nature of exercises, making it hard to make sure that the gained knowledge will be applicable across all critical infrastructures (Luiijf et al., 2019, pp. 174–175). The chosen path of enhancing relationships with the private sector in Lithuania is limited to raising awareness and is generally risk-based. This risk-based approach is outlined in the Law on Management of State Information Resources No XI-1807. It requires state, municipal institutions and agencies which are part of the emergency mobilization process to use a secure state data transfer network (Seimas of the Republic of Lithuania, 2011). This network is separate from public communication networks so it would be able to remain functional in the event of a crisis or war (Jacuch, 2021, p. 113). Implementation of the Secure Network project allows for quicker and more effective response to cyber incidents, as well as savings in state resources dedicated to cybersecurity. Thus, centralization of cybersecurity is considered as the only good measure to provide conditions for more effective collective defense measures.

## Summarization and Evaluation

Lithuanian international cooperation in terms of cybersecurity is highly effective. The country has been working hard to improve its cybersecurity infrastructure and has made great progress in recent years. In particular, Lithuania has also been active in the Council of Europe's efforts to combat cybercrime, and is a member of the European Union's Agency for Network and

Information Security (ENISA). Overall, Lithuania has repeatedly called for greater international cooperation on cybersecurity, urging countries to share information and best practices. Given its experience with cyberattacks and its commitment to international cooperation, it is likely that the country will continue to play a key role in shaping global policy on cybersecurity.

In terms of relationships with national actors, it is clear that the Lithuanian government is taking steps to improve its cooperation with the private sector on cybersecurity matters. This is an important development, as it recognizes that businesses play a critical role in protecting against cyberattacks. It is less clear that there is a significant chance for the private sector to be able to weigh in on cybersecurity legislation. In Lithuania, private businesses can submit comments on draft cybersecurity policies during commentary periods. However, it is unclear whether or not these comments are always taken into consideration by legislators. As such, there may be room for improvement in this area to ensure that private businesses can have their voices heard in the policymaking process. It is largely the main cybersecurity authorities and institutions that are making the decisions and initiating legislative changes.

The risk-based approach in regulating the private sector should also be noted. Lithuania decided on a measure that helps to create a data transfer network that is independent of public communication networks and suitable for use during a crisis.

## General Effectiveness

After a thorough analysis and detailed consideration of the effectiveness criteria, it is safe to suggest that Lithuania has an effective unitary cybersecurity system with clear jurisdiction, a robust regulatory system, and vigorous international cooperation as well as public-private partnerships. According to the latest NCSI index (93.81), Lithuania's cybersecurity environment is quite secure (*NCSI :: Lithuania*, 2021). In particular, the index measures four key areas: legal framework, technical infrastructure, incident response, and information sharing. In each of these areas, Lithuania scored relatively high, indicating that it has in place a strong legal and technical framework for protecting its digital infrastructure. Moreover, the country has an effective incident response system in place, and information about cybersecurity threats is shared efficiently between different stakeholders.

Lithuania's government established several institutions with the primary responsibility for ensuring cybersecurity. In addition, there are a number of other institutions that play important roles in cybersecurity that work together to strengthen national and international cyber resilience. While these institutions have well-defined responsibilities when it comes to cybersecurity, there is still room for improvement. There is a risk that gaps and overlaps could develop in the future. In addition, Lithuania's laws on cybersecurity are still in the revision stage and are not yet as comprehensive as they could be. However, overall, Lithuania's approach to cybersecurity is fairly well-developed and aligned between authorities.

In Lithuania, private businesses can work with the government to help shape cybersecurity policy. Industry groups can submit comments on draft legislation, and there are often public commentary periods where businesses can have their say. However, it is possible that some comments are ignored or not given due consideration. Overall, though, the avenue for businesses to influence cybersecurity policy in Lithuania is narrow. In the case of Lithuania, it is unclear whether or not there are any lobbying pathways associated with its public-private partnerships. Further research is needed to determine whether or not this is a problem. In terms of cybersecurity meetings or conventions in Lithuania, CERT multi-sectoral body is tasked with

coordinating the efforts of government, law enforcement, and private industry. CERT-LT is convening regular meetings and conventions that bring different stakeholders together. These forums provide an opportunity for stakeholders to share information and best practices, identify gaps in cybersecurity preparedness, and develop collaborative solutions to address shared challenges. In addition, CERT also provides training and certification programs for security professionals, which helps to ensure that private sector partners have the knowledge and skills needed to effectively contribute to Lithuania's cybersecurity effort.

Lithuania's law requires public and private entities to take measures to ensure both the security of personal data and the ability to safely share information that can strengthen the cybersecurity of the country. In terms of information sharing, there are several mechanisms in place for communication between government agencies. There are also clear pathways defined in policy for communicating things like breaches, vulnerability information, and crisis management. Overall, Lithuania has robust mechanisms in place for protecting personal data and sharing information among government agencies.

As the world becomes increasingly reliant on digital technology, the need for strong cybersecurity measures is more important than ever. One of the key challenges facing cybersecurity in Lithuania is the need to create more outcome-focused, technology-neutral regulations. This can be a difficult task, as different technologies often have different security risks associated with them. However, by taking a risk-based approach to regulation, Lithuania ensures that its cybersecurity measures are effective and up to date. Another important challenge facing Lithuanian cybersecurity is the need to keep pace with the rapidly changing digital landscape. In order to do this, it is essential to have a strong research and development infrastructure in place. By investing in new technologies and approaches, Lithuania can ensure that its cybersecurity measures are fit for the future.

# Singapore

Singapore has a unitary governance model with an effective cybersecurity governance system in place, based on its established national cybersecurity framework and robust international cooperation. Singapore's cybersecurity landscape is primarily focused on its international and private sector relationships and strong national cybersecurity framework. Singapore has highly developed public-private partnerships, as demonstrated by the ability for the private sector and other stakeholders to provide feedback on legislation. Singapore acts as a good case study to demonstrate the effectiveness of a unitary cybersecurity governance model. Table 12 summarizes findings on Singapore's cybersecurity framework.

Table 12: Findings on Singapore's Cybersecurity Framework

| **Overall Cybersecurity Assessment** | |
|---|---|
| Overall system effectiveness | Effective |
| System style | Unitary |
| National Strategy and Framework | Established |
| NCSI index rating | 71.43 |
| **Legal Framework and Effectiveness** | |
| Is the framework parsimonious? | Yes |
| Is jurisdiction clear? | Yes |
| Are there gaps in the framework? | Yes |
| Is regulation: outcome-focused, technology-neutral, and risk-based? | Outcome-focused, technology neutral |
| **Regulation and Enforcement** | |
| Are regulation/enforcement sector-specific? | Somewhat |
| Is there an enforcement agency? | Yes |
| **Relationships** | |
| Are there international relationships? | Yes |
| Can the private sector weigh in? | Yes |
| What characterizes information sharing? | Sufficient |

## Country Background

Singapore is a democracy, but the People's Action Party has won a majority in every election and held power continuously since the 1950s. Singapore has a GDP of 396 billion (*GDP - Singapore*, 2021). Singapore earned a score of 71.43 out of 100 on the NCSI Index in which Singapore ranked 29th globally. As a nation that has always been highly reliant on technology to power its economy, Singapore began investing in cybersecurity in 2005 with the Infocomm Security Masterplan to coordinate efforts that would strengthen the public sector's cybersecurity capabilities and secure Singapore's cyberspace (Cyber Security Agency of Singapore, 2016 October). Singapore has continued to prioritize its cybersecurity efforts with the addition of new legislation, strategies, and the creation of new agencies to oversee cybersecurity operations through the years. These efforts include the establishment of the Singapore Infocomm Technology Security Authority in 2009 to defend Singapore against cyberattacks and the Cyber Security Agency in 2015, which is the current agency that oversees all cybersecurity related activities. With Singapore's latest Smart Nation initiative in 2014 that aims to digitalize their economy, government, and society, Singapore has also doubled its efforts with its cybersecurity initiatives to keep up with the digitization of the country. Singapore's unitary cybersecurity style of governance provides other countries with a good example of strong international and private sector relationship and outcome-focused and technology-neutral regulations.

## Cybersecurity Agencies

Singapore has a unitary cybersecurity model in which its Cyber Security Agency is the central agency that develops and enforces cybersecurity policies. Other agencies such as the Personal Data Protection Commission and the Singapore Police Force, as well as sector regulators, work together to coordinate cybersecurity efforts.

Established in April 2015, the Cyber Security Agency (CSA) of Singapore strives to secure and protect Singapore's cyberspace, support Singapore's National Security effort, and power and protect Singapore's digital economy and way of life (CSA | Our Organisation, 2022). The CSA is part of the Prime Minister's office and is managed by the Ministry of Communications and Information. The Minister of the Ministry of Communications and Information is responsible for appointing the Commissioner of the CSA, who enforces the Cybersecurity Act. The CSA is responsible for protecting critical information infrastructure, investigating and defending against cyberattacks, creating a safe cyber environment, and providing important cybersecurity information for businesses and individuals, and encouraging technological innovation.

The Commissioner has the authority to appoint Assistant Commissioners, who can be sector leads. As sector leads have better insight into their respective sector, they will be able to create regulations and guidelines that suit their sector on top of the national cybersecurity framework (*FAQ: Cybersecurity Act*, n.d.). The CSA notes that not every sector lead is ready to assume the role of an Assistant Commissioner at the moment in which case they would fall under the designation of critical information infrastructure and thus, CSA regulations (*FAQ: Cybersecurity Act*). Assistant Commissioners have most of the same powers as the Commissioner except for the powers under section 6, 7, 9, and 20 of the Cybersecurity Act. One power of the Commissioner that is shared with the Assistant Commissioners is the ability to create new regulations as necessary, which is beneficial for sector leaders to be able to continue

improving and developing new regulations and guidelines as the cybersecurity threat landscape evolves.

GovTech is the Singapore government's sectoral leader for cybersecurity. GovTech is the lead Cyber Security Group (CSG) and it develops the government's cybersecurity strategies, detects and responds to cyber threats, conducts cybersecurity training, provides advisories and risk assessments, and other duties for Singapore's governmental agencies (*Cybersecurity*, n.d.). CSG works closely with the Chief Information Security Officers of government agencies to provide cybersecurity and technical guidance as well as collaborates with external partners for cybersecurity training and research and development projects (*Cybersecurity*, n.d.). CSG has also hosted one of the largest Capture the Flag competitions in Singapore with over 1,400 participants in order to engage the cybersecurity community and beginners in cybersecurity (*Over 1,400 Registered for GovTech's First-Ever "Capture-the-Flag" Cybersecurity Competition*, 2021). Furthermore, CSG has a blog where members of the CSG posts cybersecurity tips and tricks for developers and cybersecurity specialists (Kai, 2020).

The Infocomm Media Development Authority (IMDA) is a statutory agency within Singapore's government that develops and enforces infocomm and media regulation guidelines. The IMDA provides information regarding infocomm, media, Built Environment, logistics, modern services, retail, and other sector regulations including the cybersecurity guideline. The IMDA enforces the Telecom Competition Code 2012, Telecommunications Act, telecommunication license conditions and other related telecommunications regulations which also includes the cybersecurity guideline. The IMDA also has its own in-house Singapore Computer Emergency Response Team (ISG-CERT) that responds to cyber incidents within the infocomm and media sector, shares cybersecurity advisories, promotes cybersecurity awareness, and cooperates with other CERTs and organizations while resolving cyber incidents (*Infocomm Media Cyber Security*, 2021). The IMDA has a voluntary program called the Cyber Security Vulnerability Reporting (CSVR) where cybersecurity researchers can voluntarily report cybersecurity vulnerabilities in public-facing applications and networks of Telecommunication service providers in which the IMDA will act as the middleman between the researcher and affected organization and work with the affected organization to resolve the issue (*Cyber Security Vulnerability Reporting (CSVR) Guide*, 2021 April).

The Personal Data Protection Commission is the main agency responsible for data protection and is located within the Infocomm Media Development Authority. It creates standard guidelines for data protection in regards to the collection, use, disclosure and care of personal data in Singapore (PDPA Overview, n.d.). The Personal Data Protection Commission strictly oversees data protection only and not cybersecurity. Even though Singapore, similar to the United States and Japan, defines the realm of cybersecurity as relating to the hardware and software that allows access to cyberspace, data breaches can occur simultaneously with a cyber incident in which the Cyber Security Agency and the Personal Data Protection Commission would have to coordinate efforts to address the breach in personal data and the cyber incident (*Next Steps for Cyber Norms in ASEAN - RSIS*, October 2018).

The Monetary Authority of Singapore (MAS) is Singapore's central bank and financial sector regulator which includes banking, capital markets, insurance and payment. The Monetary Authority of Singapore Act gives the MAS the authority to regulate the financial sector. The MAS has released notices for its sectors that are legally binding requirements for the specific sector or individual. In addition to notices, the MAS releases guidelines which are principles or best practice methods that regulate the conduct of an institution or individual (*Supervisory*

*Approach and Regulatory Instruments*, n.d.). Guidelines are not legally binding and do not have fines or penalties attached, but the MAS recommends following the spirit of the guideline as it affects the MAS' overall risk assessment of the institution or individual (*Supervisory Approach and Regulatory Instruments*, n.d.). The MAS has a Cyber Security Advisory Panel composed of leading cybersecurity experts that provides information on the cybersecurity threat and technology landscape, advises the MAS on cybersecurity best practices, and recommends measures for increasing cybersecurity resilience (*Cyber Security Advisory Panel*, n.d.).

The Singapore Police Force is responsible for responding to "cyber-dependent crime" and "cyber-enabled crime." Cyber-dependent crime involves offenses such as hacking, ransomware, and website defacements in regards to the Computer Misuse Act. Cyber-enabled crime involves online scams, harassment, extortion, among other crimes. (Cybercrime, n.d.). The Singapore Police Force enforces the Computer Misuse Act and cooperates with the Cyber Security Agency, Personal Data Protection Commission, and other agencies in the case of cyber incidents.

### Summary and Evaluation

Singapore's unitary cybersecurity structure provides a simple and clear understanding of jurisdiction on cybersecurity authorities. Each agency has their own roles and responsibilities that are clearly defined and do not overlap with other agencies that create a streamlined process for understanding cybersecurity authorities. Sectoral agencies may have overlapping regulations with the national Cyber Security Act, but it is still clear on who enforces what regulations. In the event that sectoral regulations are stricter than the national framework, sectoral regulations take precedence over the national framework (*FAQ: Cybersecurity Act*, n.d.). The CSA is responsible for developing cybersecurity laws, enforcing the Cybersecurity Act, investigating and defending against cyberattacks, and protecting critical information infrastructures. Other agencies include GovTech, which develops cybersecurity strategies for government agencies defends and protects against cyberattacks, the Personal Data Protection Commission that develops and enforces personal data protection guidelines, the Infocomm Media Development Authority and the Monetary Authority of Singapore that develops infocomm and media regulations and cybersecurity guidelines regarding financial institutions, and the Singapore Police Force that investigates cybercrimes.

Sharing information between agencies is crucial for the detection, protection, and swift response of a cyberthreat. The CSA as well as SingCERT shares information on cybersecurity threats and vulnerabilities with sector leaders and critical information infrastructures. SingCERT also publishes alerts and advisories for the general public. Certain sectors may have their own CERT team in which they share advisories with their respective sector. SingCERT also coordinates with sectoral CERTs to share information on cyberthreats and vulnerabilities. Among government agencies, GovTech is responsible for creating and coordinating cybersecurity strategies for government agencies and fostering collaboration between government agencies.

## Regulatory Framework

Singapore has a national cybersecurity law that is overarching along with sector-specific cybersecurity regulations that regulate specific sectors such as the financial, healthcare, and

telecommunications sectors. The national cybersecurity law applies primarily towards critical information infrastructure and the licensing of cybersecurity service providers, which has some overlap with certain sector regulations. Singapore also has other laws that work together with the cybersecurity laws if applicable.

The Cybersecurity Act of 2018 provides the legal framework in regards to Critical Information Infrastructures. The First Schedule provides a list of essential services which include: energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, services relating to the functioning of the government, and media. Part 3 of the Act lays out specific laws regarding critical information infrastructure (CII). A CII entity may be wholly or partly located in Singapore, which means that the Cyber Security Act applies to international entities with business operations in Singapore too (section 7). If the CII is owned by the Government of Singapore and is operated by the Ministry, then the Permanent Secretary assigned to the CII is considered the owner of the CII (section 7). critical information infrastructures are required to provide the necessary information about their computer(s) or computer system to the CSA to determine if the entity satisfies the criteria of a critical information infrastructure (section 8). CIIs are required to report cybersecurity incidents to the CSA, perform cybersecurity audits a minimum of every two years and risk assessments a minimum of once a year and report findings back to the CSA, and participate in cybersecurity exercises if directed by the Commissioner. The CSA can impose fines of up to $100,000 and/or imprisonment for up to two years for failure to report an incident as well as other fines and imprisonment combinations for violations of other parts of the Act.

The CSA has created the CII Code of Practice in which CII are required to comply. The CII Code of Practice expands upon the Cybersecurity Act by explaining the minimum requirements of cybersecurity measures CIIs have to implement with the expectation that critical information infrastructure owners (CIIO) will enhance these requirements on their own. CIIO must conduct an audit to review compliance of these Codes a minimum of once every 2 years. The Code of Practice addresses the establishment of policies, standards and guidelines that align with national and sectoral regulations and a procedure for information sharing, the monitoring of and protection against cyber threats, and the creation of a cyber incident response plan (*Cybersecurity Code of Practice for Critical Information Infrastructure*, 2022).

Part 4 establishes the CSA's response to cybersecurity threats and incidents. The Commissioner has the authority to respond and investigate cyber threats and prevent further harm from a threat or incident that satisfies the severity threshold (section 19/20). Under the Act, a serious threat or incident satisfies the threshold if: it has the potential to cause significant harm to a critical information infrastructure, it risks disrupting essential services, it threatens the national security, defense, foreign relations, economy, public health, public safety or public order of Singapore, or the nature of incident is severe enough to harm people in Singapore or harm computer systems, whether the systems are designated CII or not (section 20). The Commissioner also has the authority to direct any individual or organization to take measures or comply with requirements as necessary to prevent, detect or counter any threat to a computer or computer system or any class of computers or computer systems (section 23). SingCERT is Singapore's national Computer Emergency Response Team. They collaborate with international and local CERT to respond to cyber incidents in Singapore only, detect and prevent cyber threats, provide cybersecurity advisories and cyber awareness workshops as well as information on how to respond to incidents.

The Computer Misuse Act, enforced by the SPF, criminalizes unauthorized actions and modifications to computers and computer systems and the unlawful obtaining of personal data. Section 11 works together with the Cybersecurity Act when an individual or organization attempts to gain unauthorized access to computer materials (section 3), perform an unauthorized modification to computer materials (section 5), illegally use or intercept computer services (section 6), and/or illegally obstructs the use of a computer(s) (section 7). The Computer Misuse Act is relevant to cybersecurity only in the case of violations of the Computer Misuse Act in the event of a cyber incident. If any cyber threats and incidents violate the above sections in regards to "protected computers," the CSA and Singapore Police Force (SPF) should be notified of the threat or incident so appropriate action by the appropriate agency can occur. Violators of the Computer Misuse Act are subject to persecution by the (SPF). It is important to note that regardless of the person's nationality or citizenship or the location of the person at the time of the offense, they will be subject to the penalties present in this Act.

The Personal Data Protection Act, enforced by the PDPC, establishes a framework regarding the collection, use, disclosure, and care of personal data. Organizations are required to follow the Data Protection Obligations if they are involved in the collection, use, disclosure, and care of personal data. One part of the obligations that relate to cybersecurity is the requirement of organizations to provide reasonable security protection of personal data to prevent unauthorized access, which means that organizations will have to invest a fair amount in their cybersecurity to prevent a breach (*Data Protection Obligations*, n.d.). A financial penalty of up to $1 million or up to 10% of an organization's annual turnover that is not being enforced yet (Alfred et al., 2021).

Organizations are required to notify the PDPC if a significant data breach is likely to result in significant harm to individual(s) and/or are of significant scale. In addition, this Act works alongside the Cybersecurity Act when a data breach occurs due to a vulnerability in critical information infrastructure or any organization's computer systems. Thus, organizations are required to notify both the CSA and the PDPC if the data breach occurred within a critical information infrastructure entity.

The Monetary Authority of Singapore has set forth Technology Risk Management guidelines for the financial sector. As stated above, guidelines set forth by the MAS do not require financial institutions to comply with the guidelines, but if an institution or individual does not follow the guidelines, they risk a negative overall risk assessment from the MAS, which can negatively affect their reputation and future endeavors. The TRM guideline states that financial institutions should monitor for cyber threats, participate in information sharing, create an incident response plan, and conduct regular vulnerability assessments and penetration testing as well as cyber exercises and attack simulations (*Technology Risk Management Guideline*, 2021). Financial Institutions are also required to report cyber incidents to the Monetary Authority of Singapore and the Cyber Security Agency of Singapore if they are designated as critical information infrastructure. In addition to the TRM guidelines, the MAS has posted notices for each individual sector and certain institutions within a sector to secure administrative accounts, create baseline security standards, deploy network security devices, implement security patching and anti-malware measures and strengthen user authentication (*Notice FHC-1119 on Cyber Hygiene*, July 2022). Notices, as mentioned earlier, require financial institutions and individuals to comply.

The broad guidelines and notices leave room for financial institutions to implement strategies and practices as they see fit as long as the strategies and practices fulfill the

requirements, which can lead to financial institutions implementing the bare minimum. Financial institutions are not required to report compliance of the Notice to the MAS, but the MAS expects that financial institutions report their compliance to their senior management in which the MAS will review it during the MAS' supervisory process (*FAQ - Notice on Cyber Hygiene*, n.d.). However, because it is only an expectation that financial institutions report their compliance and not a requirement, it is unknown whether financial institutions comply or not with the Notices.

The Ministry of Health strongly encourages healthcare businesses and organizations to follow the Healthcare Cybersecurity Essentials, but it is not required. The Healthcare Cybersecurity Essentials provide only a basic guideline for implementing the bare minimum of cybersecurity measures. The Healthcare Cybersecurity Essentials consist of three steps in which providers can follow in establishing a cybersecurity framework for their organization. First, the organization should create an IT asset inventory of all items connected to the corporate network; second, secure their data, detect, respond to, and recover from breaches; and lastly, implement cybersecurity guidelines into place for each respective organization. In the case of cyber incidents, the MoH directs incident organizations and individuals to report to SingCERT, the CSA's Computer Emergency Response Team, and to the Singapore Police Force if the cyber incident also violates the Computer Misuse Act.

As with guidelines from other sectors such as the financial sector, the Ministry of Health and the Monetary Authority of Singapore do not require organizations to follow the guidelines, which leave room for many organizations to not adhere at all to the guidelines or just establish the bare minimum and not attempt to enhance the cybersecurity measures beyond the bare minimum. However, the financial sector has other cybersecurity regulations in place, more than the sole Healthcare Cybersecurity Essentials from the Ministry of Health that are generalized security measures and not enforced, that leaves the financial sector more secure. Based on these findings, we have to assume that healthcare organizations understand the natural cybersecurity risks that come with being a healthcare provider and already have acceptable cybersecurity measures in place. The healthcare sector will be covered under the Personal Data Protection Act, which will help in securing information and computer systems somewhat, but not to the extensive extent as a proper healthcare cybersecurity regulation.

The Infocomm Media Development Authority (IMDA) has created Codes of Practice based on international standards and best practices such as the ISO / IEC 27011 and IETF Best Current Practices for designated licensees to strengthen their cybersecurity. Currently, only major Internet Service Providers (ISP) including related structures that provide internet services are required to comply with the Codes of Practice. The Codes of Practice consists of requirements to prevent, protect, detect and respond to cyber security threats in which periodic audits are conducted to ensure compliance with the Codes of Practice and identify vulnerabilities organizations currently have in their cybersecurity strategies (*Infocomm Media Cyber Security*, 2021). The cybersecurity Code of Practice includes requirements from other government agencies as well. The IMDA does not state how they enforce or ensure compliance of the Code of Practice.

## Summary and Evaluation

Singapore has one broad national cybersecurity framework with overlapping sectoral regulations that provides an overall effective cybersecurity framework. Sectoral regulations help fill in the gap of the national cybersecurity legislation by covering entities not covered under the CII designation of the Cybersecurity Act that requires critical information owners to implement

adequate cybersecurity measures. Regulations and guidelines have clear jurisdiction even with some overlap, but sectoral regulations can take precedence over the Cybersecurity Act. The Cybersecurity Act establishes the powers of the Commissioner of the Cyber Security Agency and the regulations for CIIs. Sectoral regulations from the Monetary Authority of Singapore and the Infocomm Media Development Authority have some overlap with the Cybersecurity Act because some entities in these sectors are designated as CIIs which require them to report cyber incidents to both the Cyber Security Agency and their respective sectors. Depending on the nature of the cyber incident, the CII will also have to report to the Personal Data Protection Commission and/or the Singapore Police Force. In addition, CIIs in these sectors are required to conduct risk assessments and cybersecurity audits by the CSA but are also recommended by their sector regulators to do the same too.

Between the national cybersecurity framework and sector regulations, there is one major point of concern regarding gaps in regulations. Currently, the Cybersecurity Act applies primarily to critical information infrastructures, so entities not designated as critical information infrastructure are not required to report any cyber incidents, which can potentially lead to the Cyber Security Agency missing a cyber incident that could affect other entities. Furthermore, for entities not designated as critical information infrastructure, they are not required to have cybersecurity strategies in place unless specified by sector regulators which can potentially lead to cyberattacks in which Singapore has seen an increase in attacks in recent years, especially against small-and-medium enterprises in which 2 in 5 are affected, due to the lack of cybersecurity regulations for non-critical information infrastructures, (*CSA | Singapore's Safer Cyberspace Masterplan 2020*, 2020). A 2019 report conducted by the Infocomm Media Development Authority reported that only 42%, a decrease from 52% in 2017, of enterprises adopted cybersecurity measures that mainly consisted of virus checking or protection software and anti-spyware software and out of the 39% of enterprises that engaged in digital investment, 42% invested in cybersecurity software and only 12% invested in cybersecurity training (*Annual Survey On Infocomm Usage By Enterprises For 2019*, 2019). The gap in cybersecurity regulations for non-designated critical information infrastructure is a problem that Singapore is currently facing and addressing in their Singapore's Safer Cyberspace Masterplan 2020, which will be elaborated on further in a later section discussing Singapore's future endeavors.

Singapore is continuously updating and improving their cybersecurity strategies each year to address new and evolving cyberthreats. In recent years, Singapore has recognized the need to protect the cyber supply chain due to an increase in attacks and Singapore's Smart Nation initiative that opens up more opportunities for cyberattacks. The latest large scale supply chain attack was the SolarWind incident in which hackers were able to infiltrate a third-party organization that would install malware on multiple organizations' networks, thus bypassing a single target attack and increasing the scale of attack. To prevent and mitigate cyber supply chain attacks, Singapore has collaborated with Boston Consulting Group to release a Critical Information Infrastructure Supply Chain Programme Paper just this year in July 2022 that would highlight supply chain vulnerabilities and challenges and provide solutions and strategies to address the vulnerabilities and challenges. The Paper outlines five key initiatives: a toolkit that would help CIIOs to assess and rate a vendors cyber supply chain risks; a handbook with various cybersecurity contractual terms that would allow for CIIOs to negotiate the cybersecurity practices of vendors; a certification program CII vendors to meet minimum cybersecurity requirements to improve cybersecurity capabilities of CII vendors; a learning hub for sharing information and training resources; and a platform for international cooperation to discuss with

international agencies and industry groups on cyber supply chain resilience (Critical Information Infrastructure Supply Chain Programme Paper, 2022).

# Relationships

One of Singapore's key strategic pillars is to increase international cybersecurity cooperation, which Singapore is upholding as seen by their various activities such as participation in the ASEAN Computer Capacity Programme and Memoranda of Understandings with multiple countries in the international scene. The private sector also actively participates in consultations with the government on cybersecurity policies and issues and the government also has programs that encourage the private sector to be involved in cybersecurity. Singapore's involvement in international institutions and partnership with the private sector demonstrates Singapore's continuing effort to cybersecurity.

## International Cooperation

As one of founding members of Association of Southeast Asian Nations (ASEAN), Singapore is committed to achieving the ASEAN'S purpose of fostering peace and security in the region and cooperating with each other in cultural, economic, educational, social, technical, and other fields (*The Founding of ASEAN*, n.d.). Recognizing that cyber incidents is an international issue that goes beyond its own borders, Singapore seeks to strengthen cybersecurity coordination across the region and enhance the cyber capabilities of Member States. Singapore demonstrates its commitment to forging its international relations which began during Singapore's chairmanship in 2018 with the establishment of the multi-million dollar ASEAN Cyber Capacity Building Programme to help Member States increase their own cybersecurity capabilities (Tikk & Kerttunen, 2020).

With the support of the ASEAN Member States, Singapore launched the ASEAN Computer Capacity Programme (ACCP) to increase the security of the cyberspace of the region and increase Singapore's ability to respond to emerging cyber threats. The ACCP is now in its third phase called the Cyber Capabilities & Capacity Development Project (C3DP), which expands on the previous phases' work by creating specialized training courses to respond to cyber threats, e-learning courses to obtain electronic evidence, a knowledge base that peers from different regions can access, and experts' groups on emerging cyber threats (*Cyber Capabilities & Capacity Development Project*, n.d.). One of the primary events that occur annually for the ACCP is the Singapore International Cyber Week (SICW) in which industry leaders and experts from ASEAN and the world come together to discuss cybersecurity strategy and policies. The ACCP has conducted more than 30 cybersecurity-related programs that have reached more than 900 senior government officials from ASEAN Member States and beyond (*ASEAN Cyber Capacity Programme (ACCP) - Cybil Portal*, 2021).

The Singapore Cybersecurity Centre of Excellence (ASCCE) is an extension of the ACCP and one function of the ASCCE is to train Computer Emergency Response Teams (CERTs) from the region to respond to cyber threats and promote information sharing among the CERTs of the region (*ASEAN – Singapore Cybersecurity Centre for Excellence (ASCCE) - Cybil Portal*, 2021). Furthermore, the ASCCE collaborates with the ASEAN Member States, their Dialogue Partners, and other international partners that include the United States, Japan,

Australia and others to create cybersecurity capacity building programs (*ASEAN – Singapore Cybersecurity Centre for Excellence (ASCCE) - Cybil Portal*, 2021).

Singapore has also signed Memoranda of Understandings (MoU) with multiple countries that includes Australia, France, the United States, the UK and many others, a Memorandum of Cooperation on cybersecurity with Japan, and a Joint Declaration on cybersecurity cooperation with Germany (Tikk & Kerttunen, 2020). The MoU with the UK in July 2015 covered the agreement to cooperate in four key areas: developing cybersecurity talent, cybersecurity incident response, and a joint research and development collaboration (*Singapore and the UK Commit to Work Together to Ensure a Secure Cyberspace*, 2015). The Memorandum of Cooperation on Cybersecurity with Japan in 2017 focuses on information sharing, collaboration to increase cybersecurity awareness, policy dialogues, and joint regional capacity building efforts (*Singapore Signs Memorandum of Cooperation on Cybersecurity with Japan at the Sidelines of SICW 2017*, 2017). These efforts demonstrate Singapore's commitment in accomplishing the third pillar of their Cyber Security Strategy of 2021 of enhancing their international cooperation (*The Singapore Cybersecurity Strategy 2021,* 2021 October).

## Private Sector

Singapore's private sector is active in the cybersecurity politics of Singapore's government. For instance, key stakeholders such as potential critical information infrastructure owners, government agencies, and cybersecurity experts were consulted by the Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) in closed-door meetings in the drafting of the Cybersecurity Act in 2015. Another round of public consultations occurred in 2017 in which 92 submissions were received by the public and taken under consideration in the revision of the Cybersecurity Act and another in 2021 to the licensing framework of cybersecurity providers under the Cybersecurity Act (*Industry Consultation*, 2022 April). In addition to consultations, Singapore also has a Government Bug Bounty Programme (GBBP) and Vulnerability Disclosure Programme (VDP). Finishing their third round in 2019, the GBBP is a program that monetarily rewards hackers registered with the bug bounty program, HackerOne, who finds any vulnerabilities in Singapore's ICT systems and digital services (*Third Government Bug Bounty Programme Offers Bonus Payouts for Mobile Applications*, 2019). The VDP is a program that encourages voluntary reporting of vulnerabilities found in IT services, systems, resources and/or processes that may affect the access of government applications and give recognition upon validity of the report (*Vulnerability Disclosure Programme*, n.d.). These programs help Singapore identify and address vulnerabilities in their cybersecurity with the help of the public.

## Summary and Evaluation

The Singapore government understands that they must increase their cybersecurity efforts if they want to strive forward with their Smart Nation Initiative. Thus, they have increased their participation in ASEAN and the international community through Memorandum of Understandings with various countries and the hosting of one of the Asia-Pacific region's largest cybersecurity event, the Singapore International Cyber Week, to enhance cybersecurity cooperation, training, response and information sharing with ASEAN Member States, international actors, and cybersecurity experts and stakeholders. It is important to note that ASEAN Member States have varying technological, economic, legislative and policy capacity

and capabilities that make it difficult for some Member States to create a secure cybersecurity environment which makes cooperation challenging, however, Singapore and other ASEAN programs are helping to fund resources to help struggling Member States develop their cybersecurity infrastructure and policy.

In the private sector, the Singapore government has had multiple consultations with key stakeholders of cybersecurity and the public in the drafting of the Cybersecurity Act and other strategies and policies concerning cybersecurity. The CSA had also partnered with TNB Ventures in 2019 to launch a Cybersecurity Industry Call for Innovation that invited industry providers to innovate solutions that addressed specific cybersecurity issues (*CSA and Industry Partners Launch Industry Call for Innovation*, 2018 September). Furthermore, the government-run programs, the Government Bug Bounty Programme and the Vulnerability Disclosure Programme, help foster public-private partnerships by requesting the help of white hat hackers to discover vulnerabilities and encouraging voluntary vulnerability reporting. All these activities demonstrate Singapore's commitment to enhancing their cybersecurity capabilities in the evolving cybersecurity landscape.

## Overall Effectiveness

Singapore has made significant progress and effort in strengthening its cybersecurity capabilities. Singapore's approach to cybersecurity through a unitary organizational structure, broad and sector-specific regulations, and robust international and private sector relationships, have fostered a cybersecurity landscape that is able to continuously evolve to respond to cyberthreats and encourage local and international involvement in cybersecurity that has improved Singapore's overall cybersecurity capabilities.

According to the National Cyber Security Index (NCSI), Singapore ranks 29th in the world in cybersecurity with a score of 71.43 out of 100 (*NCSI: Singapore*, 2021). Singapore began their cybersecurity journey in the early 2000s and have continued to demonstrate dedication to enhancing their cybersecurity. Its transition to a unitary cybersecurity structure ensures that there is minimal jurisdiction overlap between the central cybersecurity agency and other agencies relevant to providing cybersecurity services. Every agency has their own legislation and guidelines that empowers them to act in the case of cyber incidents and even though the jurisdiction may overlap due to the nature of the incident, there is strong cooperation between agencies in the response of an incident.

Regarding legal frameworks, Singapore has a national Cybersecurity Act that mainly protects critical information infrastructure (CII), mandates cyber incident reporting for CII, has a national cybersecurity response plan for large scale cyberattacks, and requires cybersecurity service providers to acquire a license through the CSA before providing any services. Some sectors such as the financial, health, and telecommunications sector, also have their own guidelines and regulations for entities in their sector and in the case of CIIs, mandatory reporting and required cybersecurity strategies in place will overlap with the national framework. Even though Singapore has a strong national and sector-specific frameworks in place, they lack legislation requiring cyber incident reporting and required cybersecurity strategies in place for non-CIIs. As Singapore is transitioning to a Smart Nation and as a leading global financial center, this oversight has led to an increase in cyberattacks against small-and-medium enterprises (SMEs) that has led to disruption of services, lost revenue and loss of trust of the SME from the public due to the cyberattack. Furthermore, it is not expressly stated in the Cybersecurity Act that

SMEs working with CII are required to follow regulations set out for CIIs in the Act, but if the CII does not ensure that the SMEs and contractors they are working with have secure cybersecurity strategies in place, cyber incidents involving the SME or contractor could potentially affect them too.

Singapore is constantly adjusting their legislation and national strategies in response to the evolving cybersecurity landscape. Singapore's Safer Cyberspace Masterplan of 2020 strives to increase the cybersecurity level of individual users, communities, enterprises, and organizations not designated as CII under the Cybersecurity Act by strengthening the cybersecurity of cloud services, creating an internet cyber hygiene portal, raising community awareness of cybersecurity and other initiatives, which will hopefully fill the gap mentioned above (2020). In March 2022, the CSA released a press release for a review of the Cybersecurity Act to address securing the digital infrastructure and services due to increased usage and reliance as Singapore digitalizes and expanding the Act to protect virtual assets and expand to cover digital infrastructure and digital services such as apps (*Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs*, 2022). In addition to the Cybersecurity Act, the CSA will update the Cybersecurity Code of Practice for CIIs that may no longer be sufficient in addressing evolving cyberthreats, particularly large-scale ransomware in addition to sector-specific threats that current generic hygiene practices may not be able to address the cyberthreat (*Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs*, 2022).

Singapore prioritizes their international relationships and private partnerships in which they demonstrate through their active participation in international organizations and agreements with multiple countries and pathways for the private sector to provide feedback on regulations. The private sector, which includes cybersecurity experts, industry leaders, and organizations, have been consulted multiple times during the drafting process of the Cybersecurity Act. Sector leaders and organizations have also been consulted in the drafts of sector regulations. Furthermore, the Vulnerability Disclosure Programme encourages the private sector to report vulnerabilities of ICT systems and digital services to the government and has hosted multiple Government Bug Bounty Programmes for white hackers locally and globally to identify vulnerabilities.

Overall, as an example of a unitary cybersecurity model, Singapore has created a cybersecurity framework that provides, for established and upcoming businesses in Singapore and international agencies and organizations, clear understanding of authority and regulation jurisdictions. Furthermore, the opportunity for the private sector to provide feedback on legislation and regulations and guidelines creates a strong private sector partnership that fosters beneficial collaboration, cooperation, and innovation. Lastly, Singapore has created a secure cybersecurity environment in which Singapore demonstrates extreme dedication to continuously update and introduce new legislation, regulations and guidelines as well as collaborating with local and international partners to address the ever evolving cybersecurity threat landscape.

# Bibliography

## Brazil Sources


(www.deepocean.com.br), D. O. (2021, February 8). *Azevedo Sette Advogados*. News & Recent Work | Azevedo Sette Advogados. Retrieved August 14, 2022, from https://www.azevedosette.com.br/news/en/telecommunications-cybersecurity-recent-developments/6099

2020 Cybersecurity Report: Risks, Progress, and the way forward in Latin America and the Caribbean. (n.d.). Retrieved August 16, 2022, from https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

*About Brazilian insurance market*. SUSEP Superitendência de Seguros Privados. (n.d.). Retrieved August 15, 2022, from http://www.susep.gov.br/menuingles/about_bim

Bank, E. C. (2021, November 18). *Memoranda of understanding*. European Central Bank - Banking supervision. Retrieved August 16, 2022, from https://www.bankingsupervision.europa.eu/legalframework/mous/html/index.en.html

*BNAMERICAS - Brazil's SUSEP publishes resolution for admi...* BNamericas.com. (n.d.). Retrieved August 16, 2022, from https://www.bnamericas.com/en/news/brazils-susep-publishes-resolution-for-administrative-sanctions

*Brazil creates a data protection authority*. Brazil Creates a Data Protection Authority - Hogan Lovells Engage. (n.d.). Retrieved August 15, 2022, from https://www.engage.hoganlovells.com/knowledgeservices/news/brazil-creates-a-data-protection-authority

*Brazil: Freedom on the net 2021 country report*. Freedom House. (n.d.). Retrieved August 14, 2022, from https://freedomhouse.org/country/brazil/freedom-net/2021

*Brazilian Central Bank proposes cybersecurity rule for financial institutions - highlights > banking, insurance and finance*. Machado Meyer. (2017, September 25). Retrieved August 17, 2022, from https://www.machadomeyer.com.br/en/decisions/decisions-banking-insurance-and-finance/brazilian-central-bank-proposes-cybersecurity-rule-for-financial-institutions

*Breaking down the vote on Russia's new cybercrime resolution at the UN*. New America. (2018, November 19). Retrieved August 16, 2022, from https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/breaking-down-vote-russias-new-cybercrime-resolution-un/

BRICS, B. C. (2022, February 21). *Brazil joins the Convention on Cybercrime: How Will It Impact Other BRICS countries?* MediaNama. Retrieved August 17, 2022, from https://www.medianama.com/2022/02/223-brazil-budapest-convention-cybercrime-impact-brics/#:~:text=The%20South%2DAfrican%20example%20is,have%20joined%20the%20Budapest%20Convention.

*CERT.br stats (Janeiro a dezembro de 2015)*. CERT.br. (n.d.). Retrieved August 14, 2022, from https://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.html

Choi, J. (2021, August 8). *Biden envoy told Brazil's Bolsonaro not to undermine elections: Report*. The Hill. Retrieved August 14, 2022, from https://thehill.com/policy/international/americas/566894-biden-envoy-told-brazils-bolsonaro-not-to-undermine-elections/

Council of Europe. (2021, December 15). *Congress of Brazil approves accession to the Budapest Convention*. Cybercrime. Retrieved August 17, 2022, from https://www.coe.int/en/web/cybercrime/-/congress-of-brazil-approves-accession-to-the-budapest-convention

Council on Foreign Relations. (n.d.). *Brazil must rebalance its approach to cybersecurity*. Council on Foreign Relations. Retrieved August 14, 2022, from https://www.cfr.org/blog/brazil-must-rebalance-its-approach-cybersecurity

Council on Foreign Relations. (n.d.). *Brazil-EU cyber cooperation: Swinging bridges on the road to stability in Cyberspace*. Council on Foreign Relations. Retrieved August 16, 2022, from https://www.cfr.org/blog/brazil-eu-cyber-cooperation-swinging-bridges-road-stability-cyberspace

Council on Foreign Relations. (n.d.). *Brazil-EU cyber cooperation: Swinging bridges on the road to stability in Cyberspace*. Council on Foreign Relations. Retrieved August 17, 2022, from https://www.cfr.org/blog/brazil-eu-cyber-cooperation-swinging-bridges-road-stability-cyberspace

Dascalu, G. (2021, July 27). *Brazil establishes Cyberattack Response Network*. softpedia. Retrieved August 16, 2022, from https://news.softpedia.com/news/brazil-establishes-cyberattack-response-network-533572.shtml

*Data Protection and cybersecurity laws in Brazil*. CMS Expert Guide. (n.d.). Retrieved August 16, 2022, from https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/brazil

*Decree n. 9637: Brazilian government guidelines to guarantee the authenticity, confidentiality and integrity of information contained in Federal Administration Networks :: Eu Cyber Direct*. Horizon. (n.d.). Retrieved August 16, 2022, from https://eucyberdirect.eu/atlas/sources/decree-n-9637-brazilian-government-guidelines-to-guarantee-the-authenticity-confidentiality-and-integrity-of-information-contained-in-federal-administration-networks

*GDP (current US$) - latin america & caribbean*. World Bank. (n.d.). Retrieved August 14, 2022, from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=ZJ

International cyber law: interactive toolkit. (2022, April 1). *National Position of Brazil (2021)*. International cyber law: interactive toolkit. Retrieved August 16, 2022, from https://cyberlaw.ccdcoe.org/wiki/National_position_of_Brazil_(2021)

Kujawski, F. F., Sombra, T. L., & Brancher, P. M. R. (2021, October 15). *Cybersecurity Regulation in Brazil: An overview*. Lexology. Retrieved August 15, 2022, from https://www.lexology.com/commentary/tech-data-telecoms-media/brazil/mattos-filho-veiga-filho-marrey-jr-e-quiroga-advogados/cybersecurity-regulation-in-brazil-an-overview#:~:text=Approved%20in%202020%2C%20the%20National,take%20between%202020%20and%202023.

M. Mueller M. van Eeten B. Kuerbis. (2020, April 10). *Brazil's First National Cybersecurity Strategy: An analysis of its past, present and future*. Internet Governance Project. Retrieved August 16, 2022, from https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future/

Mar 03, 2017. (n.d.). *Top 5 countries where cyber attacks originate*. Security Today. Retrieved August 14, 2022, from https://securitytoday.com/Articles/2017/03/03/Top-5-Countries-Where-Cyber-Attacks-Originate.aspx?Page=2

*Most Brazilian companies don't pay to get data back after ransomware attacks*. ZDNet. (n.d.). Retrieved August 17, 2022, from https://www.zdnet.com/article/most-brazilian-companies-dont-pay-to-get-data-back-after-ransomware-attacks/

Nacional, I. (n.d.). *Decreto nº 10.222, de 5 de fevereiro de 2020 - dou - Imprensa Nacional*. DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 - DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 - DOU. Retrieved August 16, 2022, from https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419

NIC.br. (n.d.). *CGI.br Abre Chamada de Contribuições sobre temas da regulamentação do Marco civil da internet*. CGI.br. Retrieved August 16, 2022, from https://marcocivil.cgi.br/

Person. (2021, July 7). *Brazil's Bolsonaro says he may not accept 2022 election under current voting system*. Reuters. Retrieved August 14, 2022, from https://www.reuters.com/world/americas/brazils-bolsonaro-says-may-not-accept-2022-election-under-current-voting-system-2021-07-07/

Pooler, M. (2021, September 15). *Business relations with Brazil's Bolsonaro Fray*. Subscribe to read | Financial Times. Retrieved August 24, 2022, from https://www.ft.com/content/9ac922e9-e1b5-4496-9d7d-a44b779277a2

*Resolution CMN 4,557 of February 23, 2017 provides for the ...* (n.d.). Retrieved August 16, 2022, from https://www.bcb.gov.br/ingles/norms/brprudential/Resolution4557.pdf

*RFC 2350 (English)*. CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. (n.d.). Retrieved August 16, 2022, from https://www.gov.br/ctir/pt-br/assuntos/rfc-2350

*Security spend to reach $1 billion in Brazil in 2022*. ZDNet. (n.d.). Retrieved August 16, 2022, from https://www.zdnet.com/article/security-spend-to-reach-1-billion-in-brazil-in-2022/

*Telecommunications cybersecurity: Recent developments: Article: Chambers and partners*. Article | Chambers and Partners. (n.d.). Retrieved August 16, 2022, from https://chambers.com/articles/telecommunications-cybersecurity-recent-developments

Thomson Reuters. (2020, May 28). *Brazil's Bolsonaro urges Supreme Court to shelve 'fake news' probe*. Reuters. Retrieved August 16, 2022, from https://www.reuters.com/article/us-brazil-politics/brazils-bolsonaro-urges-supreme-court-to-shelve-fake-news-probe-idUSKBN234253

U.S. Department of State. (2020, December 1). *U.S.-Brazil Bilateral Cooperation on Cyber and internet policy - united states department of state*. U.S. Department of State. Retrieved August 17, 2022, from https://2017-2021.state.gov/u-s-brazil-bilateral-cooperation-on-cyber-and-internet-policy/index.html

## Chile Sources

About the State Intelligence System and Creates the National Intelligence Agency, H.R. 19,974 (Oct. 4, 2011). https://www.bcn.cl/leychile/navegar?idNorma=230999

Aldoney, R., Albertz, P., & Alcaíno, E. (2022, June). New Cybercrime Law: Criminal and Compliance Aspects. Retrieved August 23, 2022, from https://www.carey.cl/en/new-cybercrime-law-criminal-and-compliance-aspects/

Amends Supreme Decree No. 533, of 2015, of the Ministry of the Interior and Public Security, Which Creates the Inter-ministerial Committee on Cybersecurity, H.R. Supreme Decree Nº 579 (2020). https://www.bcn.cl/leychile/navegar?idNorma=1140740

Approves Technical Standard on General Foundations of Cybersecurity for the Design, Installation and Operation of Networks and Systems Used for the Provision of Telecommunications Services, H.R. 1318 (Aug., 2020). https://www.bcn.cl/leychile/navegar?idNorma=1148274

Bnamericas. (2015, December). Chile joins Microsoft Government Security Program. Retrieved August 23, 2022, from https://www.bnamericas.com/en/news/chile-joins-microsoft-government-security-program

Bnamericas. (2020, November). Chile unveils cybersecurity plan for mining industry. Retrieved August 24, 2022, from https://www.bnamericas.com/en/news/chile-unveils-cybersecurity-plan-for-mining-industry

Bnamericas. (2021, November). Chile's mining industry strengthens cybersecurity efforts. Retrieved August 24, 2022, from https://www.bnamericas.com/en/news/chiles-mining-industry-strengthens-cybersecurity-efforts

Carey, G., & Mercado, J. I. (2022, March 25). Bill that establishes a Framework Law on Cybersecurity and Critical Information Infrastructure enters Chilean Senate. Carey y Cía. Ltda. Retrieved August 15, 2022, from https://www.carey.cl/en/bill-that-establishes-a-framework-law-on-cybersecurity-and-critical-information-infrastructure-enters-chilean-senate/

Carlos, L. J., & Pablo, V. (2016). Mapping the Cyber Policy Landscape: Chile. https://www.gp-digital.org/wp-content/uploads/2017/02/Mappingthecyberlandscape_chile.pdf

Central Intelligence Agency. (2022, may 11). Chile Country Summary. Retrieved August 15, 2022, from https://www.cia.gov/the-world-factbook/countries/chile/summaries

Computer Security Incident Response Teams. (2021, October 9). Chilean Government CSIRT RFC 2350. Retrieved August 15, 2022, from https://www.csirt.gob.cl/media/2021/10/RFC2350-english.pdf

Consumers International. (2022). National Consumer Service (SERNAC). Retrieved August 23, 2022, from https://www.consumersinternational.org/members/members/servicio-nacional-del-consumidor-sernac/

Convention on Cybercrime. (2022, August). Chart of signatures and ratifications of Treaty 185. Retrieved August 23, 2022, from https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Creates the Financial Analysis Unit and Amends Various Provisions Regarding Money Laundering and Laundering, H.R. 19.913 (Dec., 2003). https://www.bcn.cl/leychile/navegar?idNorma=219119

Creates the Ministry of the Interior and Public Security and the National Service for the Prevention and Rehabilitation of Drug and Alcohol Consumption, and Amends Various Legal Bodies, H.R. 20,502 (Feb. 11, 2011). https://www.bcn.cl/leychile/navegar?idNorma=1140740&idParte=10091351

CSIRT. (n.d.). Cybersecurity decrees. Retrieved August 23, 2022, from https://www.csirt.gob.cl/eng/cybersecurity-decrees/

CSIRT. (2021). Notification Guide Of Incidents. Retrieved August 24, 2022, from https://www.csirt.gob.cl/media/2021/10/Guia-de-notificacion-ciberincidentes.pdf

Cybersecurity in Chile: Ministry signed a collaboration agreement. (2020, June). Retrieved August 23, 2022, from http://newtechmag.net/2020/06/24/cybersecurity-in-chile-ministry-signed-a-collaboration-agreement/

Enacts the Convention on Cybercrime, H.R. 83 (Aug., 2017). https://www.bcn.cl/leychile/navegar?idNorma=1106936

Established Consolidated, Systematized and Agreed Text of the Law General of Banks and Other Legal Bodies Indicated, H.R. 19.978 (1997). https://www.cmfchile.cl/portal/principal/613/articles-27827_doc_pdf.pdf

Establishes a Regime of Limitation of Liability for Holders or Users of Payment Cards and Electronic Transactions in the Event of Loss, Theft, Robbery or Fraud., H.R. 20.009 (May, 2020). https://www.bcn.cl/leychile/navegar?idNorma=236736

Establishes Rules on Computer Crimes, Repeals Law No. 19,223 and Amends Other Legal Bodies in Order to Adapt Them to the Budapest Convention, H.R. 21.459 (June, 2022). https://www.bcn.cl/leychile/navegar?idNorma=1177743&idParte=10343833

Establishes the Principle of Purpose in the Processing of Personal Data, H.R. 20.575 (Feb., 2012). https://www.bcn.cl/leychile/navegar?idNorma=1037366

Facilitates the Reciprocal Exchange of Information With Other Countries, H.R. 21.016 (June, 2017). https://www.bcn.cl/leychile/navegar?idNorma=1104397&idParte=

General Telecommunications Law, H.R. 18,168 (Oct. 2, 1982). https://www.bcn.cl/leychile/navegar?idNorma=29591

GLACY+: Chile focuses on streamlining cybercrime and electronic evidence in the national training strategies for judges and prosecutors. (2020, October). Retrieved August 23, 2022, from https://www.coe.int/en/web/cybercrime/glacyplusactivities/-/asset_publisher/DD9qKA5QlKhC/content/glacy-chile-focuses-on-streamlining-cybercrime-and-electronic-evidence-in-the-national-training-strategies-for-judges-and-prosecutors?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fcybercrime%2Fglacyplusactivities%3Fp_p_id%3D101_INSTANCE_DD9qKA5QlKhC%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1

The Government of Chile, National Cybersecurity Policy, H.R. Rep. (2016). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Chile_NCSP%20%28ENG%29.pdf

Magliona, C., & Araya, C. (2022, March). Cybersecurity 2022. Chambers and Partners. Retrieved August 23, 2022, from https://practiceguides.chambers.com/practice-guides/cybersecurity-2022/chile

Ministry General Secretariat of the Presidency of Chile. (2014). AGENDA DIGITAL 2022. Retrieved August 23, 2022, from http://www.agendadigital.gob.cl/#/

Ministry of Education. (2016, August 4). Oportunidades de la Formación Inicial Docente en la era digital [Opportunities for Initial Teacher Training in the digital age]. Retrieved August 15, 2022, from https://www.mineduc.cl/oportunidades-la-formacion-inicial-docente-la-digital/

Ministry of Foreign Affairs. (2022)a. Dirección de Seguridad Internacional y Humana [International and Human Security Directorate]. Retrieved August 15, 2022, from https://www.minrel.gob.cl/direccion-de-seguridad-internacional-y-humana/minrel_old/2008-08-29/151231.html

Ministry of Foreign Affairs. (2022)b. Principios de la Política Exterior Chilena [Principles of Chilean Foreign Policy]. Retrieved August 15, 2022, from https://www.minrel.gov.cl/minrel_old/site/artic/20080802/pags/20080802194424.html

Ministry of Foreign Affairs. (2017, April). Chile deposits the instrument of accession to the Budapest Convention on Cybercrime. Retrieved August 23, 2022, from https://www.minrel.gov.cl/chile-deposita-el-instrumento-de-adhesion-al-convenio-de-budapest-sobre/minrel_old/2017-04-21/175923.html

National Service for Older Persons. (2021). Guía de orientaciones técnicas del programa Comunas Amigables [Guide of technical orientations of the Friendly Communes program]. Retrieved August 15, 2022, from http://www.senama.gob.cl/storage/docs/Guia_de_orientaciones_tecnicas.pdf

National Standards Institute. (2016). Proceso de Normalización [Normalization Process]. Retrieved August 15, 2022, from https://www.inn.cl/Ensayos-de-Aptitud#dg

NCSI: Chile. (n.d.). Retrieved August 23, 2022, from https://ncsi.ega.ee/country/cl/

NIC Chile. (2020). Reglamentación para el funcionamiento del Registro de Nombres del Dominio .CL [Regulation for the operation of the Registry of Domain Names .CL]. Retrieved August 23, 2022, from https://www.nic.cl/dominios/index.html

On Access to Public Information, H.R. 20.285 (Mar., 2020). https://www.bcn.cl/leychile/navegar?idNorma=276363

On Associations and Citizen Participation in Public Management, H.R. 20.500 (Feb., 2011). https://www.bcn.cl/leychile/navegar?idNorma=1023143

O'Neil, S. K. (2022, January). Latin America's New Economic Model May Emerge in Chile. Council on Foreign Relations. Retrieved August 15, 2022, from https://www.cfr.org/article/latin-americas-new-economic-model-may-emerge-chile

On Protection of Private Life, H.R. 19.628 (Aug., 1999). https://www.bcn.cl/leychile/navegar?idNorma=141599

On Recovery and Continuity in Critical and Emergency Conditions of the Public Telecommunications System, H.R. 20,478 (Dec. 10, 2010). https://www.bcn.cl/leychile/navegar?idNorma=1020622

Osborn, C. (2022, July). Chile Unveils Its Proposed New Constitution. Foreign Policy. https://foreignpolicy.com/2022/07/08/chile-new-constitution-rewrite-boric-protests-pinochet-dictatorship-referendum/

Principle of Network Neutrality for Consumers and Internet Users, H.R. 20.453 (Aug., 2010). https://www.bcn.cl/leychile/navegar?idNorma=1016570

ProChile. (n.d.). Servicios [Services]. Retrieved August 15, 2022, from https://www.prochile.gob.cl/sectores-exportadores/servicios

Rodriguez-Ferrand, G. (2017). Chile: Information Sharing with Other Countries. Retrieved August 23, 2022, from https://www.loc.gov/item/global-legal-monitor/2017-07-11/chile-information-sharing-with-other-countries/

Silva, E. (1997). Business Elites, the State, and Economic Change in Chile. In B. R. Schneider & S. Maxfield (Authors), Business and the State in Developing Countries. Cornell University Press.

Silva, P. (2018, November). Chile: Presidential Instructive On Cybersecurity. Retrieved August 23, 2022, from https://www.mondaq.com/security/751016/presidential-instructive-on-cybersecurity

To the Law Project That Regulates the Protection and Treatment of Personal Data and Creates the Personal Data Protection Agency, H.R. N°046-370 (June 3, 2022). https://www.camara.cl/verDoc.aspx?prmID=30357&prmTIPO=OFICIOPLEY
The World Bank. (2022). GDP (current US$) - Chile. Retrieved August 15, 2022, from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=CL
Velasco, C. (2016), "Jurisdicción y competencia penal en relación al acceso transfronteirizo en materia de ciberdelitos", Monografias, Tirant lo Blanch, Valencia, www.tirant.com/libreria/libro/jurisdiccion-y-competencia-penal-en-relacion-al-acceso-transfronterizo-en-materia-de-ciberdelitos-cristos-velasco-san-martin-9788490869925.

## France Sources

Ahmed Baladi. (2019). *French Implementation of the GDPR*. Practical Law accessed August 2, 2022.
ANSSI (2015, March 31). *CYBERSECURITY AND CYBERDEFENCE TRUST SERVICE PROVIDERS IN FRANCE*. https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/cyberdefence-trusted-service-providers-in-france
ANSSI. (2021, September 8). *Cooperation and solidarity: cybersecurity is being built at* the *European Union level* [Press release]. https://www.ssi.gouv.fr/uploads/2021/09/anssi-press_release-fic_2021.pdf
ANSSI. (n.d.). LE CENTRE DE CYBERDÉFENSE. Retrieved August 18, 2022, from https://www.ssi.gouv.fr/agence/organisation/les-sous-directions/centre-operationnel-de-la-securite-des-systemes-dinformation-cossi/le-centre-de-cyberdefense/
ANSSI. (n.d.). *NIS DIRECTIVE: ANSSI SUPPORTS THE FIRST OPERATORS OF ESSENTIAL SERVICES*. Retrieved August 19, 2022, from https://www.ssi.gouv.fr/en/actualite/nis-directive-anssi-supports-the-first-operators-of-essential-services/
ANSSI. (n.d.). *The French CIIP Framework*. Retrieved August 2, 2022, from https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/
SGDSN. (n.d.). *Au cœur de l'exécutif | Secrétariat général de la défense et de la sécurité nationale*. http://www.sgdsn.gouv.fr. Retrieved August 18, 2022, from http://www.sgdsn.gouv.fr/le-sgdsn/au-coeur-de-lexecutif/
Baumard, P. (2017). *Cybersecurity in France*. Springer International Publishing.
Brangetto, P. (2015). *National Cyber Security Organisation, France*. NATO Cooperative Cyber Defence Centre of Excellence.
Calcara, A., & Marchetti, R. (2021). State-industry relations and cybersecurity governance in Europe. *Review of International Political Economy*, 1-26.
CERT-FR. (n.d.). *À PROPOS DU CERT-FR*. Retrieved July 31, 2022, from https://www.cert.ssi.gouv.fr/a-propos/
CNIL. (n.d.). La CNIL, c'est quoi ? Retrieved July 31, 2022, from https://www.cnil.fr/fr/cnil-direct/question/la-cnil-cest-quoi
*Common Criteria Certification*. (n.d.). ANSSI. Retrieved August 5, 2022, from https://www.ssi.gouv.fr/en/certification/common-criteria-certification/
CSFRS. (n.d.). *Conseil supérieur de la formation et de la recherche stratégiques*. Retrieved August 18, 2022, from https://archive.wikiwix.com/cache/index2.php?url=https%3A%2F%2Fwww.csfrs.fr%2Fsites%2Fdefault%2Ffiles%2Fplaquette_csfrs_2015_0.pdf%2Findex.html#federation=archive.wikiwix.com&tab=url
CyberEdge Group. (2020). *2020 Cyberthreat Defense Report*. https://cyber-edge.com/resources/2020-cyberthreat-defense-report/
Décret n° 2009-834 du 7 juillet 2009 (2009). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212

DLA Piper. (2021, January). *GDPR fines and data breach survey*. https://inform.dlapiper.com/10/5202/uploads/data-breach-report-2021.pdf?intIaContactId=9kI6kGBmIMGlWwjkwq7aLQ%3d%3d&intExternalSystemId=1
French Ministry for Foreign Affairs. (2019). *France and cyber security*. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/
Geostrategia. (n.d.). Qui sommes-nous ? Retrieved August 18, 2022, from https://www.geostrategia.fr/qui/
Hentzen, P. (2021, April 15). *National Strategy for Cybersecurity: the French response*. Stormshield. Retrieved July 31, 2022, from https://www.stormshield.com/news/national-strategy-for-cybersecurity-the-french-response-to-the-threat/
Penal Code. (1992). https://sherloc.unodc.org/cld/uploads/res/document/french_penal_code_html/french_penal_code.pdf
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, OJ L 119, 04.05.2016 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
République Française. (2014) Journal officiel électronique authentifié n° 0258 du 07/11/2014. Journal Officiel de la République Française. Retrieved August 18, 2022, from https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000029716883
Lecomte, F. (2021). *Cybersecurity Laws and Regulations Report 2022 France*. International Comparative Legal Guides International Business Reports. Retrieved August 2, 2022, from https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france
Ministère de l'Interieur. (n.d.). *Bienvenue sur le site du Ministère de l'Interieur*. Retrieved July 31, 2022, from https://www.interieur.gouv.fr/
Ministère des Armées. (n.d.). *Les missions du ministère des Armées*. Retrieved July 31, 2022, from https://www.defense.gouv.fr/ministere/missions-du-ministere-armees
National Cybersecurity Agency of France (ANSSI). (n.d.-a). *Executive office*. Retrieved July 31, 2022, from https://www.ssi.gouv.fr/en/organisation/executive-office/
National Cybersecurity Agency of France (ANSSI). (n.d.). *The National Cybersecurity Agency of France*. Retrieved July 31, 2022, from https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/
Nationale, A. (n.d.). *Welcome to the English website of the French National Assembly*. Welcome to the english website of the French National Assembly - Assemblée nationale. Retrieved July 31, 2022, from https://www2.assemblee-nationale.fr/langues/welcome-to-the-english-website-of-the-french-national-assembly
Navarro, P., le Roux, C., Hassani, S., & Lecordier, G. (2022, March 17). *Cybersecurity 2022 - France | Global Practice Guides | Chambers and Partners*. Chambers and Patners. Retrieved August 19, 2022, from https://practiceguides.chambers.com/practice-guides/cybersecurity-2022/france/trends-and-developments
NCI Agency. (n.d.). *NCI Agency | CIS3 Partnership for CIS Security Standards Development*. NATO Communications and Information Agency. Retrieved August 4, 2022, from https://www.ncia.nato.int/what-we-do/cyber-security/cis3-partnership-for-cis-security-standards-development.html
NCSI: France. (n.d.). National Cyber Security Index. Retrieved August 14, 2022, from https://ncsi.ega.ee/country/fr/
Nussbaum, A. (2021, February 17). *France's Macron Boosts Cyber Security Spending After Attacks - BNN Bloomberg*. BNN Bloomberg. Retrieved August 14, 2022, from https://www.bnnbloomberg.ca/france-s-macron-boosts-cyber-security-spending-after-attacks-1.1564970

O'Driscoll, A. (2022). *France cyber security and cyber crime statistics (2020–2021)*. Comparitech. Retrieved August 5, 2022, from https://www.comparitech.com/blog/information-security/france-cyber-security-statistics/
Terpan, F., & Saurugger, S. (2021). Soft and hard law in times of crisis: budget monitoring, migration and cybersecurity. *West European Politics*, 44(1), 21-48.
World Bank. (n.d.). *GDP (current US$) - France | Data. Data.Worldbank.Org*. Retrieved July 31, 2022, from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=FR

## Lithuania Sources

About RCDC. (2022). National Cyber Security Centre. https://www.nksc.lt/rkgc/en.html
Andrijauskas, R. (2020). Review of Personal Data Protection Supervision in Lithuania in 2019 by the State Data Protection Inspectorate (p. 58) [Review]. Data Protection Inspectorate. https://vdai.lrv.lt/uploads/vdai/documents/files/02_%20REVIEW%20OF%20PERSONAL%20DATA%20PROTECTION%20SUPERVISION%20IN%20LITHUANIA%20IN%202019.pdf
Annual Report of Personal Data Protection Supervision in Lithuania in 2021. (2021). https://vdai.lrv.lt/en/news/annual-report-of-personal-data-protection-supervision-in-lithuania-in-2021
Bada, M., & Weisser Harris, C. (2017). Cybersecurity Capacity Review Republic of Lithuania. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3658453
Beržanskiene, S.-R. (2017, April 4). Data Security and Cybercrime in Lithuania. Lexology. https://www.lexology.com/library/detail.aspx?g=ebb436e8-7b1c-41d7-8f6b-40ceebb1ba81
Cyber Security Council of Lithuania convened for the first time. (2015, July 25). http://l24.lt/en/education/item/81013-cyber-security-council-of-lithuania-convened-for-the-first-time
Cybersecurity and defence exercise underway in Lithuania | The Baltic Word. (2018, October 9). https://balticword.com/cybersecurity-and-defence-exercise-underway-in-lithuania/
Hassan, W. (2018, June 6). GDPR Responsibilities of Controllers and Processors – Dr. Waël Hassan. https://waelhassan.com/gdpr-responsibilities-of-controllers-and-processors/
Jacuch, A. (2021). Comparative Analysis of Cybersecurity Strategies. European Union Strategy and Policies. Polish and Selected Countries Strategies. On-Line Journal Modelling the New Europe, 37, 102–120. https://doi.org/10.24193/OJMNE.2021.37.06
Judson, J. (2019a, July 16). A necessary rise: Lithuania bolsters its cybersecurity, catching the attention of other nations. DefenseNews. https://www.defensenews.com/smr/a-modern-nato/2019/07/15/a-necessary-rise-lithuania-bolsters-its-cybersecurity-catching-the-attention-of-other-nations/
Judson, J. (2019b, July 16). A necessary rise: Lithuania bolsters its cybersecurity, catching the attention of other nations. Defense News. https://www.defensenews.com/smr/a-modern-nato/2019/07/15/a-necessary-rise-lithuania-bolsters-its-cybersecurity-catching-the-attention-of-other-nations/
Key Trends and Statistics of the National Cyber Security Status of Lithuania. (2022). Ministry of National Defence of the Republic of Lithuania. https://www.nksc.lt/doc/en/Key-trends-and-statistics-2021-q1-2022.pdf
Luiijf, E., Žutautaitė, I., & Hämmerli, B. M. (Eds.). (2019). Critical Information Infrastructures Security: 13th International Conference, CRITIS 2018, Kaunas, Lithuania, September 24-26, 2018: Revised Selected Papers. Springer.
National Cyber Incident Management Plan. (2018). Government of the Republis of Lithuania.
National Cyber Security Centre. (2018). Incident management. https://www.ncsc.gov.uk/section/about-ncsc/incident-management
National Cybersecurity Strategy of Lithuania. (n.d.). Retrieved August 13, 2022, from https://www.cyberwiser.eu/sites/default/files/National%20Cybresecurity%20Strategy%20of%20Lithuania%20%282%29.pdf

NATO. (2022, July 1). Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016). NATO. https://www.nato.int/cps/en/natohq/official_texts_133169.htm
NCSI :: Lithuania. (n.d.). Retrieved August 13, 2022, from https://ncsi.ega.ee/country/lt/
Petkevičius, R. (2021, July 14). Regional Cyber Defence Centre officially starts work [Interview]. https://kam.lt/en/regional-cyber-defence-centre-officially-starts-work/
Prime Minister: Lithuania leads the world in cyber security. (2019, January 29). My Government. https://lrv.lt/en/news/prime-minister-lithuania-leads-the-world-in-cyber-security
Republic of Lithuania Law on Cyber Security. (2014). Translated by the Ministry of National Defence. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ceb0e7b291ad11e8aa33fe8f0fea665f
Republic of Lithuania Law on Electronic Communications. (2014). Seimas of the Republic of Lithuania. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/7092f502c43811e5a141fecd4d43d786
Seimas of the Republic of Lithuania. (2011). Republic of Lithuania Law on Management of State Information Resources No XI-1807. https://e-seimas.lrs.lt/portal/legalAct/en/TAD/TAIS.432270
Skvernelis, S., & Karoblis, R. (2018). Resolution on the Approval of the National Cyber Security Strategy. Government of the Republis of Lithuania.
Štitilis, D., Pakutinskas, P., Laurinaitis, M., & Malinauskaitė-van de Castel, I. (2017). A Model for the National Cyber Security Strategy. The Lithuanian Case. Journal of Security and Sustainability Issues, 6(3). https://doi.org/10.9770/jssi.2017.6.3(3)
World Bank. (n.d.). GDP (current US$) - Lithuania | Data. Data.Worldbank.Org. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=LT

## Singapore Sources

Alfred, D., Kin, L. C., & Picklmaier, A. (2021, November 3). Cybersecurity Laws and Regulations Singapore 2022. International Comparative Legal Guides. Retrieved August 23, 2022, from https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/singapore
ASEAN Cyber Capacity Programme (ACCP). (n.d.). Cybil. https://cybilportal.org/projects/asean-cyber-capacity-programme-accp/
ASEAN – Singapore Cybersecurity Centre for Excellence (ASCCE). (n.d.). Cybil. https://cybilportal.org/projects/asean-singapore-cybersecurity-centre-for-excellence-ascce/
Benjamin, A. (2018, October 22). Next Steps for Cyber Norms in ASEAN. RSIS Commentary. Retrieved August 22, 2022, from https://www.rsis.edu.sg/wp-content/uploads/2018/10/CO18174.pdf
Computer Misuse Act 1993. (2020). Singapore Statutes Online. Retrieved August 6, 2022, from https://sso.agc.gov.sg/Act/CMA1993?WholeDoc=1
Critical Information Infrastructure Supply Chain Programme Paper. (2022, July 27). Cyber Security Agency. https://www.csa.gov.sg/-/media/Csa/Documents/Publications/CSA-CII-Supply-Chain-Programme.pdf
CSA and Industry Partners Launch Industry Call for Innovation. (2018, October 18). Cyber Security Agency. Retrieved August 23, 2022, from https://www.csa.gov.sg/news/press-releases/csa-and-industry-partners-launch-industry-call-for-innovation
Cybercrime. (n.d.). Singapore Police Force. Retrieved August 5, 2022, from http://www.police.gov.sg/Advisories/Crime/Cybercrime
Cybersecurity. (n.d.). GovTech. Retrieved August 17, 2022, from https://www.tech.gov.sg/capability-centre-csg
Cybersecurity Act. (2018). Singapore Statutes Online. Retrieved August 8, 2022, from https://sso.agc.gov.sg/Act/CA2018?WholeDoc=1
Cybersecurity Code of Practice for Critical Information Infrastructure. (2022, July 4). Cyber Security Agency. https://www.csa.gov.sg/-/media/Csa/Documents/Legislation_COP/CCoP_Second-Edition.pdf

Cyber Capabilities & Capacity Development Project. (n.d.). Interpol. Retrieved August 15, 2022, from https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Cyber-Capabilities-Capacity-Development-Project
Cyber Security Advisory Panel. (n.d.). Monetary Authority of Singapore. Retrieved August 23, 2022, from https://www.mas.gov.sg/who-we-are/MAS-Advisory-Panels-and-Committees/Cyber-Security-Advisory-Panel
Cyber Security Agency of Singapore. (2016, October 16). Singapore's Cyber Security Strategy 2016. Cyber Security Agency. Retrieved August 9, 2022, from https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy
Cyber Security Agency of Singapore. (2020, October 6). Singapore's Safer Cyberspace Masterplan 2020. Cyber Security Agency. Retrieved August 10, 2022, from https://www.csa.gov.sg/-/media/Csa/Documents/Publications/Safer-Cyberspace-Masterplan-2020.pdf
Cyber Security Vulnerability Reporting (CSVR) Guide. (2021, April). Infocomm Media Development Authority. Retrieved August 23, 2022, from http://www.imda.gov.sg/regulations-and-licensing-listing/cyber-security-vulnerability-reporting--csvr--guide
Data Protection Obligations. (n.d.). Personal Data Protection Commission. Retrieved August 6, 2022, from https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act/Data-Protection-Obligations
FAQ: Cybersecurity Act. (n.d.). Cyber Security Agency. Retrieved August 15, 2022, from https://faqs.csa.gov.sg/CSA/apps/fcd_faqmain.aspx#TOPIC_210883
FAQ - Notice on Cyber Hygiene. (n.d.) Monetary Authority of Singapore. https://www.mas.gov.sg/-/media/MAS/Notices/PDF/FAQ---Notice-on-Cyber-Hygiene.pdf?la=en&hash=57A6DF29D6F73F30CF871883A95C99083241F67F
GDP (current US$) - Singapore. (2021). The World Bank. Retrieved August 16, 2022, from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=SG
Industry Consultation. (2022, April 11). Cyber Security Agency. Retrieved August 15, 2022, from https://www.csa.gov.sg/Legislation/industry-consultation
Infocomm Media Cyber Security. (2021, April 6). Infocomm Media Development Authority. Retrieved August 6, 2022, from http://www.imda.gov.sg/regulations-and-licensing-listing/infocomm-media-cyber-security
Kai, W. Z. (2020, February 20). About CSG@GovTech Medium. Cyber Security Group. https://medium.com/csg-govtech/beginnings-9d0a97025514
Notice FHC-1119 on Cyber Hygiene. (2022, June 29). Monetary Authority of Singapore. Retrieved August 23, 2022, from https://www.mas.gov.sg/regulation/notices/fhc-1119
Organisation Structure. (n.d.). Ministry of Communication and Information. Retrieved August 6, 2022, from https://www.mci.gov.sg/about-us/our-organisation/organisation-structure
Our Organisation. (n.d.). Cyber Security Agency. Retrieved August 5, 2022, from https://www.csa.gov.sg/Who-We-Are/Our-Organisation
Over 1,400 registered for GovTech's first-ever "capture-the-flag" cybersecurity competition. (2021, March 8). https://www.tech.gov.sg/media/technews/capture-the-flag-competition
PDPA Overview. (n.d.). Personal Data Protection Commission. Retrieved August 5, 2022, from https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act
Research and Statistics. (2019) Annual Survey On Infocomm Usage By Enterprises For 2010. Infocomm Media Development Authority. https://www.imda.gov.sg/-/media/imda/files/industry-development/fact-and-figures/infocomm-usage-business/infocomm-usage-survey-public-report-2019.pdf
Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs. (2022, March 4). Cyber Security Agency. Retrieved August 15, 2022, from https://www.csa.gov.sg/News/Press-Releases/review-of-the-cybersecurity-act-and-update-to-the-cybersecurity-code-of-practice-for-ciis

Singapore. (2021, October 18). National Cyber Security Index. Retrieved August 15, 2022, from https://ncsi.ega.ee/country/sg/

Singapore and the UK Commit to Work Together to Ensure a Secure Cyberspace. (2015, July 29). Cyber Security Agency. Retrieved August 23, 2022, from https://www.csa.gov.sg/news/press-releases/singapore-and-the-uk-commit-to-work-together-to-ensure-a-secure-cyberspace

Singapore Signs Memorandum of Cooperation on Cybersecurity with Japan at the Sidelines of SICW 2017. (2017, September 18). Cyber Security Agency. Retrieved August 23, 2022, from https://www.csa.gov.sg/news/press-releases/singapore-signs-memorandum-of-cooperation-on-cybersecurity-with-japan-at-the-sidelines-of-sicw-2017

Supervisory Approach and Regulatory Instruments. (n.d.). Monetary Authority of Singapore. Retrieved August 23, 2022, from https://www.mas.gov.sg/regulation/MAS-Supervisory-Approach-and-Regulatory-Instruments

The Founding of ASEAN. (n.d.). ASEAN. Retrieved August 23, 2022, from https://asean.org/about-asean/the-founding-of-asean/

The Singapore Cybersecurity Strategy 2021. (2021, October 5). Cyber Security Agency. Retrieved August 23, 2022, from https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021

Tikk, E., & Kerttunen, M. (Eds.). (2020). Singapore, ASEAN, and international cybersecurity. Taylor & Francis Group.

Third Government Bug Bounty Programme offers bonus payouts for mobile applications. (2019, November 11). GovTech. https://www.tech.gov.sg/media/media-releases/third-govt-bug-bounty-programme-offers-bonus-payouts-for-mobile-applications

Vulnerability Disclosure Programme. (n.d.). GovTech. Retrieved August 15, 2022, from https://www.tech.gov.sg/report_vulnerability