MASTER THESIS

STRATEGIC ASSESSMENT OF CYBER SECURITY CONTENDERS TO THE BRAZILIAN AGRIBUSINESS IN THE BEEF SECTOR

Virgínia de Melo Dantas Trinks

Brasília, June 2023

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

STRATEGIC ASSESSMENT OF CYBER SECURITY CONTENDERS TO THE BRAZILIAN AGRIBUSINESS IN THE BEEF SECTOR

Virgínia de Melo Dantas Trinks

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Robson de Oliveira Albuquerque ____________________
Presidente

Carlos André de Melo Alves ____________________
Examinador interno

Ana Lucila Sandoval Orozco ____________________
Examinadora externa

Fábio Lúcio Lopes de Mendonça ____________________
Suplente

FICHA CATALOGRÁFICA

TRINKS, VIRGÍNIA DE MELO DANTAS
STRATEGIC ASSESSMENT OF CYBER SECURITY CONTENDERS TO THE BRAZILIAN AGRIBUSINESS IN THE BEEF SECTOR [Distrito Federal] 2023.
xvi, publicação: PPEE.MP.041, 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Agribusiness	2. Cyber Security
3. Cyber Threat Intelligence	4. Threat Analysis
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

TRINKS, V. M. D. (2023). *STRATEGIC ASSESSMENT OF CYBER SECURITY CONTENDERS TO THE BRAZILIAN AGRIBUSINESS IN THE BEEF SECTOR* . Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, publicação: PPEE.MP.041

CESSÃO DE DIREITOS

AUTOR: Virgínia de Melo Dantas Trinks
TÍTULO: STRATEGIC ASSESSMENT OF CYBER SECURITY CONTENDERS TO
THE BRAZILIAN AGRIBUSINESS IN THE BEEF SECTOR .
GRAU: Mestre em Engenharia Elétrica ANO: 2023

Virgínia de Melo Dantas Trinks
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATION

I dedicate this work to all working mothers to reaffirm our strength and tenacity to pursue our goals, here represented by my fierce grandmothers Maria Dulce Dantas and Anailde de Freitas Melo.

ACKNOWLEDGEMENTS

First of all, I thank my family, who enabled me for this achievement.

I would like to thank professors Robson de Oliveira Albuquerque and Rafael Rabelo Nunes, for their guidance, dedication, patience and support, without which this work would not have been possible. Above all for their courage to face new research endeavors with open minds and hearts.

I am grateful to have had the companion of my fellow researchers from Programa de Pós-graduação em Engenharia Elétrica (PPEE), it was an honour to share doubts, hopes and achievements and to be ale to count on your support, here represented by João Pincovscy and Alexandre Pasiani.

A sincere appreciation and love to my parents, Tarcísio Bezerra Dantas and Edailna Maria de Melo Dantas, whose inspiring history aligned with resilient faith and confidence in their kids talents made this possible.

A heartfelt acknowledgement to my brothers, Diogo Luis de Melo Dantas and Thiago Luis de Melo Dantas, whose talents were a never-ending source of inspiration and whose undying sense of camaraderie motivated me to become a better person, student and professional.

My deep love to my dear husband, Maickel Josué Trinks, and to my three baby boys, Miguel, Noah and Theo, you are the true drive and impetus for anything I create.

Finally, I wish to thank the University of Brasília and the PPEE and its staff, for their exceptional quality, and support.

ABSTRACT

Current world commercial structure places Brazilian Agribusiness at constant conflict to protect its interests before other nations in the global market. Technological innovations are used in all stages from the simplest production tasks, up to the design of negotiation tactics at high-level affairs. This paper has the objective of identifying main State contenders against Brazilian beef in the international arena. To reach such a list, a review of the literature on Threat and Cyber Threat Intelligence is presented, followed by a background presentation of how embedded technology is in nowadays agriculture and supply chains in general, and the real necessity for those sectors to be seen as critical infrastructure by governments in general. Also as background information recent cyber attack cases and attacker countries are shown. A Step-by-Step multidisciplinary method is presented that involves the extent of international trade, the interest on specific markets, and the intersection of country cyber capacity index. After applying the method and criteria, it generated a list of five contender countries to the Brazilian Beef in the International Market that hold cyber attack capacities. The list includes the USA, Australia, China, Netherlands and Russia. The method may be replicated and/or applied, considering adequate data source assessment and following specifics of each sector.

Keywords: Agribusiness, Beef Sector, Cyber Security, Cyber Threat Intelligence, Threat Analysis.

RESUMO

A atual estrutura comercial mundial coloca o Agronegócio brasileiro em constante conflito para proteger seus interesses perante outras nações no mercado global. As inovações tecnológicas são utilizadas em todas as etapas, desde as tarefas de produção mais simples até o desenho de táticas de negociação em assuntos de alto nível. Este trabalho tem como objetivo identificar os principais concorrentes brasileiros no mercado de carne bovina na arena internacional. Para chegar a tal lista, é apresentada uma revisão da literatura sobre Inteligência de Ameaças e Ameaças Cibernéticas, seguida de uma apresentação dos antecedentes de como a tecnologia embarcada está hoje na agricultura e nas cadeias de suprimentos em geral, e a real necessidade desses setores serem vistos como infra-estrutura crítica pelos governos em geral. Também como informações básicas, casos recentes de ataques cibernéticos e países atacantes são mostrados. É apresentado um método multidisciplinar passo a passo que envolve a extensão do comércio internacional, o interesse em mercados específicos e a interseção do índice de capacidade cibernética do país. Após a aplicação do método e dos critérios geramos uma lista de cinco países que competem contra a carne bovina brasileira no mercado internacional e que detêm capacidades de ataques cibernéticos, a lista inclui os EUA, Austrália, China, Países Baixos e Rússia. O método pode ser replicado ou aplicado, considerando a avaliação adequada da fonte de dados e seguindo as especificidades de cada setor.

Palavras-chave: Agronegócio, Setor de Carne bovina, Segurança Cibernética, Inteligência de Ameaças Cibernéticas, Análise de Ameaças.

Título: AVALIAÇÃO ESTRATÉGICA DE CONCORRENTES DE SEGURANÇA CIBERNÉTICA AO AGRONEGÓCIO BRASILEIRO NO SETOR DE CARNE BOVINA

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

General Acronyms

CI	Critical Infrastructure
CICARNE	Centro de Inteligência da Carne Bovina
CISA	Cyber security and Infrastructure Security
CSRI	Centre for Cyber Security Research and Innovation
CTI	Cyber Threat Intelligence
DBIR	Data Breach Investigations Report
DOJ	The Justice Department
DP	Gross Domestic Product
Embrapa	Empresa Brasileira de Pesquisa Agropecuária
ENISA	The European Union Agency for Cybersecutirty
EU	European Union
GSI/PR	Institutional Security Office of the Presidency of the Republic
ISO	International Organization for Standardization ISO
IT	Information Technology
ITC	International Trade Centre
ITU	International Telecommunication Union
KRITIS	Betreiber Kritischer Infrastrukturen
NCPI	National Cyber Power Index
NEI	National Economic Intelligence
OECD	Organisation for Economic Co-operation and Development
OSINT	Open Source Intelligence
SaaS	Software-as-a-Service
TISN	Trusted Information Sharing Network
UK	United Kingdom
USA	United States of America
USAHerds	Animal Health Emergency Reporting Diagnostic System

1 INTRODUCTION

Currently the world is facing the changes brought by the fast development of technology. Agribusiness, despite usually being located in more remote areas and being perceived as less prone to fast changes, is rapidly catching up to the advantages and challenges that the data and automation filled technology brings to the supply chains, commerce, industry, consumers, crime, society, etc. As globally available information doubles every two years, technology outcomes are proving to be increasingly more efficient than human analysts, even before artificial intelligence kicks in. For example, machines can identify Chinese missile sites on satellite images more quickly than human analysts.

According to Goel [1], "the Internet has become a potent tool for influencing geopolitical conflicts, including interference in internal affairs of other nations, undermining national security, destabilizing financial infrastructure, and attacks on critical infrastructure". Barara also tells us that today most command and control systems are connected to the Global Information Grid (GIG) or have embedded computer chips [2].

The 2022 Verizon Data Breach Investigations Report (DBIR) informs that Latin American businesses are facing cyber attacks targeting the functioning of their businesses, such as Ransomware and Denial of Service attacks, as everywhere else in the world. The interesting point being that the vast majority of the attacks are done by financially motivated actors that continue to be the main threat actors in this region [3].

In this context, it is no longer an overstatement to say that "today's critical information infrastructure networks are key targets for cyber attack because they have grown to the point where they run the command and control systems, manage the logistics, enable the staff planning and operations, and are the backbone of the intelligence capabilities"(2).

In this dissertation, Agribusiness is the industry chosen to present this cross-reference study due to the wide economic influence it holds in Brazil and because of its inter-sector relationships to critical infrastructure and food safety and security. More specifically the sector with Agribusiness chosen is the international exportation of beef. The performance of this sector has been highlighted as a critical component of the economic development of regions where agribusiness has a considerable share in economic activity [4].

Keeping those necessities in mind, we intertwine the two realities of Contemporary cyber connected productive sector to the need to ensure the protection of such sector‘s interests in the Cyber Space to safeguard the country‘s commercial interests. The Beef Sector was chosen as main focus to produce a case study methodology where we propose a holistic and pragmatic approach of cyber security issues that take into consideration the protection of critical commercial sectors to Brazil and that are likely to be contemporary targets due to their format, conduct, and supply-chain operations.

This thesis takes International Relations and Economic foundations to understand and pull contenders of the beef market world wide. With that information we use data analyses tactics to cross-reference interests of rival States to Brazil on the beef sector all according to International Relations principles versus operational threat intelligence information and capacities of such States. The focus is to produce relevant information and a methodology that may be replicated in other markets and sectors of Brazilian Agribusiness. All to produce pragmatic information that will forge intelligence to threat hunters and decision makers. We believe that this interdisciplinary approach is more realistic to nowadays societal demands because it will generate information and data that could base future research endeavors.

The cross-reference of economic interests of rival States to Brazil on specific product market according to International Relations principles versus operational threat intelligence information and capacities of such States is based on State Economic Intelligence (SEI) principles as stated by de Souza [5]. NEI is a term that embraces State Intelligence for the purpose of economic development, which is consistent with a set of coordinated actions for the search, treatment, dissemination and protection of information useful to different economic actors with the effective employment of Intelligence Services for economic purposes [5].

This dissertation presents a methodology that reduces the term of NEI to include cyber defense in order to produce structured information on Brazilian Key markets and products that may be targeted in the cyber commercial warfare of nowadays. By doing such, it proposes an understanding to the topic that is able to correlate different subject matters that are knotted in today‘s social-economic reality. Comprehending theses connections might be key to determine the future of relevant intelligence making. The increasing prominence of cyber warfare suggests that States and countries are aware of the issues at stake. However, it is unclear to what extent intelligence creation is directly engaging with government policy in this area.

1.1 RELEVANCE OF AGRIBUSINESS TO BRAZILIAN SOCIETY

Agribusiness is essential in today's global economy for public and private sectors. It is a complex sector that holds interests from diverse players. Similar to other global players of this sector, Brazil's Agribusiness is core for the country's Gross Domestic Product (GDP). In Brazil, Agribusiness is responsible for more than 20% of the country's GDP; close to one third of its employment; and almost 40% of its exports. Globally, Agribusiness represents 10% of consumer spending. Such market holds interests of players that range from powerful governments through large corporations and small building societies [6].

Agribusiness is the central generator of foreign exchange with a positive trade balance in Brazilian economy. Because it is able to establish connection amongst agriculture, industry, and services. there is no denying that the development of agribusiness is highly relevant to the process of Brazilian economic development and to advance economic policies [4].

Historically Agribusiness has played a key role in the development of the Brazilian economy. Brazil's economic upturns were around its mains export products so there were the cycles of coffee, cattle, sugarcane, sugar, rubber, cocoa, and others to prove of this industry's economic and social importance. The availability of vast natural resources in Brazil aligned with the size of Brazilian territory of 880,000,000 hectares, of which 388,000,000 is arable, and 90,000,000 has yet to be explored confirm The country's economic tradition in agribusiness that should continue in the future [4].

Those conditions are also pushed by the evolving trend of global growth in food demand. Such circumstances settle an ever positive scenario for Brazilian agribusiness. Making it an economic industry of vital importance to Brazil.

> *"It [Agribusiness] is responsible for a significant share of job creation, positively supports the balance of trade with the strength and magnitude of its exports, and substantially influences the composition of Brazilian GDP."[4]*

The Covid-19 pandemic has brought light to the debate on the maintenance of food safety and security to ensure food and nutritional security of families, during the pandemic, more than half of the consulted Brazilian households faced a situation of food insecurity [7]. That creates contrasts in one of the biggest food exporters in the world.

> *"Brazilian Agribusiness needs to reconcile the interests of producers, in order to guarantee the maintenance of the performance of agribusiness, assuming its leading role in contributing to the Brazilian economy, in terms of generating income and employment; as well as carrying out public policies that provide Brazilian families with enough income to guarantee food security, calibrated according to the evolution of the cost of living and the degree of unemployment and/or underemployment."[7]*

Machado [7] suggests that the formation of public reserve stocks as a viable solution as long as they are compatible with the economic sustainability of production. He also cites agricultural policy instruments that might ease adequate food access, such as the Food Acquisition Program (PAA), the National School Meals Program (PNAE). However Brazilian decision makers direct their attention, effective policies in this area need bulk investments and demand agility in decision-making over availability of resources and logistical efficiency.

Hence, The critical relevance of the agribusiness market to Brazilian economy is notorious and undeniable. Positively, it brings to the table the immediate need to face the protection of commercial interests of specific markets as strategic to the country‘s intelligence, policy makers and decision making processes. So much so that the government should be facing the protection of certain key markets closely in order to ensure the protection of the Country‘s commercial interests in the long run. For example, it has been noted that

> *"Foreign direct investment in agricultural land may contribute to a shift in the aim of Brazilian food policies toward commodities of higher market value instead of the ones essential to local production and also the concentration of these valuable products which may threaten the food security of this society"[8]*

Agricultural foreign direct investment has shown to have an influence on the depth of the food deficit, the arable land, employment in agriculture, and food, crop and livestock productions. On that note, a strategic approach to risk assessment of Brazilian beef production chain is necessary to expose threats and vulnerabilities and protect the interest of the Brazilian product in the global market. Impact assessments can be used to calculate the level of risk to these assets, from which appropriate remediation Steps should follow [9]. Producers should have instructive policies that support their efforts to increase their competitive advantage and decrease risks when having a sustainable production line.

1.2 MOTIVATION

Cyber Security issues come as a front that must be tackled urgently. Countries should be aware that commercial and state level interests are taken into consideration in today‘s new era of commercial intelligence gathering and state interests protections. This is not to say that universal approaches to the issue should be dismissed or not considered, it is quite the opposite. States must understand strategic sectors and interest to protect them accordingly until a more trustworthy and stable universal policy is reached in the cyber crimes and information and privacy protection are reached in the world. Until then, it is essential that governments understand what sectors, information, data, etc should be determined as material do be protected.

In general, the strategic position of Brazilian Agribusiness within the formation of the country‘s wealth and well-being is in contrast to the little care given to its security by Brazilian Policy makers. In today‘s society, which is interconnected by technology and bound to commercial and marketing interests, the protection of the Brazilian Agribusiness activities should be taken as first priority by our government and our society. After all, this industry is not only source of great wealth today, but also holds enormous potential in the near future, especially if we are able to adapt to modern sustainable production means. Finally, this industry speaks to food safety and guarantee which are a common concern to governments from everywhere nowadays.

The most unpretentious role of Threat Hunt is to produce reliable information for decision and policy makers. The aim of this thesis was to raise the need to understand possible cyber threats considering regimens other than the Information Technological capacities alone. The influence of a range of factors from different sciences must be considered when defining a possible threat actor all to reach a full and comprehensive conclusion amid today‘s cyber reality.

In this context, I propose an analysis of possible contenders that are interested in the world beef market and that hold capacities to act in the cyber world in favor of their interest. Pragmatically, let us convey that an action might occur even if that happens in the shade of lawfulness and against Brazilian interests, all based on the true defense of commercial needs.

1.3 OBJECTIVES

The main objective is to identify main State contenders against Brazilian beef in the international arena. We present a model to assess threat analysis of potential contenders and improve threat mitigation through the diagnosis of potential threat actors and their intent. To reach such Objective we followed a thread of a few specific ones:

- List what factors may be taken into consideration when searching for contenders on a specific Agribusiness market;
- Create a model to assess the listed factors;
- Study recent cases to construe cyber threat analysis accordingly;
- Produce a threat analysis of potential contenders considering cyber interests and capacities;and
- identify and assess main State contenders against Brazilian beef in the international arena.

In summon, this work will focus on the identification of main State contenders against Brazilian beef in the international arena and assessment of their cyber attack capabilities according to previous cyber attacks and other known and studied attacks against similar supply chains.

1.4 RESEARCH CONTRIBUTIONS AND LIMITATIONS

The main contribution of this reasearch work was the formulation and proposal of a methodology of strategic assessment that addresses Cyber capabilities and economic interests of states on a specific world commodity, with focus on creating an analytical scheme that interfaces economic and political interests against cyber attack capabilities and intent, to introduce an analysis interface that target both academic and corporate issues through Cyber Threat Intelligence (CTI) perspecitve.

The methodology was submitted to peer review process for assessment by independent experts whom judged the validity, significance, and originality of the work. In consequence, an article was published by a journal under the following information: TRINKS, Virgínia de Melo Dantas et al. Strategic Assessment of Cyber Security Contenders to the Brazilian Agribusiness in the Beef Sector. Information, v. 13, n. 9, p. 431, 2022.

Finally, as a limitation, this dissertation is not intended to present a risk assessment nor a risk evaluation model as that would require a specific line of research and the strategic assessment of its own with characteristic scenarios, definitions for risk levels and mitigation proposals. It is, however, a context study that an ex ante stage for a risk assessment.

1.5 OUTLINE

The organization of this dissertation is arranged in a manner to facilitate understanding and to present concepts before they are put to practice. The introduction section provides the context of our work while presenting the main goals and limitations. Besides this introduction, this thesis is divided as follows: Chapter 2 explores important background concepts concerning Food supply chains the impact of technology in Agribusiness nowadays, including Brazilian Beef Production Chain and its relation to technology and it demonstrates related works in the threat intelligence area that are crucial for understanding our research; chapter 3 presents recent cases of cyber attacks against agribusiness sector and supply chain providers; Chapter 4 presents the methodology design; Chapter 5 presents how the methodology was put to work in accordance to the concepts presented in the previous sections in order to reach the proposed objective; Finally, Chapter 6 exposes the results of the countries that have potential to act in the cyber world against the Brazilian Beef Production Chain, that may support other relevant assessment for intelligence gathering on potential risks, actors. In the conclusion, there is an analysis of how the results match contemporary concerns over cyber security even in a traditional sector as agriculture and the possibilities of future works related to this issue.

2 RELATED WORKS AND BACKGROUND

To understand contemporary food supply chain structure it is necessary to consider different knowledge areas, first we examine country regulations on infrastructure and their varied definitions, then we bring forth specific studies about the beef sector world market today. For the cyber security analysis part of this work there is a need to understand how the technological an innovative sectors are influencing the beef sector. Finally, we present how today‘s intelligence creation and presentation is of relevance for the maintenance and security of a stable production chain cycle.

Hence, to appropriately assess cyber Security issues in the agribusiness sector we present definitions and principles in Related Works from Threat Intelligence (TI) and Cyber Threat Intelligence (CTI). Finally, to adequately assess any findings, it is necessary to understand Countries with cyber attack capabilities and their targets considering trends in the cyber security sector and previous cases presented here as Related Work.

We conducted a refined review of works about agribusiness and CTI and we did not manage to find prior study that connects the elements presented here in a way to intersect CTI and possible contenders against Brazilian products on the beef agribusiness specific economic sector.

2.1 CONTEMPORARY FOOD SUPPLY REGULATORY CONTEXT

Demand for food is growing at the same time the supply faces constraints in land and farming inputs. The world’s population is on track to reach USD 9.7 billion by 2050, requiring a corresponding 70% increase in calories available for consumption, even as the cost of the inputs needed to generate those calories is rising. Prediction shows that by 2030, the water supply is likely to fall 40% short of meeting global water needs, and rising energy, labor, and nutrient costs are already pressuring profit margins. About one-quarter of arable land is degraded and needs significant restoration before it can again sustain crops at scale.

Environmental pressures are on the rise, also due to climate change and the economic impact of catastrophic weather events. Increasing social pressures highlights the push for more ethical and sustainable farm practices, such as higher standards for farm-animal welfare and reduced use of chemicals and water [10].

All the issues mentioned create a context prone to the increase in price and the complication of production challenges in the food sector, hence the use of technology in the area is likely to guide and ease producers adaptation to a new world. Countries need to prepare for the upcoming circumstances surrounding food production, especially large exporters that are economically dependent on their food commodities revenues, such as Brazil. It is necessary to ensure productivity and reduce food scarcity that might even cause civil unrest and societal tumult.

After the 9/11 attacks, USA updated its definition of Critical Infrastructure (CI) as to include *"Systems and assets, whether physical or virtual, so vital to the USA that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters"* [11]. According to Ossevorth et al. [12]:

> *"In this context resilience, which is defined as the resistance of a system to external effects, is required. A field that is indeed part of the critical infrastructure, but which has not been considered as intensively as the energy sector, is food production."*

In the USA, the Cyber security and Infrastructure Security Agency (CISA) [13] understands that, amongst others, the Food and Agriculture Sector is one of the infrastructures that need protection under federal regulation. The regulation also recognizes that each infrastructure sector possesses its unique characteristics and operating models. Finally, it is highlighted which sectors hold dependencies with the Food and Agriculture Sector.

In Brazil, CI was defined by decrees nº 10.569, 2020 [14], and no. 6.703, 2008 [15], as strategic facilities, services and goods whose interruption or destruction will cause a serious social, economic, political, international or national security impact, in particular in the sectors of energy, transport, water and telecommunications. Therefore the decrees state that those facilities need security measures capable of guaranteeing their integrity and functioning. All to mean that physical and operational security need to be known and monitored in order to ensure the provision of those essential services.

As the world faces a rapidly changing environment, CI plays an ever-more important role in maintaining the reliable delivery of essential services. In Brazil, the increasing significance of CI is leading to growing awareness of its importance for safeguarding essential services for citizens and businesses alike. As such, understanding how Brazil's approach to CI affects the food sector should be an attraction point for policy makers, business leaders, and other stakeholders.

Existing regulation for protecting essential services and its security measures are key to ensure these services remain available. Also, it is important to understand the role of technology in helping producers prepare for imminent changes in their operating models and what this means for the food sector going forward.

Here it is relevant to understand the terminology of essential services that is used in many of the CI definitions world wide to determine what is in fact important ans basic for a Country to maintain stability, some examples of those sectors may be food, water, healthcare, electricity, communications, transportation and banking. The rationale is that without these services, social cohesion, economic prosperity and public safety are threatened.

Agriculture, food production or protection of commodities or commercial interests are not mentioned in any of those federal regulations, even though Brazilian legislation provides for cooperation in protecting national CI, by monitoring threats related to acts of sabotage that might threaten the functioning of those strategic facilities.

In Europe, OECD classifies six sectors as CI: information and communication technologies, energy, finance, health, transport and water [16]. Food supply appears in a second group of sectors that includes government, chemical industry, or public safety, for about half of the countries.

In Canada, the National Strategy for Critical Infrastructure [17] establishes a collaborative, federal-provincial-territorial and private sector approach built around partnerships, risk management and information sharing and protection. The central idea is that the National Strategy may give coherent and complementary approach to the ten chosen sectors in order to strengthen resiliency across jurisdictions, food supply is considered one of those sectors.

In Japan, the National Strategy for Critical Infrastructure Protection [18] admits that there is suspicion of the involvement of national governments in targeted attacks aimed at stealing secret information such as trade secrets and that cyber attacks against Japan involving the participation of foreign governments could occur, therefore that country's regulation affirms that there are also fears of attacks on one point in a global supply chain. In this context, even though food is not nominated as a CI by Japanese authorities, that Country is aware of the necessity of protecting basic supply chains.

In Australia, The Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience was established by the Australian Government in 2003. The TISN provides national level forums for owners and operators of CI to develop strategies and solutions to mitigate risk in the following sectors: Energy, Water, Communications, Banking and Finance, Health, Transport, and Food. [16].

OECD whitepaper considers that the list of critical sectors can evolve over time to address emerging vulnerabilities and evolving risks and that has lead to differences in categorisation across countries. [16]

> "The aim of defining critical infrastructure is to target sectors that are most crucial to societal and economic security and stability. Along with the definitions, lists of sectors also vary across countries... Some countries have a large number of critical infrastructure sectors, like the United States with 16 different sectors. Other countries can limit their critical infrastructure policy to two sectors only, such as Portugal, with only electricity and transportation considered as critical infrastructure sectors as per the provisions of the 2008 Directive of the European Council on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection."

The general understanding of public and private stakeholders is that there are major benefits to specifying CI in order to set up platforms for information sharing among policy makers and owners and operators of critical infrastructure. Also it has become necessary to establish Business-government partnerships that encourage the private sector to address mutual interests, such as business continuity and resilience. the objetives are to create an ambience favorable to resilient, identifiable and well developed CI that have a deep level of understanding of its risks, threats and vulnerabilities.

In recent years, many countries have made massive investments in CI to ensure the effective functioning of essential services. Improving CI's security is crucial in providing essential services while keeping citizens away from harm and economic stagnation. In order to increase safety levels, countries must be aware of the risks imposed by both physical and cyber-attacks on such infrastructures and prepare themselves to face these challenges. Hence, the matter to manage food production and supply risk management, connecting with the current worldwide context of geopolitical tensions, climate change, global pandemics, and economic interests is of utmost importance to all Countries world wide.

It is necessary for countries to approach concepts such as cybersecurity, regulatory frameworks and public-private partnership arrangements in order to protect their food sector from disruptions that can cause severe damage both economically and socially.

2.2 THE BEEF SECTOR

The cattle beef agribusiness chain reached a value of almost USD 40 billions, which account for 15.98% of the Brazilian agribusiness Gross Domestic Product (GDP) and around 3.64% of the national GDP. If one takes into account only cattle beef participation in Brazilian GDP, there was an increase from 8.4% to 10% percent in 2020 if compared with 2019. That demonstrates the primary function of the sector for the

Brazilian economy [19].

At the same time, Brazil has registered an 8% increase in cattle beef exports. Of the total beef produced, 73.93% were destined for the domestic market, and the remaining were destined for exports. Of the total exported, there was an increase of 9.8% in the volume of fresh beef; such increase was due to the expansion in the volume of meat destined for already consolidated markets and to the rise of destination countries, which went from 154 to 157 countries. It is necessary to emphasize the 127% increase of volume exported from Brazil to China in the period of 2021 [19].

All those numbers to prove that livestock has considerable relevance in Brazilian economy. Beef production is increasing in Brazil, and its exports have reached record levels since 2018, which favors the trade balance, and it allowing for the advancement of the continuous development of the sector. Brazil is the main beef exporter in the world in terms of tons [20]. Exports from the meatpacking sector contribute to a surplus in the country's trade balance, collecting foreign currency, even with the existence of commercial and operational barriers that can make the process of exporting meat to foreign markets difficult. It is important to mention that competitiveness in international trade involves production volume, supply, production cost, product quality and export logistics.

The Brazilian livestock sector can be considered as privileged by the large territorial extensions, and the favorable climate for cattle breeding both leading to a lower production cost than in other regions. This positive storm of characteristics generate attractive prices of Brazilian beef in international market, and they increase the country's competitive advantages, all according to Albuquerque et al [20]. Because of these favorable aspects, Brazil occupies the first position in the number of herds, with more than 217 million heads of cattle, followed by India, with 190 million.

Brazil has been the largest exporter of beef in the world since 2017, surpassing its competitors India and Australia by at least 400,000 metric tons carcass weight equivalent (CWE) every year. In 2019, Brazil exported 2.3 million tons, accounting for over 21% of total global beef exports. The U.S. Department of Agriculture (USDA) estimated that Brazil would reach 23% of the world's total beef exports, by 2028 [21].

Main importers of fresh beef in 2019 were China, Hong Kong, Egypt, and Chile, which accounted for a combined 63 percent of fresh beef from Brazil. The key importers of prepared or preserved meat, like corned beef, are the U.S. and the European Union (EU), together importing 72 percent of processed beef exports from Brazil [21].

Ribeiro et all [22] argues that, despite internal and external pressure from sanitary issues on farms and in exporter cold storages, and others of political nature, Brazil has a consolidated beef export market, which is strong and resistant to exogenous shocks in either the domestic market or from abroad. Meaning that its leadership is consolidated and tends to provide quality beef to all economic blocs. Baked up by the country structural conditions to become the world's main animal protein supplier.

According to the Organisation for Economic Co-operation and Development (OECD), meat exports are concentrated, and the combined share of the three largest meat exporters – Brazil, the European Union, and the United States – is projected to remain stable and account for around 60% of global world meat exports until 2030. Brazil, which is the largest exporter of poultry meat, will become the largest beef exporter with a 22% market share by then. Meat trade in value is dominated by beef and veal, but increasingly dominated by poultry in quantity [23]. All those points to express the importance of the beef supply chain and export revenue to Brazilian economy, food supply and society.

Malafaia et all [24] demonstrated that since the 1990s the Brazilian beef cattle supply chain has undergone a technological modernisation in its production and organisation systems, resulting in higher productivity, better meat quality and improvement on competitiveness. All due to "the country's favourable climatic conditions, availability of land at low prices, adequate labour supply and production technology adapted to a tropical country."The author supported the idea that livestock production model in Brazil has prioritised more capital-intensive technologies with better technical and economic performances since then. This change was brought by:

- Integrated production systems;
- New forages;
- Genetic improvement of the herd;
- Management and recovery of pastures;
- Feed supplmentation;
- Good producion practices; and
- Calf early producion.

Malafaia et all [24] also argued that Brazil is expected to be a major exporter of meat and probably animal genetics, specialised and with added value, also that arguments to describe agribusiness scenarios should include a myriad of key components among them we mention risk management, economic consequences, production expansion, climate change impacts, land use, and the effects of diverse periods. Malafaia et all identified 10 megatrends for the Brazilian beef cattle supply chain by 2040, megatrend number 8 admits digital technology that transforms the entire supply chain among those.

On the other hand, adverse impacts of the cattle supply chain on the environment forces the Brazilian beef industry to evolve to more sustainable production cycle. The market increasingly recognizes sustainability risks, that might be translated into material financial implications in the long run. Major consumer markets are tightening regulations to reflect concerns over environmental and social impacts of international commodity supply chains [21]. Producers need to adapt their production and supply chain to such reality.

Finally, Martins et all [25] showed that enhancing productivity capacity will be indispensable if the Brazilian beef sector wants to maintain its position as a key player in both the domestic and international markets through productivity growth methods that should include technical efficiency, technological change, scale efficiency, and environmental efficiency. It is clear that technological advances in the sector are not only at play at this moment as they are needed and expected for the maintenance of this market as a high value sector to Brazil.

2.2.1 Brazilian Beef Production Chain

The beef production chain starts in the input sector, after, it passes through the production sectors, where the slaughterhouses transform the raw material into a finished product, finally distribution to the retail segment is responsible for the advancement of end product towards the consumer [26]. Aspects related to foreign trade, macroeconomic evolution, inspection, legislation, product availability, reliability of statistical information, environmental legislation, trace-ability and certification mechanisms, innovation systems, among others, strongly condition the competitiveness in the sector.

It is strongly recommended that livestock farmers use tools that minimize the impact of price volatility in the livestock market on their business for the long run. In the last 20 years, Brazilian beef was able to reduce operational costs due to the increase of technology use, also as a result, the amount of not inspected beef produced dropped from 50% percent to less than 22% [19].

Given production set, industrialization, domestic consumption and export of beef in Brazil, the sector is one of the agricultural markets most susceptible to price uncertainties. Despite the significance of Brazilian beef cattle, the lack of scientific and transparent information about the interdependence between prices in the Brazilian and international markets is an important problem to be considered. Also, the fact that it is unknown how the price transmission occurs, added to the lack of knowledge about the dominance in the transfer and the unfamiliarity whether cross-market pricing is symmetrical between transmitters and receivers.[27]

In addition to Brazil, other relevant countries in the set of production, export and domestic per capita consumption of beef are the USA, Australia, Argentina, Paraguay, and Uruguay. India also has representative numbers, but, for religious reasons, the country produces mainly buffalo meat.

Even though specifics of beef production make it difficult to perceive the advances that took place along the production chain, those numbers show that slowly and steadily Brazilian beef production is moving towards what is seen internationally as Precision Livestock Farming (PLF) [28], which enables the collection of more precise data.

Technology should supply farmers with more precise data, broader management options, possible productivity increase, better disease control or healthier flock, food safety improvement in general, etc. Total production costs of farms that count with the complete cycle of six levels of technology are much lower than those who do not[19].

The 2021 edition of the OECD-FAO Agricultural Outlook [23] projects the global meat supply to expand over the projection period, reaching 374 Mt by 2030. Herd and flock expansion, especially in the Americas and China, combined with increased per animal productivity (average slaughter weight, improved breeding, and better feed formulations) will support the meat market. All that to explain the importance of the use of technology in the interest of lowering costs, improving effectiveness, food safety, product availability, and organizations' reliability and security as a whole.

Malafaia [29] explains that the Brazilian beef cattle supply chain has undergone technological modernisation in its production systems, resulting in better productivity, meat quality and competitiveness. This demonstrates that Brazilian food sector is central to world economy and, as such, it is the point of interest of a wide range of actors. In an international reality where weaponizing CI has become a means to undermine countries capabilities in a contemporary Hybrid Warfare format [30].

The agricultural industry has undergone significant transformation due to technological advancements. Technology has transformed the production and organization systems of the beef supply chain. It has resulted in higher productivity and better meat quality. The use of precision agriculture, big data analytics, and the Internet of Things (IoT) has enabled farmers to monitor and manage their herds more efficiently. This has resulted in better animal health, reduced use of antibiotics, and improved feed efficiency. The use of blockchain technology has enabled the tracking of beef from farm to fork, ensuring transparency and traceability in the supply chain.

Nevertheless, Brazil has become a leader in global beef exports due to favourable climate conditions, land availability at low prices, adequate labour supply, and production technology adapted to a tropical country. The adoption of sustainable production practices, such as rotational grazing and the use of cover crops, has also contributed to the success of the Brazilian beef industry.

Technology has played a significant role in transforming the modern beef supply chain. It has resulted in higher productivity, better meat quality, and improved transparency and traceability in the supply chain. Brazil's success in global beef exports can be attributed to favourable climate conditions, land availability, adequate labour supply, and production technology adapted to a tropical country. The use of sustainable production practices has also contributed to the success of the Brazilian beef industry. [6]

2.2.2 Strategic Assessment

Analysts, research centers, security and intelligence professionals, both from private and public institutions, all have different methodologies and Intelligence cycles to elaborate on data and produce knowledge based on facts. The results are directed and vary according to the specific interest of the decision maker. There are all sorts of material from books, university courses, whitepapers, and frameworks, methods, systems, etc, that detail a myriad of analysis tools and techniques. From the academic point of view, there are some of those intelligence creating methods that are more popular, and, therefore, are worth mentioning:

- Results Analysis - provide gaps and best practices;
- Pattern Analysis - provide management decisions for tactical or operational prioritization;
- Market Analysis - provide prioritization of remediation activities, or operational enhancements;
- Demographics and Social Trend Analysis – provide insights of future pressures;
- Network Analysis – provide understanding of operational losses, insights of gaps, and of potential targets within the organization;
- Risk Analysis – provide impact and probability, and prelude to prioritizing actions, at both the strategic and operational levels.

Intelligence professionals understand the importance of having a solid methodology and intelligence cycle to produce accurate and reliable knowledge based on facts. The results are directed towards specific decision makers, and therefore, it is crucial to have a clear understanding of their interests. From an academic point of view, there are certain intelligence creation methods that are more popular and widely used. One such method is the Scientific Method, which involves a systematic approach to gathering and analyzing data, forming hypotheses, and testing those hypotheses through experimentation.

Another popular method is the Analytic Hierarchy Process (AHP), which is a structured technique for organizing and analyzing complex decisions. The Structured Analytic Techniques (SATs) system is another popular approach that involves using specific techniques such as brainstorming, red teaming, and key assumptions check to improve the quality of analysis. While there are many tools and techniques available, certain methods such as the Scientific Method and SATs, are widely used and have proven to be effective in producing quality intelligence.

The mentioned approaches to intelligence production employ different analytical techniques to produce strategic assessments of threats. So it has become evident that analysis and reporting of cyber risk needs to be part of any business periodic audit and strategic assessment of threats and vulnerabilities [31]. Businesses should have rational processes of how the cyber data enters the life cycle and how analysis may transform raw data to become “knowledge” and produce appropriate reporting in business terms. [32]

Moore et al demonstrated that such reports ought to happen

> *"reactively and at the tactical level, meaning no business decisions are being made, and the information being reported is only valuable for use by a chief information security officer (CISO) or chief information officer (CIO) and is only used to make technology risk decisions. While this type of information is still valuable to the technician, as a risk or business leader you can most likely only use these tactical-level metrics and reporting as a way to find key performance indicators. The data or information at this stage in the cyber intelligence life cycle is still raw and provides no indicators of risk or useful information to business leaders.[32]"*

In the realm of cybersecurity, basic cyber intelligence serves as a foundation for analysis and trend identification. While it may not be decisive in nature, it provides a descriptive account of the existing cyber situation. This includes identifying vulnerabilities within a certain system, as well as possible exploits that may lead to a compromise of said system [32].

The cycle of intelligence creation requires that information is articulated for discussion and understood by business executives. This is necessary in order to be able to debate in business terms and make informed decisions based on reinforceable facts. It is imperative that decision makers understand the real intent or criticality of the information when they are made aware of technology vulnerabilities [32].

In light of this, the strategic assessment of cyber intelligence becomes all the more relevant. By understanding the implications of vulnerabilities and possible exploits, decision makers can make informed decisions that protect their systems and ultimately their business. The importance of this cannot be overstated, as the consequences of a compromised system can be dire. Therefore, we must approach the subject of cyber intelligence with the utmost attention, in order to ensure the safety and security of businesses and systems.

According to Hammond, [33], academic literature demonstrating potential applications of strategic intelligence in security is almost non-existent. Although there is a growing understanding that using strategic intelligence resources to understand and assess transnational threats to enable action to reduce them, there is very little theory or practitioner guidance.[33]

Strategic assessments that are able to combine Sector related security threats and sensitive areas of organisational opportunity are bound to produce broader applicability on topics, due to the focus on consultation, engagement and collaboration alongside traditional intelligence analysis processes, hence creating more effective, and reality connected intelligence reports for decision makers.

2.3 CONTEMPORARY CYBER CONNECTED REALITY

Currently the world is facing the changes brought by the fast development of technology. Agribusiness, despite usually being located in more remote areas and being perceived as less prone to fast changes, is rapidly catching up to the advantages and challenges that the data and automation filled technology brings to the supply chains, commerce, industry, consumers, crime, society, etc.

According to Goel [1], "the Internet has become a potent tool for influencing geopolitical conflicts, including interference in internal affairs of other nations, undermining national security, destabilizing financial infrastructure, and attacks on critical infrastructure."Barara also tells us that today most command and control systems are connected to the Global Information Grid (GIG) or have embedded computer chips [2].

Until 2007, the US intelligence community's annual threat assessment had no mention to cyber warfare. In the face of the Ukrainian war reality, such point is recognized as central to security. Some argue that the transfer, theft, and release of secrets have been made easier by the migration of information from paper to computers. With the 2020 SolarWinds hack of Washington systems, it has come to the world‘s attention that most corporations and some elements of national defense are vulnerable.

Nowadays, stakeholders are diverse and grow more complex, once almost anybody can play the game of cyber warfare. Small commercial satellites provide information that allows civilian intelligence geeks to unravel extraordinary secrets. For example: a satellite image of an earth landscape that a few years back sold for USD 4000 is now available for USD 10. Another example was the college student who used publicly accessible facial recognition technology to identify most of the faces of the people who sought to storm the American Capitol on behalf of President Donald Trump in January 2021.

Only around a quarter of all material in intelligence reports derives from secret sources today. The intelligence community are aware of the need to exploit open sources into its processes. All to create up-to-date results in a timely manner the most important assets to the formulation of relevant intelligence.

In the 2022 Verizon Data Breach Investigations Report (DBIR) [3], it has been revealed that Latin American businesses are facing a significant increase in cyber attacks that target the functioning of their businesses. These attacks include Ransomware and Denial of Service attacks, which are similar to the threats faced by businesses elsewhere in the world. However, what is interesting is that the vast majority of these attacks are being carried out by financially motivated actors, who continue to be the main threat actors in this region.

Given this context, it is no longer an overstatement to say that critical information infrastructure networks are key targets for cyber attacks. This is because these networks have grown to the point where they run the command and control systems, manage the logistics, enable the staff planning and operations, and are the backbone of the intelligence capabilities. As a result, it is essential to have a robust cybersecurity strategy in place to safeguard against such attacks [2]. The threat posed by financially motivated actors cannot be ignored, and it is imperative that businesses take proactive measures to safeguard their operations.

If countries are to face the cyber space is a new and unknown battlefield that grows and develops at unprecedented speed, it is only logic that protection of markets relevant to state level stability, through food safety and Security and Economic stability, should be top priority for the governance and intelligence bodies.

The first regulatory response to those threats from most countries has been to create internet borders and to develop cyber weaponry that may leverage and protect interests during conflicts [1]. However, one must point that state-by-state regulation and the attempt of creating borders to technology might lead to downfalls on innovation and technology creation or simply to ineffective regulations. After all, the Internet has fostered freedom of speech that has led to the social integration as it has been a field for chaos lead by crime and the lack of rules, norms, and ethics [2].

Policy makers have the challenge to balance between regulation, the protection of national interests and potential lawlessness in cyber space. We will not enter the discussion over the necessity to build trust in cyber space versus the fragmentation of the Internet. Nonetheless, it is relevant to note the escalation of cyber conflicts an that is pushing Countries to adapt to another level of protection and security of their interests in the cyber domain.

Under the presented context, cyber Security Specialists have understood that it is necessary to tackle cyber security issues transversely across the most different areas of knowledge. It is clear that, the new dimension of cyber existence is spilling to the kinetic world, hence nation states and companies need to prepare accordingly.

Many countries already hold multidisciplinary research centers and separate considerable investments on Cyber Research Centers. Take The Australian Centre for Cyber Security Research and Innovation (CSRI) for example, its webpage states that CSRI researchers represent a diverse span of expertise and that they work closely with executive cyber security leaders from some of Australia's best-known companies. According o them, this broad network is essential to carry out the demanded research. Also the Center sheds light upon two specific research areas as relevant to today‘s cyber security spotlight the first being Securing data and infrastructure and the second Harmonising cyber governance Research. Other research areas are:

- Advancing cyber security technologies
- Promoting cyber safe behaviours
- Disrupting cyber harms

Another notorious example is the Blavatnik Interdisciplinary Cyber Research Center (ICRC) in Israel, there they have funded researches from areas that range come from the Exact Sciences, Technology, Engineering, Mathematics through Social, Law, Behavior, Management, Health and other scientific disciplines.

Such Countries consider that to completely safeguard the interests of a nation state nowadays it is necessary to establish strategic direction for the development of cyber policy and cyber strategy [2]. Such directives can only come from aggregated and strategic long-term actions and abundant research investments in different areas of study. All with focus to deepen comprehension of national capability, points of interest, needs, technological must-haves, possible threats and threat actors, and vulnerabilities. Without such comprehension it might be impossible to effectively pin-point and safeguard national critical information and/or infrastructures.

In this thesis, Agribusiness is the industry chosen to present this cross-reference study due to the wide economic influence it holds in Brazil and because of its intersector relationships to critical infrastructure and food safety and security. The performance of this sector has been highlighted as a critical component of the economic development of regions where agribusiness has a considerable share in economic activity [4].

Keeping those necessities in mind, this thesis proposes intertwining the two realities of Contemporary cyber connected productive Sector to the need to ensure the protection of such sector‘s interests in the cyber space to safeguard the country‘s commercial interests. The Beef Sector was chosen as main focus to produce a case study methodology where we propose a holistic and pragmatic approach of cyber security issues that take into consideration the protection of critical commercial sectors to Brazil and that are likely to be contemporary targets due to their format, conduct, and supply-chain operations.

This thesis takes International Relations and Economic foundations to understand and pull contenders of the beef market world wide. With that information we use data analyses tactics to cross-reference interests of rival States to Brazil on the beef sector all according to International Relations principles versus operational threat intelligence information and capacities of such States. The focus is to produce relevant information and a methodology that may be replicated in other markets. All to produce pragmatic information that will forge intelligence to threat hunters and decision makers. We believe that this interdisciplinary approach is more realistic to nowadays societal demands because it will generate information and data that could base future research endeavors.

The cross-reference of economic interests of rival States to Brazil on specific product market according to International Relations principles versus operational threat intelligence information and capacities of such States is based on SEI principles as stated by de Souza [5]. SEI is a term that embraces State Intelligence for the purpose of economic development, which is consistent with a set of coordinated actions for the search, treatment, dissemination and protection of information useful to different economic actors with the effective employment of Intelligence Services for economic purposes [5].

This thesis proposes a methodology that reduces the term of SEI to include cyber defense in order to produce structured information on Brazilian Key markets and products that may be targeted in the cyber commercial warfare of nowadays. So this new Cyber Economic Intelligence may produce knowledge to support threat categorization and defense prioritization for Brazilian Agribusinesses and to give relevant information to policy and decision makers on cyber defense issues.

Contemporary agriculture is in the early days of a revolution, at the heart of which lie data and connectivity. Artificial intelligence, analytic, connected sensors, and other emerging technologies could increase yields, improve the efficiency of water usage and other inputs, and build sustainability and resilience across crop cultivation and animal husbandry. With the implementation of connectivity in agriculture, the industry could add on USD 500 billion in value by 2030 [10]. Connectivity infrastructure is expected to cover roughly 80 percent of the world's rural areas, with the exception of Africa, in this context, the key is to develop effective—digital tools for the industry and to foster their adoption [10].

Technological developments bring an infinite horizon of possibilities and uses, for beef production, for example, massive Internet of Things, Low-power networks and cheaper sensors should monitor large herds of livestock, and track the use and performance of remote buildings and large fleets of machinery, which are mission-critical services. Ultralow latency and improved stability of connections will foster confidence to run applications that demand absolute reliability and responsiveness, such as operating autonomous machinery and drones. If LEO satellites attain their potential, they will probably enable even the most remote rural areas of the world to use extensive digitization, which should enhance farming productivity [10].

The unavoidable deployment of 5G networks should impact the sector, once IoT can inherently support a significant number of more connected devices and facilitate industrial adoption and employment of automation systems. Open RAN reduces capital and operational expense levels and improve deployment agility, but it also lacks security focus, as evidenced by various Open RAN alliances [10].

de Oliveira et al makes a point that with the intensification of trade relations between agents from various productive chains and the maximization of business' internationalization contributes to the integration between markets as well as it allows for greater consideration of information and changes in the dynamics of price transmission that, technically, can drive the response to shocks within a market or between markets that trade and/or compete. In the short term, for example, the "shock"would entail the immediate influence in the price of this product, for example. So the discussion on issues that contribute to the evolution of management in agricultural marketing must develop following the findings of studies for decision-making in the production chains. [27]

So the discussion on issues that contribute to the evolution of management in agricultural marketing must develop following the findings of studies for decision-making in the production chains. Agro-industrial chains should follow strict decision making processes that are data and information driven so to be more effective. That may contribute to the economic sustainability of agribusiness as one of the main sectors of the Brazilian economy. [27]

Proper security planning and investments on the area become primordial to conform to those new realities, even to a tradition related sector such as agribusiness. Recent cases of strategic supply chains workflow being challenged after cyber attacks show that modern production of key products is heavily automated, and it is not only for safety reasons.

2.4 RELATED WORKS

2.4.1 Threat Intelligence

According to Chismon and Ruks [34], it is relevant to have a clear differentiation between vulnerability information and threat intelligence to produce relevant intelligence, after all a vulnerability might exist in a product used by the organisation that not necessarily is information about a particular threat. Considering traditional intelligence versus today's world of effective and motivated attackers, with country funding and resourcing, it is critical that security principles are valued.

Threat intelligence formation has yet to have an exhaustive format and methodology, companies, countries, academia are learning and improving on a day-by-day basis, taking into account contemporary occurrences and fast technological development. Traditional Threat Intelligence is still relevant in the sense that it comes from observation and analysis of contenders and that it [35]:

> *"Must be actionable to meet the needs of current defensive systems that have to deal with and respond to cyber attacks."*

Threat intelligence is a vital aspect of modern cybersecurity. It involves the collection, analysis, and dissemination of information about potential threats to an organization's security. The goal of threat intelligence is to provide organizations with the knowledge they need to proactively defend against cyber attacks.

In order to effectively gather and analyze threat intelligence, organizations must utilize a variety of tools and techniques. These may include network monitoring, vulnerability scanning, and threat hunting. Additionally, organizations may gather intelligence from external sources such as government agencies, security vendors, and industry groups [35].

Once threat intelligence has been gathered and analyzed, it must be disseminated in a timely and effective manner. This may involve sharing information with other organizations in the industry, as well as with government agencies. By sharing threat intelligence, organizations can work together to better defend against cyber attacks and protect their sensitive data [8]. As the threat landscape continues to evolve, it is more important than ever for organizations to prioritize threat intelligence as part of their overall cybersecurity strategy.

Consequently, trends in country strategies, ambitions, priorities and other high-level information should instruct strategic analysis. That information needs to be coupled with observations of malware or cyber attacks thought to create a picture of cyber activities. High-level sources need to feed this type of information to Threat Intelligence analysts including [34]:

> *"Policy releases by nations or groups of interest, news stories in domestic and foreign press, and news stories in subject-specific press, such as financial papers, or articles published in journals by high-ranking persons in the nation or group of interest, as all of those can be indicators of intent or capability."*

Kotsias affirms that the military mindset associated with the use of threat intelligence is of difficult assimilation to the typical business culture, so, there is limited know-how about the deployment of routines to inform actions of executives and business managers a colution might come from a compliance-driven and reactive logic towards a proactive security culture.[36]

Off course, that is much easier said than done, because it would require organisations to shift their culture of risk management from compliance with general industry and government standards towards threat intelligence collection and operationalisation.

> *"A threat intelligence team provides operational, tactical and strategic level reports through reliable and routine feeds to relevant stakeholders. At an operational level, the team should proactively monitor the threat landscape feeding actionable intelligence to analysts. At a tactical level the team predicts threat activity and validates that against the observations. At a strategic-level, the team identifies new threat actors and their tactics, techniques and procedures (TTPs) to identify and address gaps in the firm's cyber defences that might be exposed."*

Nowadays, there are threat intelligence vendors that monitor the threat landscape, collect and analyze threat intelligence and apply adversarial thinking and frameworks all to provide accurate, timely and targeted advice in the form of actionable and organisation-specific insights to security analysts They also have specialised tools with embedded threat intelligence to map threat patterns and prioritise which detection and responses require the most attention.[36]

2.4.1.1 Cyber Threat intelligence

Even though there is a general awareness for the need of CTI nowadays, it is an undeveloped field that follows the basic principles of traditional Intelligence production cycle and that should consider all details around an effective and multifaceted security system [37]. In this matter, ISO introduced an updated version of the ISO 27001 in 2022. One of the most crucial facets of this standard includes threat intelligence and it enables companies to collect and analyze data. CTI in ISO standards aims at protection by increasing awareness of the threats inside or outside of the organization [38].

According to Tounsi's work [9], most used defense techniques and tools commonly rely on static malware signatures that might leave organizations vulnerable to ever-evolving threats that exploit unknown and zero-day vulnerabilities. This ever changing scenario requires a new format of threat prevention tools and planning that adapt to the complex nature of new generation threats and work on a more precise aim for threat analysts and tools. The concept of CTI is intertwined to the one of TI in the sense that they are evidence-based knowledge representing threats that may inform and support the decision making process. Hence, CTI can be perceived as a process that helps to reduce the gap between advanced attacks and defense mechanisms.

Kotsias, [36], affirmed that Threat Intelligence are traditionally an understanding of Military organisations because of its role in directing operations against hostile actors. The author argues that CTI has the similar objective of redressing the asymmetrical advantage to cyber-attackers over cyber-defenders. In this regard, he defines CTI as the process of acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities inside the cyber domain to offer courses of action that enhance decision making, and with the power of changing cybersecurity behaviour from being reactive to proactive, anticipatory and dynamic.

If we are to expand this approach of CTI to the defense of the interests of Nation States, such as critical infrastructure and/or commercial interests, CTI thus has the potential to direct organisational behaviour in prevention, detection and response to cyber-attacks according to a countries policy. All to support prevention by alerting organisations to vulnerabilities that can exploited by specific threat actors with the means, motivation and capability to attack the firm. Finally, CTI could direct cyber-response by providing a precise defense strategy to combat specific cyber-threat actor's modus operandi.[36]

It is relevant to understand the definition of Cyber Security as the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures [39], so to fully grasp the importance of CTI and to protect the sector accordingly.

Some analytical frameworks provide structures for thinking about attacks and contenders to allow defenders to take decisive actions faster. For example, the defensive perspective of a kill chain and the Diamond model used to track attack groups over time [9].

With respect to updated cyber security necessities, Agribusiness reality and current CTI production cycles as presented by Borges *et al.* [40] added a strategic approach to understand how CTI may assist interested parties to develop long-term cyber security strategies. So that intersecting CTI with economic and political components may lead to thorough and updated assessment for the unveiling of potential cyber threats.

One of the key benefits of CTI is that it allows institurions to stay ahead of emerging threats. By analyzing data from a variety of sources, we can identify patterns and trends that may indicate a potential attack. This information can be used to develop proactive measures to prevent attacks, such as updating security protocols or implementing new software. Another important aspect of CTI is information sharing. By sharing threat intelligence with other organizations, we can work together to identify and prevent cyber attacks [39]. This collaboration is essential in today's interconnected world, where a single attack can have far-reaching consequences.

Tounsi [9] and Evans [30] provided key definitions on CTI, and how they are currently being used in the kinetic world, through International Relations and warfare. Also we were able to grasp how the literature subdivides the issues surrounding those topics and the emerging research studies, trends and standards that might mitigate those issues.

The work of Shin and Lowry [41] brightened the reasons why CTI ascended from a growing demand of organizations to understand their enemies and plan accordingly for proactive, preventive, and timely threat detection, all with focus on improving ‘general readiness’ against known or unknown threats. In this sense,

> *"CTI represents actionable threat information that is relevant to a specific organization".*

2.4.2 Countries with Cyber Attack Capabilities and Their Targets

The 2021 Threat Landscape Report of the European Union Agency for Cybersecurity (ENISA) selected State-sponsored actors as a category to be highlighted due to its prominence during the reporting period. According to the report state-sponsored threat were observed targeting healthcare, pharmaceutical, and medical research sectors, throughout the COVID-19 crisis. Apparently, the collection of scientific information related to the COVID-19 vaccine was a high priority [42]. The report also recognized that supply chain compromises by state-backed threat actors are not new and that this type of attack reached new levels of sophistication and impact since 2021.

The acts might occur for strategic objectives or for personal gain and with varying levels of national responsibility, what sheds doubt between the definitions of cyber espionage and cyber crime operations.

The main spotted trends in the sector showcase that countries with advanced cyber capabilities are using those to strategically shape global political, military, economic, and ideological power, while middle powers are focusing on initiatives related to regulation, cyber norms, and protection of their critical infrastructure. Cyber operations are aligned with the strategic objectives of states as well as the geopolitical landscape and real-world events.

ENISA also highlighted, among other examples, increased cyber intrusion activities in regions of trade routes, against strategic targets such as governmental organisations, and cyber operations as enablers for large-scale espionage. This movement, not only, is here to stay, but also, will be more used for intelligence gathering and critical infrastructure attacks. So state sponsored groups are expected to conduct operations to weaken, demoralise and discredit adversarial governments and install media misinformation in order to amplify impact through the exploitation of societal divisions, trust impairment, and society polarisation over issues that are sensitive in certain countries [42].

On the scent, the Guide to Developing a National Cybersecurity Strategy by the organized by the International Telecommunication Union (ITU) [43] stressed the importance of international law enforcement cooperation and formal or informal mechanisms to share information, build trust, and support cross-border cooperation in combating cyber crime and other cyber-enabled crimes. Even ITU guide recognized that:

> *"To fully realise the potential of technology, states must align their national economic visions with their national security priorities."*

Meaning that nations should be working on offensive and defensive capabilities to defend themselves from illicit and illegal activities in cyber space and to pre-empt incidents before they can cause harm.

In and attempt to understand actors in the sector a group of researchers in The Harvard University came up with the Harvard National Cyber Power Index (NCPI) index [44] that considers that the analysis of cyber power is the product of intent and capability. As a result the top ten "most comprehensive countries"with the highest level of Intent Ranking by Commercial Objective are as follows [44]:

1. China
2. Iran
3. United Kingdom
4. Japan
5. Switzerland
6. Netherlands
7. Sweden
8. Australia
9. USA
10. Russia

The NCPI considers cyber Power as the product of intent and capability so countries with high level of those characteristics are among the highest-ranking countries in the Index. These countries both signal in strategies and in previously attributed cyber attacks that they intend to use cyber to achieve policy goals and have the capabilities to achieve them.

The index recognizes countries not normally associated with cyber powers, due to their strong capabilities in certain areas. For example, Sweden is in the top 10 rank for surveillance, cyber defense, and information control; and Switzerland made the top 10 for cyber defense and commercial gain.

China deserves an explanation of its own once it is assessed to use industrial espionage, to incentive and grow its domestic cyber expertise through research and development, and public-private partnerships, both in a legal an illegal manner.

Finally, it is likely that state-backed threat actors will continue conducting supply chain attacks, especially targeting software, cloud, cloud-hosted development environments and managed service providers, that is not to forget that cyber crime threat actors increasingly show the same patterns of behaviour [42].

2.5 SUMMARY

In this chapter, we delve into the contemporary food supply chain structure and the various knowledge areas that must be considered to gain a comprehensive understanding of it. Firstly, we examine the regulations on critical infrastructure in different countries and their varying definitions. This is crucial as it affects the entire food supply chain, from production to consumption. Moving on, we bring forth specific studies about the beef sector and the world market today. Furthermore, we analyze how the technological and innovative sectors are influencing the beef sector, specifically in terms of cyber security.

To appropriately assess cyber security issues in the agribusiness sector, we present definitions and principles in Related Works from Threat Intelligence (TI) and Cyber Threat Intelligence (CTI). Then, we present how today’s intelligence creation and presentation is of relevance for the maintenance and security of a stable production chain cycle. This is crucial as it ensures that the food supply chain is not disrupted by cyber security threats. Finally, we assess countries with cyber attack capabilities and their targets, according to a well established methodology.

All to conclude that, a comprehensive understanding of the contemporary food supply chain structure requires consideration of various knowledge areas, including regulations on infrastructure, economic assessment of the beef sector in the world market, and possible cyber security threats.

3 RECENT CASES OF CYBER ATTACKS WITH IMPACTS IN THE AGRIBUSINESS SECTOR AND SUPPLY CHAIN PROVIDERS

ENISA admits that nowadays most states all over the world conduct cyber operations to accomplish their strategic goals, so it is a given that there is a cyber arms race towards the implementation of cyber capabilities [42]. Considering the cyber offense trends, States with great dependability on world commerce and their exports need to adapt to the contemporary commerce world and introduce themselves to this interconnected war with investment and planning. Such initiation may be through initiatives related to regulation and protection of their critical infrastructure, passing through creating a fluent dialogue between interested private and public entities or even by investing in their own cyber capabilities.

The same ENISA report, [42], informs that the food sector went from zero attacks in 2020 to 16 attacks in 2021. The only other sector that had a similar groundbreaking scenario was the postal and courier services sector who went from having no cases in 2020 to 6 cases in 2021. Nonetheless, those attacks were not enough to characterize a trend, the numbers demonstrate a significant increase in interest of attackers for the food sector.

Aligned with that thought, there is the conspicuous truth that cyber threats grow rapidly promoted by the rise of digitization in all sectors of human development, this expansion comes with dangers and target amplification. Therefore, digitization must be rethought to include information security at higher priority, in a sense that it becomes the foundation of all digitization processes.

In this context, a new concept around the idea that information systems (IS) architecture needs to consider security issues before they are built, in a manner that they are embedded all over the construction period. Such concept is called Security by design (Sbd) [45]. Sbd initially emerged from computer engineering principles, but now it is commonly presented by public regulatory bodies as a public policy ideal, partly to ameliorate the security vulnerabilities presented by the 'Internet of Things' (IoT), and partly to bring about discussions on similar digital issues around data protection and cyber hygiene. It adds to an expanding 'by design' discourse focused on integrating various values into technology production processes. The main demand here would be to develop true secure software systems from ground up.

> "The scant academic treatment of SbD is surprising given the huge amount of scholarship on data protection, cyber security and internet governance, along with the rapid growth of 'by design' discourse. This paucity of attention might be partly due to an attitude amongst legal scholars that SbD is a relatively mundane, uninteresting matter. Yet, it also arguably reflects the absence of the mantra's express manifestation in a bespoke, high profile legislative provision akin to Article 25 of the General Data Protection Regulation (GDPR). The latter has undoubtedly played a key role in bringing DPbDD into the limelight. As shown further on in this article, SbD is, in part, baked into Article 25 GDPR. Hence, parsing the latter ought to bring elements of SbD into greater focus."[45]

That is, the embedding of standards into design at the standard-setting stage in order to foster social outcomes deemed desirable by the industry, in our case here more secure and trustworthy systems against cyber attacks and that leave businesses more compatible to today´s reality.

The world wide respected cyber security company called Dragos [46] released a report in the end of 2022 in which it admits to the continued increase of threats and ransomware attacks in 2022, especially by vertical industry include:

- The first attacks against the mining and metals industries in Australia and New Zealand (ANZ) region;
- Continued targeting of renewable energy companies in the U.S. and the EU;
- Increased attacks on energy, food and beverage, pharmaceuticals, chemicals, water and wastewater; and
- Accelerated attacks in electrical, manufacturing, oil and natural gas, and liquefied natural gas

Additionaly, Dragos identified victims in the food and agriculture including manufacturing, processing, and storage sectors of the industry that were communicating with known Threat Groups called KAMACITE's and C2. So in the report's ransomware timeline for 2022 the report shows that the attacks spanned many industries, including energy, automotive, agriculture, water, mining, and metals [46]. Dragos report tracked 437 manufacturing entities in 104 unique manufacturing subsectors, it showed that that nine percent of attacks targeted food and beverage sector. Also these other Threat group were mentioned a having targeted food upply chains:

- DATALEAK
- LV
- Medusalocker
- PLAY
- Suncrypt

All to make the almot obviou point that Businesses digitization trajectories may only be successful when proper cyber security techniques are employed [6]. In this ambience, cyber attacks have become more common, bellow we present recent cases of attacks against agribusiness sector and supply chain providers with focus on attacks against beef producers.

3.1 COLONIAL PIPELINE

According to the news, on May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyber attack that impacted computerized equipment managing the pipeline. The Company had to hold the pipelines to contain the attack. With the assistance of the American Federal Bureau of Investigation (FBI), Colonial Pipeline paid the requested ransom, approximately 75 bitcoin

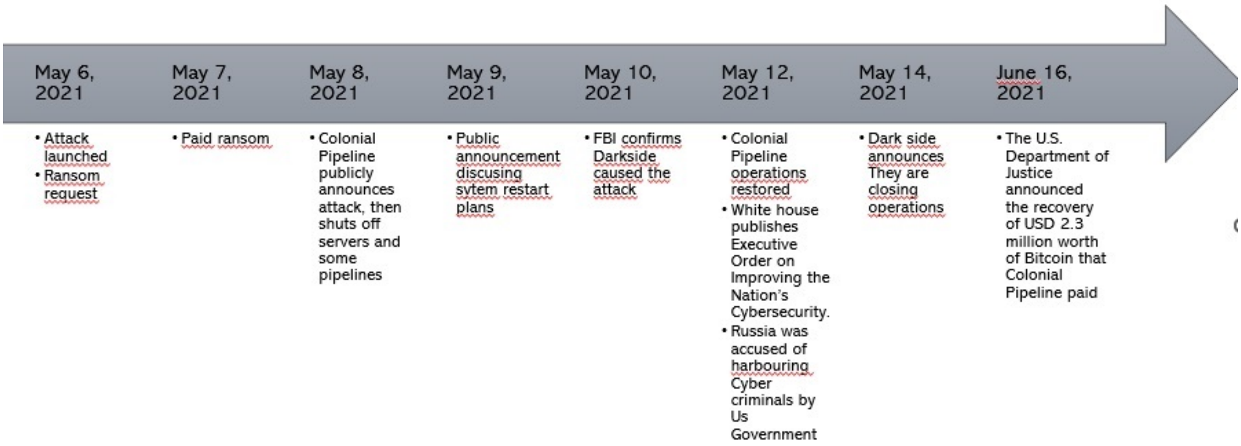

May 6, 2021
• Attack launched
• Ransom request
May 7, 2021
• Paid ransom
May 8, 2021
• Colonial Pipeline publicly announces attack, then shuts off servers and some pipelines
May 9, 2021
• Public announcement discusing sytem restart plans
May 10, 2021
• FBI confirms Darkside caused the attack
May 12, 2021
• Colonial Pipeline operations restored
• White house publishes Executive Order on Improving the Nation's Cybersecurity.
• Russia was accused of harbouring Cyber criminals by Us Government
May 14, 2021
• Dark side announces They are closing operations
June 16, 2021
• The U.S. Department of Justice announced the recovery of USD 2.3 million worth of Bitcoin that Colonial Pipeline paid

Figure 3.1: Timeline of the Colonial Pipeline attack.

(USD 4.4 million at the time of the attack) several hours after the attack. That was the largest cyber attack on an oil infrastructure target in the history of the United States and it led to fuel shortages and price spikes across the country. That is an example of the type of outcomes that a cyber attack on critical infrastructure may cause, see figure 3.1.

A couple of weeks after the attack, FBI and various media sources identified the criminal hacking group DarkSide as the responsible party for the attack. A few days after the APT group - DarkSide ransomware - started to scarce its operation, they announced they were closing up short after its servers were seized and someone drained the cryptocurrency from an account the group used to pay its affiliates.

American government agencies started to act because of the recent augmentation of cyber attacks over the last few years. In January, 2021, American Cybersecuirty and Infrastructure Security Agency (CISA) launched the Reduce the Risk of Ransomware Campaign with the aim to educate public and private sectors on anti-ransomware best practices and available tools and resources to help mitigate attacks. Another concrete measure came from the Department of Homeland Security (DHS) who offered to provide USD 25 million in grants to state and local cyber security preparedness programs with a particular focus on combating ransomware. Finally, CISA received administrative subpoena powers authorized under the 2021 National Defense Authorization Act to help it address ransomware attacks and other cyber threats. From then on CISA will be able to compel internet service providers to turn over certain subscriber information that would help better identify potential attacks as well as targeted organizations. The Department of Justice (DOJ) created a new task force dedicated to rooting out and responding to the growing threat of ransomware. The initiative came after what DOJ called the worst year ever for ransomware attacks.

Those actions highlighted how cyber security threats have become a major focus of the White House. On the political front, Federal Administration imposed new sanctions on six Russian technology companies that provide support to the cyber program run by Putin's intelligence services linked to the hacking of the SolarWinds information technology company. On the same note, Homeland Security and Governmental Affairs Committee, introduced bipartisan legislation to provide additional resources and better coordination against cyber attacks or breaches that risk the safety and security of Americans. All with focus to improve the federal response to cyber breaches in both federal networks and private companies' servers. The idea is to create an authority for the Secretary of Homeland Security, in consultation with the National

Cyber Director, to declare a Significant cyber Incident in the event of an ongoing or imminent attack that would impact national security, economic security, or government operations. That would empower CISA to coordinate federal and non-federal response efforts, and allow the creation of a Cyber Response and Recovery Fund that would help support federal and non-federal entities impacted by the event. The bill would authorize USD 20 million over seven years for the fund.

3.2 JBS ATTACK

On May 30th, 2021, newspapers all over the world brought about the case of the Brazilian based meat company called JBS had its servers and computer networks attacked, temporarily shutting down some plant operations in Australia, Canada and the USA. Even though backup Servers were not affected, the attack caused delay in transactions with clients and suppliers, damaged the companies image, and it commenced a chatter over possible meat shortage and price rise. Only by the beginning of June the company was able to fully recover and put its global IT Systems back in order.

JBS took the following crisis management steps:

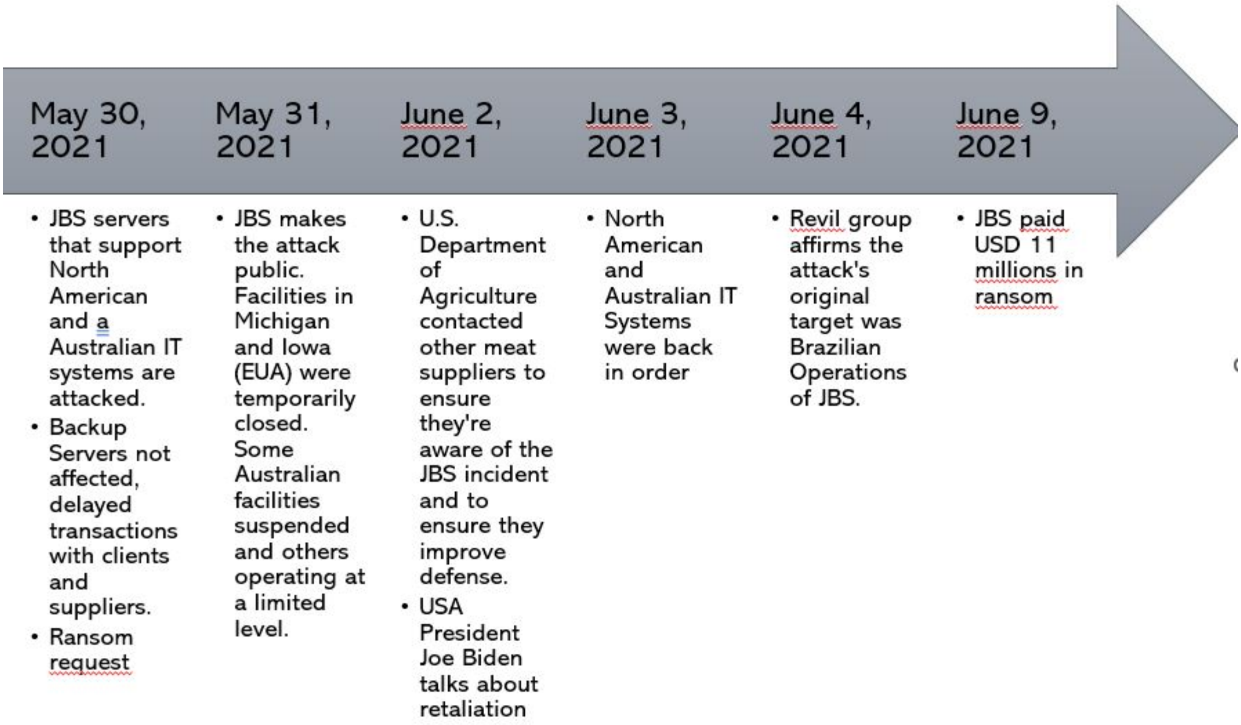
- Suspension of all affected systems;
- Notification of due authorities;
- Activation of the company's global network of IT professionals and third-party experts to resolve the situation.

Even though all crisis management steps were taken to handle the situation, JBS facilities in the American States of Michigan and Iowa were temporarily closed; some Australian facilities operations were suspended and others operated at a limited level. That disruption threatened food supplies and risked higher food prices for consumers.

The White House has said that a criminal organisation "likely based in Russia"was behind the attack. American National Security organizations expressed their concern because it affected the food supply chain which is fundamental for the health of the nation. In the beginning of June the White House stated it had put Russia on notice over the ransomware attack. The White House said the U.S. Department of Agriculture started contacting other meat suppliers to ensure that they were aware of the JBS incident and to make them take steps to defend themselves against similar attacks. As a result, there were political actions towards sanctions against possible threat actors, emergence of new cryptocurrency rules, and negotiations to turn ransom payoff into a crime were evoked.

On June 4th, 2021, Russia linked cyber group REvil announced the group was responsible for the JBS attack via an interview to Sergey R3dhunt in Telegram, in which he said the attack targeted Brazilian Operations of JBS initially. On June, 10th, JBS announced it had paid USD 11 million in ransom to put an end to the attack, the payment was reportedly made using Bitcoin after plants had come back online.

On June 16th, 2021, American and Russian President held a summit in Geneva, where cyber security was a significant topic of conversation. American President clearly stated cyber security as a vital American interest and stated that "Russian activities that run counter to those interests will be met with a response" in an intimidating discourse. That fractured relations of Russia and the USA, see figure 3.2.



May 30, 2021

- JBS servers that support North American and a Australian IT systems are attacked.
- Backup Servers not affected, delayed transactions with clients and suppliers.
- Ransom request

May 31, 2021

- JBS makes the attack public. Facilities in Michigan and Iowa (EUA) were temporarily closed. Some Australian facilities suspended and others operating at a limited level.

June 2, 2021

- U.S. Department of Agriculture contacted other meat suppliers to ensure they're aware of the JBS incident and to ensure they improve defense.
- USA President Joe Biden talks about retaliation

June 3, 2021

- North American and Australian IT Systems were back in order

June 4, 2021

- Revil group affirms the attack's original target was Brazilian Operations of JBS.

June 9, 2021

- JBS paid USD 11 millions in ransom

Figure 3.2: Timeline of the attack against JBS.

3.3 JOHN DEERE AND CASE NEW HOLLAND

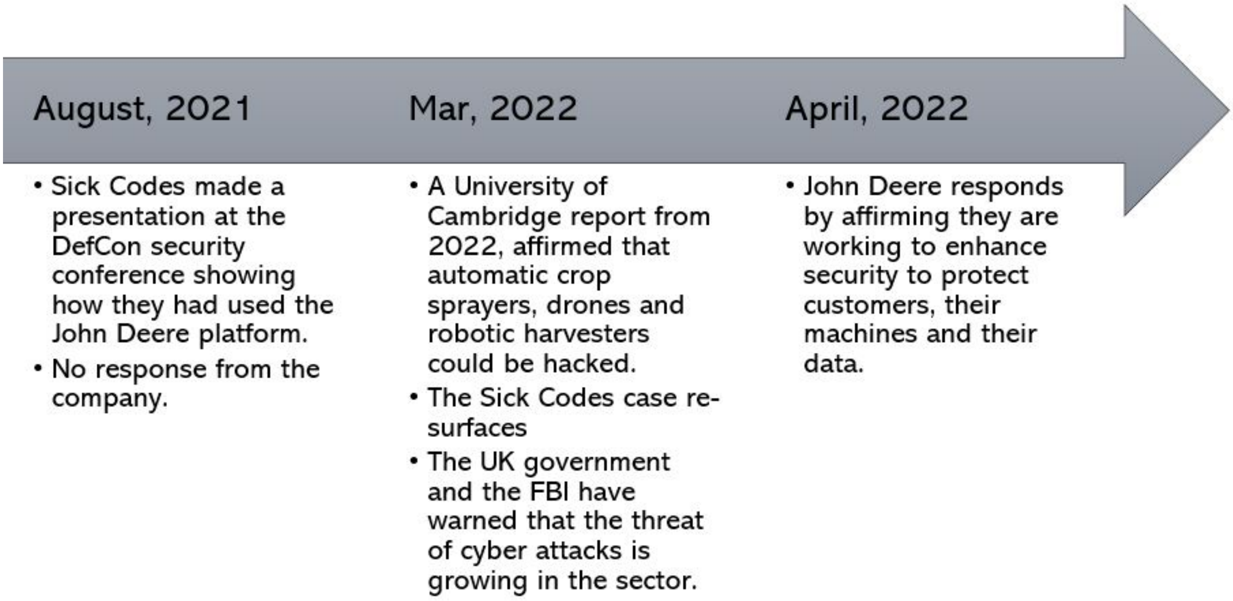
In August, 2021, a group of hackers called Sick Codes made a presentation at the DefCon security conference showing how they had used the John Deere platform to make changes to supply networks, equipment reservations and even the contact details of those who received “demo units” from the company. Sick Codes demonstrated that they found a misconfiguration that gave access over to anyone and from there they found additional credentials, the original signature password and even the encryption certificate. Once they had those information, they could have taken over the whole system on the John Deere operations center. The group asserted they did not act beyond the knowledge of being able to control the center, see figure 3.3.

Sick codes also mentioned vulnerabilities in the systems of Case New Holland, John Deere’s major competitor. Similarly Case’s system has security issues that included unprotected servers and personally identifiable information IP addresses.

A recent University of Cambridge report by Tzachor [47] affirmed that automatic crop sprayers, drones and robotic harvesters could be hacked. The UK government and the FBI have warned that the threat of cyber attacks is growing in the sector.

A University of Cambridge report from 2022, by Tzachor [47], affirmed that automatic crop sprayers, drones and robotic harvesters could be hacked. The UK government and the FBI have warned that the threat of cyber attacks is growing in the sector.

The study also reviewed risks relating to interoperability, reliability and relevance of agricultural data, unintended socio-ecological consequences resulting from Machine learning (ML) models optimized for yields, and safety and security concerns associated with deployment of ML platforms at scale. And they



August, 2021

- Sick Codes made a presentation at the DefCon security conference showing how they had used the John Deere platform.
- No response from the company.

Mar, 2022

- A University of Cambridge report from 2022, affirmed that automatic crop sprayers, drones and robotic harvesters could be hacked.
- The Sick Codes case re-surfaces
- The UK government and the FBI have warned that the threat of cyber attacks is growing in the sector.

April, 2022

- John Deere responds by affirming they are working to enhance security to protect customers, their machines and their data.

Figure 3.3: Timeline of the John Deere case.

suggested risk-mitigation measures that include inviting rural anthropologists and applied ecologists into the technology design process; applying frameworks for responsible and human-centred innovation; and setting data cooperatives for improved data transparency and ownership rights, and initial deployment of agricultural AI in digital sandboxes.

The report brought attention once more to the security of John Deere' operations. The company replied by affirming they are working to enhance security to protect customers, their machines and their data. The company's global chief information security officer ha affirmed that John Deere had been liaising with a number of ethical hackers on vulnerabilities they have found. He also said those found so far by Sick Codes did "not pose a threat to customers or their machines"and that "No company, including John Deere, is immune to vulnerabilities, but we are deeply committed and work tirelessly to safeguard our customers, and the role they play in the global food supply chain."[48]

3.4 USAHERDS

In 2021, a China-affiliated threat actor, known as APT41 or Barium, used Log4j and zero-day bugs to breach at least six US state governments networks for over a year. APT41 used a vulnerability in the USAHerds - Animal Health Emergency Reporting Diagnostic System - to penetrate state networks.

Although APT41 has historically performed mass scanning and exploitation of vulnerabilities, investigations into APT41 activity between May 2021 and February 2022 uncovered evidence of a deliberate campaign targeting U.S. state governments.

USAHERDS software is used by 18 states throughout the USA, all of them are now under scrutiny to understand if their servers could have been invaded or even hijacked by the hackers. The Barium group has not yet disclosed its objective nor what data they may have been seeking, according to a published threat report from cybersecurity firm Mandiant [49].

APT41 activity occurred between May 2021 and February 2022 and it uncovered evidence of a deliberate campaign targeting U.S. state governments. APT41 reached six U.S. state government networks through the exploitation of vulnerable Internet facing web applications. When APT41 gained access of USAHERDS, the company said that their Managed Defense quickly detected and contained the activity.

Two weeks later APT41 re-compromised the network by exploiting a previously unknown zero-day vulnerability using USAHERDS applications. On December 10th, 2021, the Apache Foundation released an advisory for a critical remote code execution (RCE) vulnerability in the commonly used logging framework Log4J. Within hours of the advisory, APT41 began exploiting the vulnerability to later compromise at least two U.S. state governments as well as their more traditional targets in the insurance and telecommunications industries.

In sequence, APT41 exploited the the Log4J vulnerability to re-compromised two previous U.S. state government victims, what shows the continuation of their campaign into 2022 and demonstrates their unceasing desire to access state government networks.

Mandiant report [49] mentions exfiltration of personally identifying information "consistent with an espionage operation," although the company said that it could not make a definitive assessment of intent of the attack. All in all, Mandiant's research demonstrates a constantly adapting adversary.

Mandiant [49] confirms that APT41's recent activity against U.S. state governments encompass new capabilities, the group is able to quickly adapt their initial access techniques by re-compromising an environment through a different vector, or by being able to operationalize a fresh vulnerability. Also, the group shows intelligence and organizational abilities when they retool and deploy capabilities through new attack vectors as opposed to holding onto them for future use. When APT41 exploited Log4J in close proximity to the USAHerds campaign cleared the group's intent to target U.S state governments through cultivated and co-opted attack vectors.

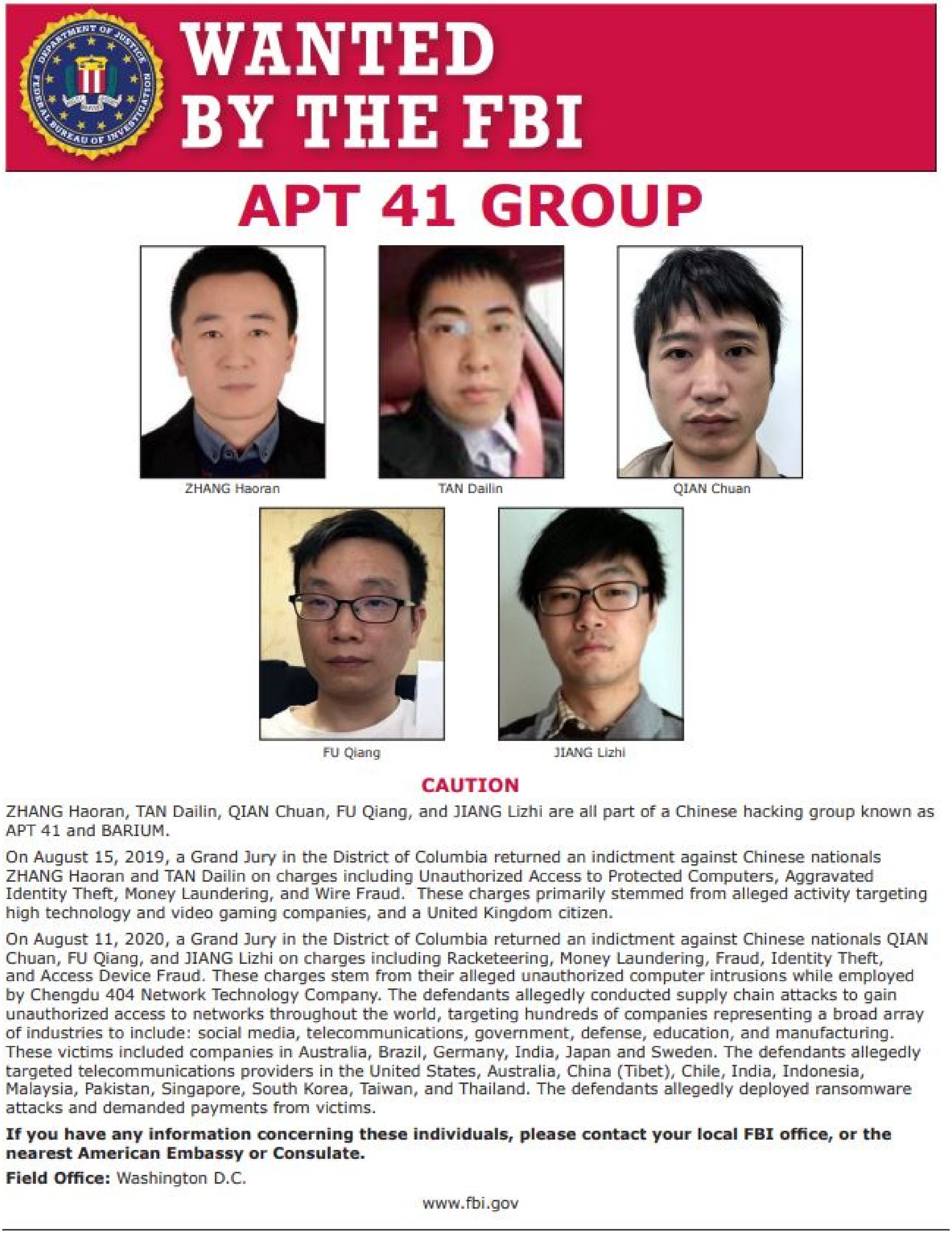
The group entered FBI's most wanted list [50] on the following counts (see figure 3.4):

- In 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud.

- In 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

The 2019 charges primarily were based on a myriad of criminal activities targeting high technology and video gaming companies, and a United Kingdom citizen. A shift is recognized by the authorities in the 2020 charges, when the group was indicted for conducting supply chain attacks to gain unauthorized access to networks throughout the world. It is noteworthy that the group moved its goals towards companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing.

The victims included companies in Australia, Brazil, Germany, India, Japan, USA and Sweden, also telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Ma-



WANTED BY THE FBI

APT 41 GROUP

ZHANG Haoran

TAN Dailin

QIAN Chuan

FU Qiang

JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov

Figure 3.4: FBI Wanted Flyer.

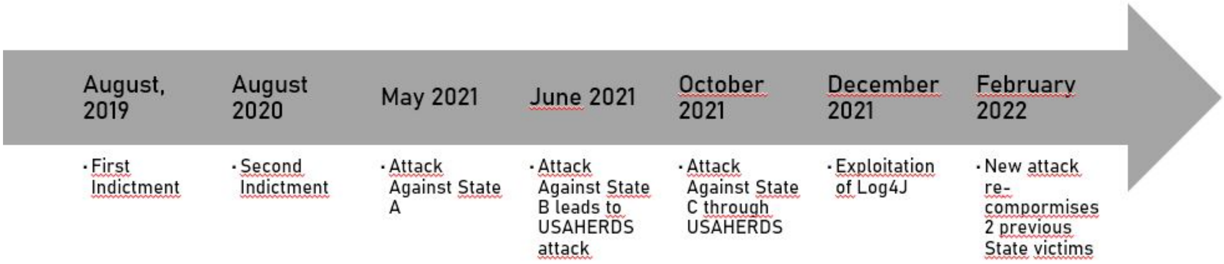


Figure 3.5: Timeline of the USAHERDS case.

laysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. the interesting aspect that may raise questions on its own is that the targeted countries and companies do not include Countries known to be more lenient in the battle against these hacking groups, such as Russia and Continental China, even though they do have large companies both in the supply chain and in the telecommunications sector.

The charges do not seem to reduce the group yearns, once the USAHERDS attacks took place about a year after the District of Columbia indictments. That is to say that maybe conventional crime mitigation and investigation techniques might not just be enough in theses cases, see figure 3.5.

3.5 DOLE

On Feb 22, 2023 The Dublin-based fresh produce giant admitted to having suffered a ransomware attack. Even though the company asserted that the attack had a limited overall impact on the company ongoing activities and supply chains it affected, the attack was disruptive to its Chilean and fresh vegetables business, according to a filing with the U.S. Securities and Exchange Commission [51]. The company announced it had experienced a cyber security incident identified as ransomware but that it was under control [52].

According to the company's website, Dole is one of the world's largest producers and marketers of high-quality fresh fruit and fresh vegetables. Dole is an industry leader in many of the products it sells, as well as in nutrition education and research.

The attack disrupted its operations and the company admitted to have hired third-party experts to assist with the mitigation and protection of the impacted systems [52]. Dole said it notified law enforcement and was cooperating with the investigation:

> "Upon learning of this incident, Dole moved quickly to contain the threat and engaged leading third-party cyber security experts, who have been working in partnership with Dole's internal teams to remediate the issue and secure systems..."

CNN informed that the company was forced to temporarily shut down production plants in North America and stopped food shipments to grocery stores, which caused disruption in salad distribution. Regardless of the company's quick moves towards crisis management, an internal memo posted on Facebook and sent to grocers on February 10 informed that the incident shut down Dole's systems throughout North America: "Our plants are shut down for the day and all our shipments are on hold..."the memo read. That document suggests that the consequences of the attack were greater than it was initially announced.

3.6 AGCO

In May 2022, the Alcohol and Gaming Commission of Ontario (AGCO), a U.S.A-based manufacturer and distributor of agricultural equipment, disclosed that they suffered a ransomware attack affecting multiple production facilities. Black Basta was responsible for this incident. Dragos assesses with low confidence that this precautionary shutdown of their IT networks also impacted AGCO's ICS networks and operations [46].

AGCO, holds its headquarter in Duluth, Georgia, and it designs, produces, and sells tractors, combines, foragers, hay tools, self-propelled sprayers, smart farming technologies, seeding and tillage equipment. AGCO sells tractors and combines, manufactures and assembles products in 42 locations worldwide with 1.810 dealerships in North America, it is the first competitor against John Deere.

The company first discovered this attack through its subsidiary, Massey-Ferguson, when its websites in France, Germany, and China were targeted. At discovery, employees were sent home from production facilities in France and operations across the globe were affected. To mitigate and remediate the attack, AGCO shut down portions of its IT systems.

According to the company's news release [53], they suffered a ransomware cyber attack that was discovered on May 5, 2022. Most affected production sites and parts operations resumed operational activities until May 16, 2022. The Company also reported that there was data exfiltration as a result of the ransomware.

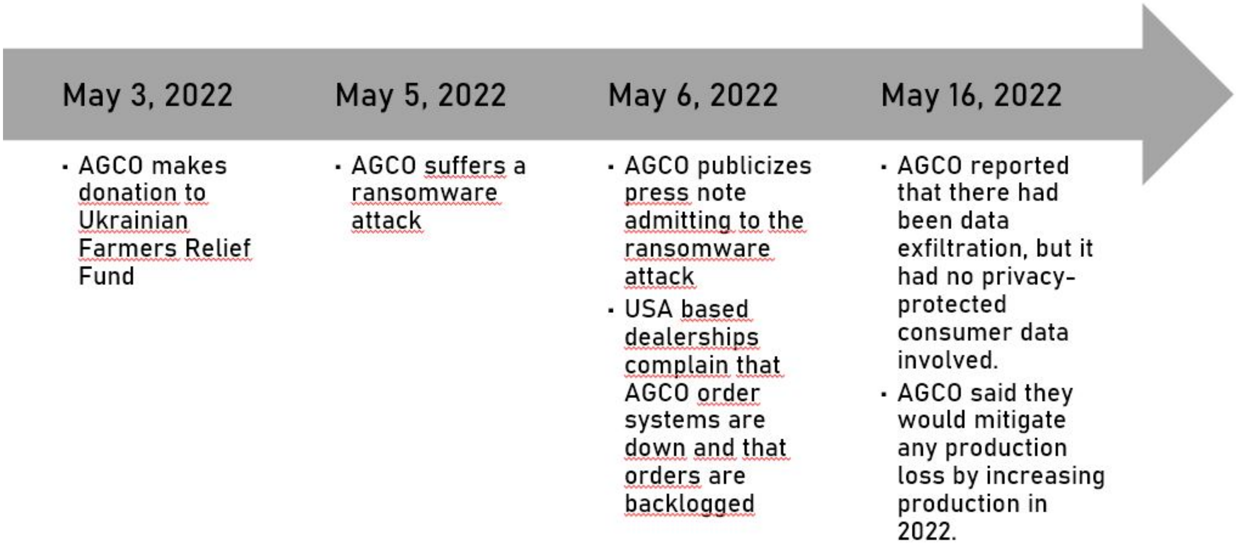
Following an article published in the National Law Review [54], the attack might have had political motivation. AGCO dispersed a donation to a Ukrainian relief fund on the day before the attack took place. AGCO Agriculture Foundation donated USD 50,000 to the BORSCH initiative, that assists Ukrainian farming communities affected by the war with Russia, see figure 3.6.

3.7 CONTEXT AFTER RECENT CASES

Recent cases demonstrate that supply chains in general are not at a very high level of security, States and private companies need to invest heavily on dialogue and cyber risk management to specify minimum cyber security requirements for companies all according to CTI requisites Section 2.4.1.1. After all, a strategic approach to understand CTI might lead to sustainable long-term cyber security strategies.

After JBS suffered the ransomware attack, it affirmed that clients and employees' information were not compromised due to fear of lawsuits concerning protection of personal data. That indicates that new regulation on the area may be bringing results to force those companies invest in cyber security and become aware of cyber issues in contemporary commerce conflicts. Recent Cases demonstrate that Agribusinesses in general are not at a very high level of security, States and private companies need to invest heavily on dialogue and cyber risk management to specify minimum cyber security requirements for companies.

Perhaps, States that hold a great dependency on their agricultural exports for internal revenue, such



May 3, 2022

- AGCO makes donation to Ukrainian Farmers Relief Fund

May 5, 2022

- AGCO suffers a ransomware attack

May 6, 2022

- AGCO publicizes press note admitting to the ransomware attack
- USA based dealerships complain that AGCO order systems are down and that orders are backlogged

May 16, 2022

- AGCO reported that there had been data exfiltration, but it had no privacy-protected consumer data involved.
- AGCO said they would mitigate any production loss by increasing production in 2022.

Figure 3.6: Timeline of the AGCO case.

as Brazil, ought to reevaluate their definitions of critical infrastructure in order to embrace agribusinesses and supply chains, for a more up-to-date and commercial centered definition of Critical Infrastructure. Sector-specific rules should consider the national economic risks of disruption. Regulation for mandatory following of basic steps could begin a small revolution in the sector:

- Hire an Experienced Cyber team;
- Keep Security Software updated;
- Use Multi Step authentication;
- Teach Cyber Vigilance to employees.

On the other hand, the USA is sending a clear message regarding its growing interest in the sector. One might argue that the rise in supply chain attacks may be due in part to improved defenses against more rudimentary assaults, as it was seen in the USAHERDS, Section 3.4, and the John Deere, Section 3.3, cases.

Since the Colonial pipeline attacks the White House has sent a clear message that Homeland Security and corporate America top priority is to confront cyber attacks and information warfare. one might argue that the rise in supply chain attacks may be due in part to improved defenses against more rudimentary assaults.

Considering cyber offense trends, countries with great dependability on world commerce and their exports need to adapt to the contemporary commerce world and introduce themselves to this interconnected war with investment and planning. Cyber threats grow rapidly promoted by the rise of digitization, this expansion comes with dangers and target amplification. Businesses digitization courses may only be successful if proper cyber security techniques are employed [6]. In this ambience, cyber attacks have become more common, below we present recent cases of cyber attacks against agribusiness sector and relevant supply chain providers in chronological order.

ENISA admits that nowadays most states all over the world conduct cyber operations to accomplish their strategic goals, so it is a given that there is a cyber arms race towards the implementation of cyber capabilities [42]. Considering the cyber offense trends, States with great dependability on world commerce and their exports need to adapt to the contemporary commerce world and introduce themselves to this interconnected war with investment and planning. Such initiation may be through initiatives related to regulation and protection of their critical infrastructure, passing through creating a fluent dialogue between interested private and public entities or even by investing in their own cyber capabilities.

Cyber threats grow rapidly promoted by the rise of digitization, this expansion comes with dangers and target amplification. Therefore, digitization must be rethought to include information security at higher priority, in a sense that it and becomes the foundation of all digitization processes. Businesses digitization courses may only be only be successful with proper cyber security techniques are employed [6]. In this ambience, cyber attacks have become more common, bellow we present recent cases of attacks against agribusiness sector and supply chain providers with focus on attacks against beef producers.

Aside from regulation talk, countries might take other actions to target critical infrastructure cyber protection. Small and medium businesses need information and support to enter this high-tech environment with even a slim chance of securing themselves from attacks. Specifically, for the Brazilian beef agribusiness sector, this is a reality since many of our breeders fit such a category. Countries must also adopt Cybernetic Security as one of their political protection agenda points when negotiating with other nations. Attackers must be pressured and unveiled as wrongdoers. Finally, investigative teams must be attentive to choke points that aid attackers such as political shelter or financial outlines.

3.7.1 FBI Takes a Stand

In April 2022, the American Federal Bureau of Investigation (FBI) released a Private Industry Notification warning on ransomware attacks targeting the U.S. agricultural industry and admitted to coincide with critical seasons in the industry. The goal was to inform Food and Agriculture sector partners about the likelihood of ransomware actors to attack agricultural cooperatives during critical planting and harvest seasons, in order to disrupt operations, cause financial loss, and negatively impact the food supply chain.[55]

On the document The FBI noted ransomware attacks during these seasons against six grain cooperatives during the fall 2021 harvest and two attacks in early 2022 that could impact the planting season by disrupting the supply of seeds and fertilizer.

Also it indicates that cooperatives are deemed as lucrative targets because they hold a time-sensitive role in agricultural production.

The document elaborates on concerns about the agricultural industry and it suggests that members of such sector should patch all systems in their organization's environment to have a robust monitoring of the environment. The FBI's warning recommended a series of steps to be considered by cooperatives in order to mitigate ransomware attacks:

- Regularly back up data, air gap (a security measure that involves isolating a computer or network and preventing it from establishing an external connection), and password protect backup copies offline.
- Ensure copies of critical data are not accessible for modification or deletion from the system in which the data reside.

- Implement a recovery plan that includes maintaining and retaining multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Identify critical functions and develop an operations plan in the event that systems go offline. Think about ways to operate manually should it become necessary.
- Implement network segmentation.
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts and use strong pass phrases where possible.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Require administrator credentials to install software.
- Audit user accounts with administrative or elevated privileges and configure access controls with least privilege in mind.
- Audit user accounts with administrative or elevated privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on cyber security awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).

If we scrutinize the suggestion list above and compare it to other security patterns and arrangements as they are suggested by specialized institutions such as ITU, NIST, CISO or even to regulations released by OECD on Information Security and Privacy Protection, it will be clear that the suggestions do not carry any originality nor innovation in the Information Security field. From that we may conclude that the agricultural sector is in need of an update of its Security Awareness Level and that the sector is, in fact, a high-demand target in the new world where Cyber Security is a major concern to basic Supply Chain Sectors.

Despite all efforts to reduce attacks it is noticeable that this has not expanded the industry's capacities to handle the issues, once that most of the cases could have been prevented if basic security command follow ups would have been put into place. Even though best practices are known and that Security regulations and knowledge base is up to date the everyday practices and basic mistakes show that the real work is done otherwise, so we mouth to rethink how to share basic information and educate CI responsibles.

Deterrence techniques, management behaviors, information security culture and awareness play a vital role into creating a secure prone environment, according to Ali [56], all those steps may be summarized in the need to substantially improve training and human capacities in the security sector.

When it comes to security behavior and issues, many researchers argue that punishments and deterrence are not always the right way to mitigate non-compliance to security guidelines. Studies demonstrate the need for more robust institutional controls that considers both intrinsic and extrinsic motivations of attackers and of institution members in protecting its information. There are four modes of information security behavior:

- not knowing-not-doing
- not-knowing-doing
- knowing-not-doing
- knowing-how

All of those contribute to the security culture, and researchers argue that employee knowledge and skills significantly affect security and build a good safety culture [56]: "employees often consider information security to be the responsibility of the IT team, so they are not part of IS security themselves. To change employees' views, organizations must cultivate a good safety culture, and senior management must play its part."

3.8 SUMMARY

We present the increase of the prevalence of cyber operations conducted by states worldwide, even through the existence of a cyber arms race towards the implementation of cyber capabilities. In this regard, we suggest that nations with significant dependence on world commerce and exports ought to adapt to this interconnected war by investing in and planning for cyber offense trends. Such actions go through the definition, regulation and protection of a nation‘s critical infrastructure. To prove this point, we presented a short study of the most recent cyber attack cases that affected the food supply chain with a time-frame for each case. Finally, we presented recent actions from public institutions in attempts to reduce case occurrences and mitigate cyber risk related issues. All to make clear that the prevalence of cyber operations conducted by states is a significant issue that requires attention. By investing in and planning for cyber capabilities, nations can better protect themselves and their commerce interests in the face of the ongoing cyber arms race of nowadays.

4 PROPOSED METHODS AND CRITERIA EVALUATION

In order to develop a reliable model that will lead to relevant and timely intelligence formulation for decision makers, it is crucial to follow a design methodology. Our proposed six-stage methodology cross references political and economic factors to create a realistic list of interested parties. This allows us to specify countries that have capacity and intent to act if find action necessary. The methodology was previously published on a journal after peer review according to Trinks et al [57].

While our methodology focuses on the Brazilian beef market interests, it can be replicated for other products and markets as well. When following our methodology, we were able to develop a reference model that is based on a rigorous analysis of political and economic factors, which ensures that our results are objective. We understand that our methodology can be a valuable tool for researchers and practitioners alike who are interested in developing trustworthy models for intelligence formulation.

Following a design methodology is crucial for the development of a trustworthy model that may lead to relevant and timely intelligence formulation to decision makers. In this sense, We propose a six-stage methodology that cross references political and economic factors in order to create a realistic list of interested parties and, therefore, be able to specify countries that are most likly to be part of a specific product threat.

4.1 STEP 1

First step is designed to extract large producers of a product that have a dependency or an economic interest in the export or world market of such product. It is important that only stakeholders that are included in the market be considered, once we have established that Cyber Operations are costly of time and resources, it is only plausible to consider Countries or parties that hold real economic interest in the market in a threat intelligence report, see Table 4.1 for visual.

The goal of this step is to identify the largest producers of the product who have a significant economic

Table 4.1: Largest Beef Producers and Export Rate.

Country	Beef Production (milTEC *)	Export/Production % (mil TEC)
USA	12,347.7	9.94
Brazil	10,187	26.42
European Union (EU)	7665.7	44.73
Argentina	3178.5	27.06
India	2474.9	31.2
Australia	2078	66.79
Canada	1304.7	36.15
New Zealand	703	84.41
Ireland	649	86.97
Poland	605.1	100.15
Uruguay	514.5	74.19
Netherlands	396.3	162.41

* Thousand Tons of Carcass Equivalent.

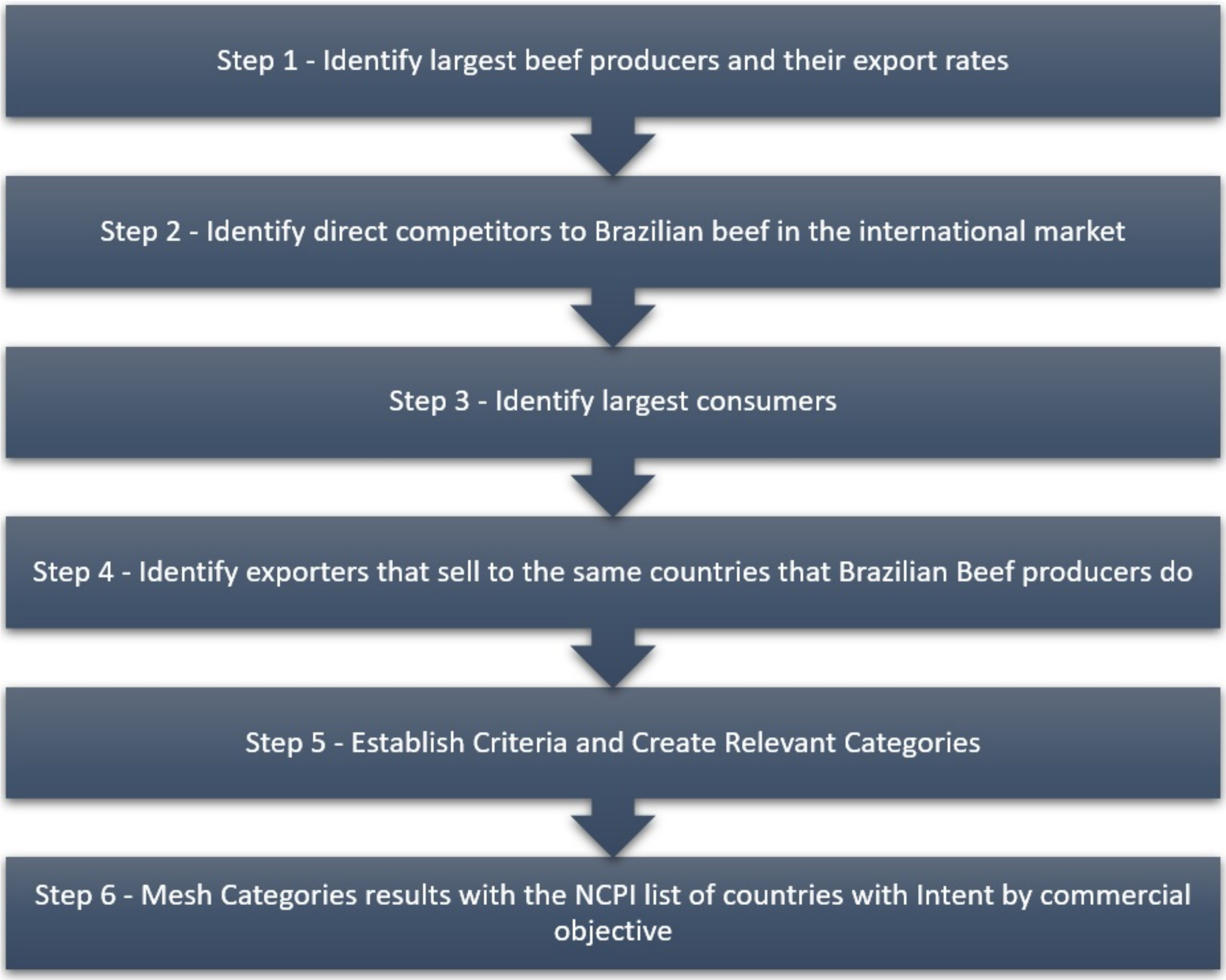

Step 1 - Identify largest beef producers and their export rates
Step 2 - Identify direct competitors to Brazilian beef in the international market
Step 3 - Identify largest consumers
Step 4 - Identify exporters that sell to the same countries that Brazilian Beef producers do
Step 5 - Establish Criteria and Create Relevant Categories
Step 6 - Mesh Categories results with the NCPI list of countries with Intent by commercial objective

Figure 4.1: Methodology to find Brazilian beef contenders with cyber attack capacities and intent.

interest in the export or world market of that particular product. These producers not only dominate the market but also have a major role in shaping the industry trends and pricing, see Table 4.2 for visual.

Typically, these large producers are multinational corporations with significant investments in the industry. They have a considerable stake in the market and often engage in price wars and other competitive tactics to maintain their position. These players, therefore, have a significant impact on the production and supply chain of the product.

Identifying these key players through market research and analysis is vital in developing a strategy to enter the market or expand an existing business. Their market share, production volume, pricing strategies, and distribution channels provide insights into the dynamics of the industry, which can be used to develop effective marketing and distribution strategies. The first step also highlights areas where there is a high degree of dependence on these large producers, which can aid in negotiating favorable contracts or partnerships. Overall, identifying key international players in a specific product market is critical to developing a comprehensive understanding of the industry and establishing a successful business presence.

4.2 STEP 2

Second, we focused on finding direct and de facto competitors of Brazilian beef in the international market. To reach that end we identified top exporters, then we intersected the top exporters list to the findings of Step 1 to understand if the largest exporters list is congruent to the largest producer one. After, we assessed and compared the lists and we could name which countries are actively involved in the beef world market competition as exporters.

Brazil is considered one of the world's largest exporters of beef, accounting for about 20% of the global market share [6]. Competitors in the international market for Brazilian beef can be categorized into two groups: direct and de facto competitors.

Direct competitors are those countries that export beef to the same markets as Brazilian beef, with similar product quality and pricing strategies. Some examples of direct competitors of Brazilian beef are Australia, Uruguay, and Argentina. These countries have a strong tradition of beef production and export, and they have been increasing their market share in recent years. To maintain its competitiveness, Brazil has been investing in technology and quality control systems to improve its product and reduce costs.

De facto competitors, on the other hand, are countries that do not export beef but have similar characteristics and can potentially enter the market. These countries may have lower production costs, less stringent regulations, or a comparative advantage in a specific market segment. For example, the United States and Canada have a large domestic market but are not significant beef exporters. However, they have the potential to be de facto competitors if they decide to increase their export volumes or target specific markets, such as Asia.

Finding and analyzing direct and de facto competitors of Brazilian beef in the international market is essential for developing strategies to maintain or increase market share. It involves identifying market trends, evaluating product quality and pricing, understanding customer preferences, and assessing competitors' strengths and weaknesses. By doing so, Brazilian beef producers can improve their competitiveness and secure a prominent position in the global market.

In this regard, we listed the largest beef producers in the world, then, we analyzed if their export rate

Table 4.2: Largest Beef Importers and Consumers.

Country	**Imports (milTEC)**	**Importers of Brazilian Beef in Percentage**
EU	5886.7	6.24
China	2223.4	50.8
USA	1459.3	41.67
Hong Kong	619.6	60.81
Netherlands	472.2	32.9
Italy	424.4	9
Egypt	403.9	41.67
Russia	344.8	21.69
Chile	283.1	41.69
Uruguay	46.7	74.96

was indeed significant for the whole country export revenue. So we cross referenced the list of the largest producers with their consumption rate. The idea is to understand if among big producers that are also large consumers that may not be interested in the export market. So we are able to extract countries that are realistically interested in the world market as stakeholders, once they are big sellers of the product. The analysis resulted in a list of countries where beef exports have significance for the whole country export revenue, ergo countries that have true economic interest in the international beef market.

4.3 STEP 3

Third, we considered the role biggest buyers play in the market, not only to have a wider understanding of the market but also to make sure what countries rely on Brazilian and foreign exports to guarantee their product supply. Thus, those countries' interests are presented in terms of price perspective, as well as for the guarantee of access to good product according to food safety and security issues.

When examining the role of the biggest buyers in the market, the main objective is to gain a better understanding of the market dynamics. It is important to recognize what countries rely on Brazilian and foreign exports to ensure their supply of products. Identifying the biggest buyers in the market is key to understanding who is driving demand. In doing so, we are able to understand the potential impact these factors may have on pricing and supply chain logistics, see Table 4.3 for visual.

In the pursuit of understanding the global dynamics of the beef industry, we have undertaken a rigorous analysis of the biggest buyers in the market. In the second part of Step 3, we scrutinized the list of the biggest buyers to understand how much of its purchase was coming from from Brazilian Producers. That is valuable to clear what is the impact of the Brazilian Beef in each of those economies, see Table 4.5 for visual.

Our analysis revealed that a significant portion of the purchases made by the biggest buyers was indeed from Brazilian producers. This finding sheds light on the important role that Brazil plays in the global beef market. It also highlights the potential impact that any changes in the Brazilian beef industry could have on the economies of these buyers.

Furthermore, our analysis allowed us to identify consumers that also hold interest in the market. This information is valuable not only for Brazilian producers but for all stakeholders in the beef industry who seek to understand the global dynamics of the market.

Furthermore, it is crucial to recognize that the interests of the biggest buyers are multifaceted. They are concerned not only with price perspective but also with the quality and safety of products. This is particularly important in the context of food safety and security issues, where countries need to ensure that the food they import meets stringent health and safety regulations. Therefore, it is important to recognize that the interests of the biggest buyers go beyond price and also include access to high-quality products that meet their food safety and security requirements.

Overall, acknowledging the role of the biggest buyers in the market is essential for understanding the broader landscape of the industry. It helps to identify key drivers of demand and highlight areas that may require additional attention, such as compliance with food safety and security regulations. By recognizing the interests and perspectives of these buyers, we are better equipped to make informed decisions and navigate potential challenges in the market.

4.4 STEP 4

Fourth, we identified which countries were direct competitors of Brazilian beef in its specific importer markets. For that to occur, we listed main providers of beef to each of the biggest buyers that were found in the third step to reach a list of the countries that export to the same countries that Brazil does, see Table 4.4 for visual.

Brazil is one of the largest exporters of beef in the world, but it faces strong competition in its specific importer markets. Each country has its strengths and weaknesses. For example, Argentina is known for its grass-fed beef, while Australia is known for its high-quality grain-fed beef. Canada, on the other hand, benefits from its proximity to one of the largest importers, the U.S.A, and from the fact that it is a NAFTA member.

The EU, for example, has strict hygiene and sanitary regulations, so only countries that meet these standards can export their beef to the EU. Uruguay has an advantage in this market because it has a Free Trade Agreement with the EU, which allows its beef to enter the market with low or no tariffs.

In China, Brazil competes with Australia and Uruguay. These countries are the main providers of beef to the Chinese market. China is the largest importer of beef in the world, and it has strict regulations on imports. Uruguay has an advantage in this market because it was the first country to sign a protocol with China that allows it to export bone-in beef [19].

Brazil faces strong competition from other countries in its specific importer markets. These countries have their advantages and disadvantages, but they all aim to provide high-quality beef to the same customers as Brazil.

4.5 STEP 5

The criteria established in the previous steps lead us to understand the competition and identify contenders according to economic and political interests. It is noteworthy that assessment showed that, to find the contenders in a specific market, a country must consider not only its own exporters but also importers interests and big producers' strategies within the world market. Hence we reached the following five ca-

Table 4.3: Brazilian Beef Conceivable Contenders, Step 6 of the methodology (Section 4.6).

Brazilian Conceivable Contenders in the Beef World Export	**Number of Categories Mentions**	**State Ranked on the NCPI**
USA	5	9th
Australia	5	8th
EU	5	N/A
New Zealand	4	N/A
Uruguay	4	N/A
Argentina	4	N/A
Mexico	3	N/A
Canada	3	N/A
India	3	N/A
China	3	2nd
Netherlands	3	6th
Ireland	2	N/A
Russia	2	10th

Table 4.4: Competitors within Consumer Markets.

Country	**Beef Export Competitors (Source ITC)**
EUA	Australia, New Zealand, Nicaragua, Uruguay, Mexico, Canada, Japan
China	Australia, New Zealand, USA, Argentina, Uruguay, Brazil
EU	Brazil, Australia, USA, India, New Zealand, Local producers
Chile	Brazil, Paraguay, USA, Argentina, Uruguay, China
Egypt	Brazil, India, Paraguay, Colombia, Australia, New Zealand
Russia	Brazil, India, Paraguay, Belarus, Argentina, India, Colombia

tegories of participants in the world market, each category holds a list of countries (see Tables for visual aid):

- Countries that produces the most, result of Step 1 (named ‘Producers’ in Table 4.1);
- Countries that exports the most, result of Step 2 (named ‘Exporters’ in Table 4.2);
- Countries that compete directly against Brazilian product because they share clients, result of Step 4 (named ‘Competitors’ in Table 4.4);
- Countries that imports more from Brazilian product, first result of Step 3 (named ‘Importers’ in Table 4.5);
- Countries that consume more beef in the world, second result of Step 3 (named ‘Consumers’ in Table 4.3).

4.6 STEP 6

After establishing a list of contenders from a political and economic perspective, we intersect the results with the NCPI index as mentioned in 2.4.2. We check what countries are mentioned in at least three categories of Step 5 and that are also listed in the NCPI top 10 Index that considers intent and capability to find "most comprehensive countries"with the highest level of Intent Ranking by Commercial Objective. Once we intersect that information we are able to come up with the result of a list of countries that are agribusiness contenders and that hold cyber capacities and have intent to actively use Cyber tools to protect its interests in the beef sector.

4.7 RESULTS AND DISCUSSIONS

In this section, the methodology presented in the last section is put in action as the international beef market is analyzed and presented with focus on our objective in order to find list of countries to be assessed and compared to the index previously explained in Section 2.4.2. We use trade numbers collected at the open platform of the International Trade Centre’s (ITC), a joint agency of the WTO and the United Nations, whose mission is to foster sustainable economic development and contribute to achieving the Millennium Development Goals in developing countries and countries with economies in transition through trade and international business development [58].

4.7.1 Identification of the Largest Beef Producers

We analyzed the significance of beef exports for the overall export revenue of different countries. To achieve this, we have utilized data from ITCtrademap and have followed Step 1 (see Section 4.1) [58]. Our findings, as presented in Table 4.1, reveal that the beef market is complex and requires a deeper understanding of the numbers to identify contenders appropriately. At this stage we identified the following coutries:

Table 4.5: Criteria comparison of all stakeholders.

Countries	Producers Step 1	Exporters Step 2	Importers Step 3.1	Consumers Step 3.2	Competitors Step 4	Mentions Step 5
Argentina	X	X	N/A	X	X	4
Australia	X	X	N/A	X	X	4
Canada	X	N/A	N/A	X	X	3
Chile	N/A	N/A	X	X	N/A	2
China	N/A	N/A	X	X	X	3
Egypt	N/A	N/A	X	X	N/A	2
EU	X	X	X	X	N/A	4
India	X	N/A	N/A	X	X	3
Ireland	X	X	N/A	N/A	N/A	2
Japan	N/A	N/A	N/A	X	X	2
Mexico	N/A	X	N/A	X	X	3
Netherlands	X	X	X	N/A	N/A	3
New Zealand	X	X	N/A	X	X	4
Poland	X	X	N/A	N/A	N/A	2
Russia	N/A	N/A	X	X	N/A	2
Uruguay	X	N/A	X	X	X	4
USA	X	X	X	X	X	5

4.7.2 Identification of Exporters of Beef in the International Market

We analyzed the congruence between the largest exporters and the largest producer states in the beef market. Our analysis was based on the information extracted from the production. The objective was to identify the countries that are competing in this market.

Our findings indicate that the interested countries in the exporter market are virtually the same as those in the largest producers list [19]. As per Step 2 (see Section 4.2), we analyzed Table 4.1 and identified the following list of countries potentially interested in the international market: Brazil; Australia; USA; Argentina; India; Netherlands; Poland; New Zealand; Ireland; and Canada.

Notably, the United States is the largest producer of beef, with nearly 10% of its production being exported. This export rate is significant, considering the large amount of production in the country. Moreover, other major producers such as Australia, New Zealand, Ireland, and Uruguay have an export rate of production higher than 50%, indicating their producers' dependence on exports and the world market.

Interestingly, the Netherlands and Poland are exporting more beef than they are producing, which suggests that they are importing to meet their export demands. This observation highlights the interconnectedness of the global beef market and the need for a comprehensive understanding of the trade dynamics involved. Our study sheds light on the importance of beef exports for the overall export revenue of different countries and underscores the need for further research to fully comprehend the complexities of the market.

These countries play a crucial role in the global beef market and their participation in the market is significant. That provides valuable insights into the beef market and it may be of use to policymakers to make informed decisions.

4.7.3 Identification of the Largest Importers and Consumers

In accordance to Step 3 (see Section 4.3), we assessed which countries are the largest importers in the world market and how much of their intake comes from Brazilian products [58]. Table 4.2 displays how Brazil represents a large portion of all those markets.

In this step we determine the largest importers in the global market and their reliance on Brazilian products as per data from ITC Trademap [58]. The results of our analysis are presented in Table 4.2, which indicates the significant share of Brazilian products in these markets.

As we observe that Brazil's products are well-represented in the import markets of various countries across the world, Brazil's presence in those countries as a major exporter is not a recent development. Our findings corroborate that Brazil play a relevant role on all markets shown on 4.2. We call attention to the EU and Italy number, which is lower than 10% due to the division of sales in the ITC methodology concerning the EU. Also, it is important to mention that the EU is not studied as one nation in the Cyber Security Index, which turns it into an unique case to be studied more deeply in the future.

Overall, step 3 highlights the importance of Brazil's position in the global market, particularly in terms of its contribution to the import markets of several countries. The insights gained from our analysis understand which countries are more reliant on Brazilian product.

4.7.4 Identification of Competitors

Exporters That Sell to the Same Countries That Brazilian Beef Producers Do

In accordance with Step 4 of our analysis (see Section 4.4), we present the next assessment in Table 4.4 to comprehend the direct competitors of Brazilian Beef in the importing markets because those Countries are exporters that sell to the same countries that Brazilian Beef Producers do.

Our analysis is based on the fact that the countries mentioned in the table target their export to the same countries as Brazil. The assessment has led us to identify ten countries as direct competitors of Brazilian Beef in the importing markets. These countries are Australia, New Zealand, Uruguay, Mexico, Canada, Japan, USA, Argentina, India, and China.

It is important to note that the identification of the direct competitors of Brazilian Beef in the importing markets is crucial for strategic planning. In conclusion, our analysis has identified ten countries as direct competitors of Brazilian Beef in the importing markets.

4.7.5 Establishing Criteria in Accordance to Relevant Categories

In this study, we aimed to evaluate the active participants in the world market that hold interest in the Brazilian participation. To achieve this goal, we followed the five-step approach outlined in Section 4.5. After gathering the results from all previous assessments, we were able to identify five categories of active participants that required evaluation.

In accordance with Step 5, we intersected the five categories and identified the players that appeared in at least 3 out of the five categories. The results of this analysis are presented in Table 4.5. It is worth noting that the classification of the identified players was based solely on their level of interest in the Brazilian participation in the market.

Our findings provide valuable insights into the active participants in the world market that hold interest in the Brazilian participation. Overall, our study highlights the importance of a systematic approach to evaluating active participants in the world market.

After gathering the results from all previous assessments, we reached five categories of active participants in the world market that needed evaluation. In accordance with Step 5 (see Section 4.5), we intersected the five categories and we were able to spot the players that hold interest in the Brazilian participation in the market. We listed the players that appeared in at least in 3 out of the five categories, and the results lead to the classification shown in Table 4.5.

4.7.6 Meshing Categories Results with the NCPI Index

In our research, we have taken the necessary steps to analyze the intersection of political and economic matters with a country index that considers CTI principles. Our focus has been on commercial interests in agribusiness markets, specifically in the beef sector of Brazil.

After going through the first steps that considered political and economic matters, it was necessary to out intersect those results with a country index that considered CTI principles. It has been shown that the analysis of cyber power is the product of intent and capability [44] for multiple cyber objectives, with a specific aim to provide an Intent Ranking according to commercial objectives and assess the proposed multidisciplinary intersection in accordance with Step 6 (see Section 4.6). The focus of the analysis was on commercial interests in agribusiness markets; thus, we were able to list the main Brazilian Agribusiness World contenders with Cyber Capabilities in the Beef Sector, as presented in Table 4.3.

Our research has shown that the main Brazilian Agribusiness World contenders with Cyber Capabilities in the Beef Sector can be listed using this approach. The results of this analysis are presented in Table 4.3.

It is important to note that our research has focused solely on the beef sector of Brazil. However, the methodology used in this study can be applied to other industries and sectors as well. By considering both intent and capability, we can provide a comprehensive analysis of cyber power and its impact on various industries.

4.7.7 Cyber Security Contenders to the Brazilian Agribusiness in the Beef Sector

Note that, for those states that have not received an applicable grade that does not mean they do not have Cybernetics Commercial Objectives and capabilities. It is merely a categorization fact that they were not ranked in the top 10 countries as such.

The EU and Russia are special cases that need clarification. First, the EU group of countries is not listed as one country when it comes to the NCPI ranking system, so, even though it receives 5 mentions as a player of interest in the market, we could not place it in a specific rank grade when it comes to cyber capabilities. That does not mean the EU or its members do not hold or could not act to favor its interests in cyber space.

It is noteworthy that, in terms of intelligence, some EU countries maintain a traditional history of protecting their commercial interest. Finally, when it comes to Russia, recent chapters of world history regarding Ukraine have shown Russia's growing intent of using its cyber capabilities to protect its own interests. Thus, despite the fact that it received only 2 mentions in the market players charter, it is not a contender to be taken lightly.

Finally, we reached a list of five contenders to the Brazilian Beef in the International Market that hold cyber attack capacities; the list includes the USA, Australia, China, Netherlands and Russia.

4.8 DISCUSSIONS

In the competitive world presented in Section 2.2.1, it is primordial to guarantee useful production intelligence to subsidize the decision making process and to defend against possible threats as successfully as possible. This context lead us to cross-reference the economic interests of rival states to Brazil on the specific product market according to International Relations principles versus the operational threat intelligence information and capacities of such states.

One must consider the principles and structure presented by the concept of SEI as it introduces the need for broad governmental approaches that give the issue the necessary applicability with a focus on producing quality intelligence and visualization in a timely manner.

Current international relations require [9]

> *"organizations looking to have technical threat intelligence are now overwhelmed with a massive amount of threat data, leaving them with the huge challenge of identifying what is actually relevant. Thus, a problem of quantity over quality has been developed."*

In this context, the objective is to produce structured information that will give strategic CTI directives about what states are most likely interested in Brazilian exports of beef, and what their cyber capabilities are in a hypothetical attack scenario according to Section 2.4.1.1. This may produce knowledge to support threat categorization and defense prioritization for Brazilian Beef Exporters as we propose in the results section of this work.

In regards to countries' capacities, we start with the public knowledge that the United States has done a number of exercises on cybersecurity, but the results of some are highly classified, making it difficult to evaluate the actual risks present on the cyber domain. Other countries, notably Russia and China, were able to recruit cyber volunteers (both internally and in the diaspora) for militia-like attacks. Cyber conflict is a general term that goes from low-level intrusions, through apt ransomware attacks, or even petty crimes to create spam networks, up to high-scale, state-sponsored cyber warfare and influence operations.

The U.S. beef industry competes with Canada, Australia, New Zealand, Brazil, Argentina, and Uruguay for the export market. In this scenario, even though significant trade barriers exist, there are still opportunities as beef consumption rapidly grows and creates room for global expansion of the beef industry [59]. This means that buyers also have an interest and play a role in the market, not only in the interest of price, but also for the guarantee of access to good products according to food safety and security issues, as seen in Section 4.7.3.

On the other hand, cybernetic cases like Stuxnet, Flame and Duqu cyber campaign against Iran (codenamed Olympic Games) in 2009–2010 and WikiLeaks' release of thousands of diplomatic cables pertaining to the US State Department and its Missions abroad 2010–2011 have clearly exposed state activities on the edge of legality in order to reach its goals, according to Gamero-Garrido [60]. In this context, major global commerce players should be aware of other players' capacities and the possible ways they might act.

The work of Gamero-Garrido [60] demonstrates that, even though cybernetic conflict cases in the last

30 years were diverse in their scope, actors, tools used, and outcome, it is safe to say the majority of those cases fit one of the following categories: espionage, attack or warfare, and public release of secret government information.

Cyberspace introduced a new field of play to International conflict of interests, and organizations are bound to conform to this reality. Traditional actors have increasingly recognized the importance of the domain, and they are investing in strategies to assert themselves. Actions range from proposals of cybernetic global regulation, through expansion of International cooperation, including both public and private actors, and a closer involvement/monitoring of critical private sectors.

All in a context where cyberspace remains unstructured, according to Cardon [61]:

> *"Especially when considered in the context of a political map, detailing the physical and sovereign boundaries between nation states. Without physical delineations to define jurisdictions, the established law, authorities, regulations, processes, structure, and concepts applied to the cyber domain are still in flux for both the public and private sectors."*

Thus, deterring, detecting, mitigating, reporting, and monitoring are the set list for defenders. They must act not only according to the sector's needs but also considering CTI specifications (as discussed in Section 2.4.1.1). Best practices nowadays dictate multidisciplinary teams, and protection planning following strict risk assessment in order to reach security levels that hold all, from supply chain risks to internal attacks, in a joint effort from private and public bodies.

For example, the US Government announced that their intelligence would conduct a 60-day "sprint" exercise focused on battling ransomware and for that they provided USD 25 million in grants to state and local cybersecurity preparedness programs with a particular focus on combating ransomware. CISA also announced it would begin to use new administrative subpoena powers authorized under the 2021 National Defense Authorization Act to help it address ransomware attacks and other cyber threats [62]. Finally, the Justice Department created a new task force dedicated to rooting out and responding to the growing threat of ransomware [63]. This initiative demonstrates how one of the contenders found in this work is acting on the matter.

Russia, another example from our contender's list, is amid a public battle with the American White House because they imposed new sanctions on six Russian technology companies that provide support to the cyber program run by Putin's intelligence services linked to the hacking of the SolarWinds information technology company. The Homeland Security and Governmental Affairs Committee introduced bipartisan legislation to provide additional resources and better coordination for serious cyber attacks or any breaches that might risk the safety and security of Americans. The Ukrainian War is not mentioned here because it would need specific assessment of its own.

As for Brazil, the country seems to be taking slow steps into this new geopolitical reality. The Brazilian National Cyber Security Strategy (E-Ciber) addresses issues of cyber security of critical infrastructure and guides cyber defense [64]. Also, the National Defense Strategy (NDS) recognized the necessity to invest on Cyber Security that is independent from other nations in order to have an updated national defense system. Brazil should not be subject to foreign technology. However, both texts are silent on the matter of protection of commercial interests [64].

When it comes to cyber security, there is a knowledge gap between Brazilian capacity when compared to other countries. Episodes such as the Snowden case and the Stuxnet malware have brought notoriety to the matter [65]. It is relevant to point our that some of the countries publicized in those episodes are contenders to Brazilian Agribusiness [6], and there is nothing stopping them from using available cyber resources to benefit their industries in commercial negotiations [66].

In this setting, identification and protection of privileged data is fundamental to facing the market competitively. Thus, it is crucial to identify threats, threat actors and their capabilities, in order to prepare [67]. Cyber Threat Intelligence (CTI) has developed into a necessity so that agribusinesses are able to manage risk accordingly, become aware of vulnerabilities in time, and produce pertinent intelligence. Similar to other industries, protection of strategic data is a requirement for the preservation and expansion of Brazilian Agribusiness interests in the global market. Strategic actions to value Brazilian agribusiness must start with proper cyber security precautions.

4.9 SUMMARY

In this chapter we present a methodology of our creation to reach a trustworthy model when identifying possible State Contenders with the capacity and motive to act for the sake of a certain asset. We present our proposed six-stage methodology that cross references political and economic factors to create a realistic list of Countries. This allows us to specify countries that are most likely to be part of a specific product threat. While our methodology focuses on the Brazilian beef market interests, it can be replicated for other products and markets as well. The proposed reference model was designed through the analysis and abstraction of the elements and practices considered in the Related Works Section of this dissertation.

The methodology suggested develop a reference model with focus on the Brazilian beef market interests, but it may be replicated to other products and markets as well. Nevertheless, as stated by Ahleman et all [68], for the development of new research areas, when there are not accepted definitions and reference models, a reference model may be designed through the analysis and abstraction of the elements and practices proposed in the bibliography.

This model may be replicated to formulate relevant and timely intelligence to decision makers in other sectors, following necessary adjustments according to the sector. After all, following a design methodology is essential in the development of a trustworthy model that can lead to successful intelligence formulation.

Based on the above, we follow a six-phase design methodology, this is the foundation for developing our proposed CTI reference model that considers points and queries consistent to the specific objective of this dissertation, which is to reach the objective of identifying Brazilian contenders in the beef market with cyber capabilities and commercial interest to act in favor of their interests. To answer such an issue, we created a methodology which is presented below Step-by-Step, see Figure 4.1 for visual.

By utilizing our methodology, we were able to come to reliable and effective reference model that lead us to a list of 5 contenders to the Brazilian Beef in the International market that hold cyber attack capacities and motive to act for the sake of a certain asset.

5 CONCLUSIONS AND FUTURE WORK

This dissertation proposes an assessment scheme that interfaces economic and political interests against potential cyber attack. In Section 2, we were able to introduce an analytics interface that targeted academic and corporate issues. In Section 2.4.1, the CTI matter was explained and connected to the agribusiness sector. We classified the main state contenders of Brazilian beef agribusiness, through the crossover of economic, political, and CTI evaluation. We believe that the intersection of CTI with economic and political components may lead to thorough and updated assessment for the unveiling of potential cyber threats.

It was possible to reach the goal of proposing a strategic assessment to introduce an analytics that target both academic and corporate issues based on CTI principles. Therefore, we were able to arrive at a list of the main state contenders of Brazilian meet agribusiness, as well as their cyber attack capacities, through economic, political, and CTI evaluation.

The main contribution of this study is described in Section **??**, where we present a model to assess information to threat analysis of potential contenders. We believe such information is primordial to improve threat mitigation through the early diagnosis of potential threat actors while considering the creation of intelligence based on CTI principles. The Brazilian authorities may advance their planning on how to understand and classify the Food Sector within the scope of the Country's Cyber Security Legal Protection Framework. In Section 2.1, we discussed how such a business sector is already considered Critical Infrastructure in many other nations.

Despite this, legislative differences between CI definitions reflect national preferences, realities and needs. In addition to the core role that Brazilian agribusiness play world wide, one must wonder whether the Brazilian CI definition should be modernized to include agribusiness to obtain a fuller and up-to-date understanding of the cyber capabilities international scenario so that one may adapt appropriate defense mechanisms through mandatory security measures.

It is important to mention that the recent [69] article on the risk of fake controversies for Brazilian environmental policies was refuted by Embrapa. The Brazilian agriculture research company asserted that the Brazilian agribusiness has become the main focus of attacks nationally and internationally to create a negative image, reduce internal support, and disperse international consumers. The discussion is controversial considering the public dispute between academia and the heads of Embrapa, and it requires further investigation.

Also, competition is varied and fierce when it comes to agribusiness. Current commercial relations put Brazilian agricultural commodities in constant conflict for market and pricing to benefit its products. In 2019, Brazil was the largest exporter of beef in the world but, on the other hand, the average price of Brazilian product was among the cheapest when compared to 20 other exporters [6]. Such information alongside the findings in this work may lead to a deeper assessment on the influence front using cyber tools as well.

Finally, our results show that we are able to draw a list of threat actors that may act or have the potential to act in the cyber world against the Brazilian Beef Production Chain. Besides this, the analysis shows characteristics of each state regarding how they usually act in this space. In itself, this may support other relevant assessment for intelligence gathering on potential risks, actors, and actions.

For future work, it is necessary to deepen the research on each contender and its history in attacks to fully understand what capabilities each holds, and how to properly analyse risk based on those capabilities, history, commercial context and intent, and with CTI principles at hand. On the other hand, we did not undertake a detailed and specific analysis about each country's cyber attack capacities; thus, future work may include further analysis on that front.

The EU case is enlisted for future work, once the countries are understood separately that within the NCPI criteria, but they are taken as a group in the ITC trade map. Hence it is necessary a specific study to untangle how the beef supply chain works inside the EU and only then be able to compare it to the NCPI results.

Also, deterrence techniques, management behaviors, information security culture, awareness, in sum cyber security training of all levels is the key to create more secure institutions. Such capacity building may only happen through strategic awareness and massive educational investments on operational, technical and leadership levels. Change in regulations is needed but it must not be seen as the only spark that may light the way.

Finally, this dissertation is not intended to present a risk assessment nor a risk evaluation model as that would require a specific line of research and the strategic assessment of its own with characteristic scenarios, definitions for risk levels and mitigation. It is our understanding that is a future Step to this study.

BIBLIOGRAPHY

1 GOEL, S. National cyber security strategy and the emergence of strong digital borders. *Connections*, JSTOR, v. 19, n. 1, p. 73–86, 2020.

2 BARARA, I. S. Capacity building for fighting cyber wars. *CYBERNOMICS*, v. 1, n. 1, p. 8–12, 2019.

3 MANSFIELD-DEVINE, S. *Verizon: Data Breach Investigations Report*. [S.l.]: MA Business London, 2022.

4 MOREIRA, V. R.; KURESKI, R.; VEIGA, C. Pereira da. Assessment of the economic structure of brazilian agribusiness. *The Scientific World Journal*, Hindawi, v. 2016, 2016.

5 SOUZA, D. N. de. Inteligência econômica de estado: necessidade estratégica para o brasil. *Revista Brasileira de Inteligência*, n. 13, p. 129–148, 2018.

6 CICB. *Qualidade da Carne Bovina*. <https://www.embrapa.br/qualidade-da-carne/carne-bovina>., 2022. CICB (Centro de Inteligencia da Carne Bovina); Accessed: February 8th, 2022.

7 MACHADO, G. C. et al. Agronegócio brasileiro: importância e complexidade do setor. 2021. *Acesso em*, v. 5, 2022.

8 OLIVEIRA, T. E. de; FREITAS, D. S. de; DIAS, E. A. Brazilian agricultural activities facing foreign direct investment. *Desenvolvimento Socioeconômico em Debate*, v. 1, n. 1, p. 81–93, 2015.

9 TOUNSI, W. What is cyber threat intelligence and how is it evolving? *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT*, Wiley Online Library, p. 1–49, 2019.

10 GOEDDE, L.; KATZ, J.; MÉNARD, A.; REVELLAT, J. Agriculture's connected future: How technology can yield new growth. *McKinsey and Company*, 2020.

11 BAGGETT, R. K.; SIMPKINS, B. K. *Homeland security and critical infrastructure protection*. [S.l.]: ABC-CLIO, 2018.

12 OSSEVORTH, F.; SEIDEL, P.; KRAHMER, S.; SEIFERT, J.; SCHEGNER, P.; LOCHMANN, P.; OEHM, L.; MAUERMANN, M. Resilience in supply systems–what the food industry can learn from energy sector. *Journal of Safety Science and Resilience*, Elsevier, v. 3, n. 1, p. 39–47, 2022.

13 USA. *HSPD 7; Homeland Security Presidential Directive 7*. Brasília, DF, 2003. Available at: <https://www.hsdl.org/?view&did=441950>. Accessed: February 2, 2022. Available: <https://www.hsdl.org/?view&did=441950>.

14 BRASIL. *Decreto nº 10.569, from December 9, 2020*. Brasília, DF. Available at: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.569-de-9-de-dezembro-de-2020-293251357>. Accessed: February 2, 2022. Available: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.569-de-9-de-dezembro-de-2020-293251357>.

15 BRASIL. *Decreto Nº 6.703, from December 18, 2008*. Brasília, DF. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Accessed: February 2, 2022. Available: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>.

16 OECD. *OECD-Reviews of Risk Mangement Policies Good Governance for Critical Infrastructure Resilience*. 2020. Available at: <https://www.oecd-ilibrary.org/sites/b1dac86e-en/index.html?itemId=/content/component/b1dac86e-en>. Accessed: March 22, 2022.

17 CANADA. *National Strategy for Critical Infrastructure*. 2009. Available at: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf>. Accessed: February 2, 2022. Available: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf>.

18 JAPAN. *The Cybersecurity Policy for Critical Infrastructure Protection*. 2017. Available at: <https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf>. Accessed: February 2, 2022. Available: <TheCybersecurityPolicyforCriticalInfrastructureProtection>.

19 CARNES), A. A. B. das Indústrias Exportadoras de. *Beef Report–Perfil da Pecuária no Brasil 2021*. 2020. Available at:<http://abiec.com.br/publicacoes/beef-report-2021/>. Accessed: February 8th, 2022.

20 ALBUQUERQUE, E. d. M.; TABOSA, F. J. S.; CASTELAR, P. U. d. C.; NETO, N. T.; KHAN, A. S.; ARAUJO, J. A. d.; LESSA, L. C. R.; SOUSA, E. C. Convergence clubs in the brazilian beef market. International Journal of Business Administration, 2022.

21 KUEPPER, B.; STEINWEG, T.; PIOTROWSKI, M.; ARNOULD, J. *Brazilian beef supply chain under pressure amid worsening ESG impacts*. [S.l.]: Washington DC. Retrieved from https://chainreactionresearch. com/wpcontent . . . , 2020.

22 RIBEIRO, V. P.; NETO, W. A. S. Brazilian beef exports to the main destinations: a persistence to shocks analysis. *Revista de Ciências Agrárias*, v. 43, n. spe1, p. 86–94, 2020.

23 OECD/FAO. *OECD-FAO Agricultural Outlook 2020–2029*. 2020. Available at: <https://www.oecd-ilibrary.org/agriculture-and-food/oecd-fao-agricultural-outlook-2020-2029_1112c23b-en>. Accessed: February 10th, 2022.

24 MALAFAIA, G. C.; MORES, G. de V.; CASAGRANDA, Y. G.; BARCELLOS, J. O. J.; COSTA, F. P. The brazilian beef cattle supply chain in the next decades. *Livestock Science*, Elsevier, v. 253, p. 104704, 2021.

25 MARTINS, M. M.; SPOLADOR, H. F.; NJUKI, E. Production environment and managerial techniques in explaining productivity growth in brazilian beef cattle production. *Agribusiness*, Wiley Online Library, v. 38, n. 2, p. 371–385, 2022.

26 CICB. *Cadeia produtiva da Carne Bovina*. <https://www.cicarne.com.br/2020/06/03/cadeia-produtiva-da-carne-bovina>, 2021. CICB (Centro de Inteligencia da Carne Bovina); Accessed: February 10th, 2022.

27 NETO, O. J. de O.; FIGUEIREDO, R. S.; WANDER, A. E. Price interdependence in the international and brazilian beef cattle market. *Revista Econômica do Nordeste*, v. 53, n. 2, p. 73–89, 2022.

28 ROJO-GIMENO, C.; VOORT, M. van der; NIEMI, J. K.; LAUWERS, L.; KRISTENSEN, A. R.; WAUTERS, E. *Assessment of the value of information of precision livestock farming: A conceptual framework*. [S.l.]: Elsevier, 2019. 100311 p.

29 MALAFAIA, G. C.; MORES, G. de V.; CASAGRANDA, Y. G.; BARCELLOS, J. O. J.; COSTA, F. P. The brazilian beef cattle supply chain in the next decades. *Livestock Science*, v. 253, p. 104704, 2021. ISSN 1871-1413. Available: <https://www.sciencedirect.com/science/article/pii/S1871141321003127>.

30 EVANS, C. V. Future warfare: weaponizing critical infrastructure. *The US Army War College Quarterly: Parameters*, v. 50, n. 2, p. 6, 2020.

31 JOSHI, M.; LEVY, O.; WELD, D. S.; ZETTLEMOYER, L. BERT for coreference resolution: Baselines and analysis. *arXiv preprint arXiv:1908.09091*, 2019. Available: <https://arxiv.org/abs/1908.09091>.

32 III, R. O. M. *Cyber Intelligence-driven Risk: How to Build and Use Cyber Intelligence for Business Risk Decisions*. [S.l.]: John Wiley & Sons, 2020.

33 HAMMOND-ERREY, M.; RAY, K. A new methodology for strategic assessment of transnational threats. *Police practice and research*, Taylor & Francis, v. 22, n. 1, p. 40–56, 2021.

34 CHISMON, D.; RUKS, M. Threat intelligence: Collecting, analysing, evaluating. *MWR InfoSecurity Ltd*, 2015.

35 RAMSDALE, A.; SHIAELES, S.; KOLOKOTRONIS, N. A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electronics*, Multidisciplinary Digital Publishing Institute, v. 9, n. 5, p. 824, 2020.

36 KOTSIAS, J.; AHMAD, A.; SCHEEPERS, R. Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, Taylor & Francis, v. 32, n. 1, p. 35–51, 2023.

37 HU, Z.; KHOKHLACHOVA, Y.; SYDORENKO, V.; OPIRSKYY, I. Method for optimization of information security systems behavior under conditions of influences. *International Journal of Intelligent Systems and Applications*, Modern Education and Computer Science Press, v. 9, n. 12, p. 46, 2017.

38 LÓPEZ, A. B. *ISO 27002 y ciberseguridad en la empresa: del control a la formación del usuario*. [S.l.]: Borrmart, 2022. 192–193 p.

39 CYBOK. *The Cyber Security Body of Knowledge - CyBOK*. <https://www.cybok.org/knowledgebase/>, 2021. Accessed: February 2, 2022.

40 AMARO, L. J. B.; AZEVEDO, B. W. P.; MENDONCA, F. L. Lopes de; GIOZZA, W. F.; ALBUQUERQUE, R. d. O.; VILLALBA, L. J. G. Methodological framework to collect, process, analyze and visualize cyber threat intelligence data. *Applied Sciences*, Multidisciplinary Digital Publishing Institute, v. 12, n. 3, p. 1205, 2022.

41 SHIN, B.; LOWRY, P. B. A review and theoretical explanation of the 'cyberthreat-intelligence (cti) capability'that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, Elsevier, v. 92, p. 101761, 2020.

42 EU. *Threat Landscape Report 2021*. ENISA, 2021. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>. Accessed: February 2, 2022. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.

43 AL-GHAMDI, M. I. Guide to developing a national cyber security strategy. *Materials Today: Proceedings*, Elsevier, 2021.

44 VOO, J.; HEMANI, I.; JONES, S.; DESOMBRE, W.; CASSIDY, D.; SCHWARZENBACH, A. National cyber power index 2020. *Belfer Center for Science and International Affairs, Harvard Kennedy School*, 2020.

45 BYGRAVE, L. A. Security by design: Aspirations and realities in a regulatory context. *Oslo Law Review*, n. 3, p. 126–177, 2022.

46 DRAGOS. *ICS/OT Cybersecurity year in review 2022*. <https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Report-2022.pdf?hsLang=en>, 2022. Accessed: April 4, 2023.

47 TZACHOR, A.; DEVARE, M.; KING, B.; AVIN, S.; HÉIGEARTAIGH, S. Ó. Responsible artificial intelligence in agriculture requires systemic understanding of risks and externalities. *Nature Machine Intelligence*, Nature Publishing Group UK London, v. 4, n. 2, p. 104–109, 2022.

48 PRIOR, M. et al. Cyber security: Global food supply chain at risk from malicious hackers. *Accesed on April 4, 2023*, BBC News. Retrieved from https://www.bbc.com/news/science-environment-61336659, May 20, 2022.

49 MANDIANT. *Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments*. <https://www.mandiant.com/resources/blog/apt41-us-state-governments>, 2022. Accessed: April 4, 2023.

50 GOVERNMENT, U. *FBI Most Wanted List*. [S.l.]: https://www.fbi.gov/wanted/cyber/apt-41-group, Feb 22, 2023.

51 GOVERNMENT, U. *REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR (g) OF THE SECURITIES EXCHANGE ACT OF 1934*. [S.l.]: https://www.sec.gov/Archives/edgar/data/1857475/000185747523000013/dole-20221231.htm, Feb 22, 2023.

52 COMPANY, D. *Dole Experiences Cybersecurity Incident*. [S.l.]: https://www.doleplc.com/news/company-news/company-news-details/2023/-Dole-Experiences-Cybersecurity-Incident/default.aspx, Feb 22, 2023.

53 AGCO. *AGCO Provides Update on Recovery from Ransomware Cyber Attack*. [S.l.]: https://news.agcocorp.com/news/agco-provides-update-on-recovery-from-ransomware-cyber-attack, May 16, 2022.

54 REVIEW, N. L. *U.S. Agricultural Machinery Manufacturer Hit with Ransomware Attack*. [S.l.]: https://www.natlawreview.com/article/us-agricultural-machinery-manufacturer-hit-ransomware-attack, May 12, 2022.

55 INVESTIGATION, F. B. of. *Ransomware Attacks on Agricultural Cooperatives, Potentially Timed to Critical Seasons*. [S.l.]: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ic3.gov/Media/News/2022/220420-2.pdf, April 20, 2022.

56 ALI, R. F.; DOMINIC, P.; ALI, S. E. A.; REHMAN, M.; SOHAIL, A. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, MDPI, v. 11, n. 8, p. 3383, 2021.

57 TRINKS, V. d. M. D.; ALBUQUERQUE, R. d. O.; NUNES, R. R.; MOTA, G. A. Strategic assessment of cyber security contenders to the brazilian agribusiness in the beef sector. *Information*, MDPI, v. 13, n. 9, p. 431, 2022.

58 ITC. *Trademap*. <https://www.trademap.org/>, 2022. Accessed: December 10th, 2021.

59 FIELDS, K. H.; THERRIEN, D. A.; HALSTROM, D.; HAGGARD, J.; CLAYTON, P. International bbef trade: A value proposition. *Animal Frontiers*, Oxford University Press US, v. 8, n. 3, p. 16–22, 2018.

60 GAMERO-GARRIDO, A. Cyber conflicts in international relations: Framework and case studies. *Available at SSRN 2427993*, 2014.

61 CARDON, E. Fighting alone is called losing. *The Cyber Defense Review*, JSTOR, v. 7, n. 1, p. 75–82, 2022.

62 EUA. *Use of Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification*. DHS, 2021. Available at: <https://www.dhs.gov/sites/default/files/

publications/privacy-pia-cisa38-adminsubpoenasforcybersecurityvulnerabilityid-may2021.pdf>. Accessed: August 5, 2022. Available: <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cisa38-adminsubpoenasforcybersecurityvulnerabilityid-may2021.pdf>.

63 Forbes Staff. *https://www.forbes.com/sites/carlieporterfield/2021/06/03/department-of-justice-creates-new-task-force-to-take-on-ransomware-attacks/?sh=218288524b80*. 2021. Access date: 2 feb. 2022. Available: <https://www.forbes.com/sites/carlieporterfield/2021/06/03/department-of-justice-creates-new-task-force-to-take-on-ransomware-attacks/?sh=218288524b80>.

64 OEA. *Revisão Da Capacidade de Cibersegurança*. <https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf>, 2020. OEA (Organização dos Estados Americanos); Accessed: February 10th, 2022.

65 DINIZ, G.; MUGGAH, R.; GLENNY, M. Deconstructing cybersecurity in brazil: Threats and responses. *Are we ready*, 2015.

66 RAVICH, S. F.; FIXLER, A. Framework and terminology for understanding cyber-enabled economic warfare. *Foundation for Defense of Democracies, Center on Sanctions and Illicit Finance Resource Document*, 2017.

67 SILVA, J. C. B. L. da. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios. *NAVAL WAR COLLEGE JOURNAL*, v. 20, n. 1, p. 193–211, 2016.

68 AHLEMANN, F.; GASTL, H. Process model for an empiracally grounded reference model construction. In: *Reference modeling for business systems analysis*. [S.l.]: IGI Global, 2007. p. 77–97.

69 RAJÃO, R.; NOBRE, A. D.; CUNHA, E. L.; DUARTE, T. R.; MARCOLINO, C.; SOARES-FILHO, B.; SPAROVEK, G.; RODRIGUES, R. R.; VALERA, C.; BUSTAMANTE, M. et al. The risk of fake controversies for brazilian environmental policies. *Biological Conservation*, Elsevier, v. 266, p. 109447, 2022.

APPENDIX