Brazilian Agribusiness in the Beef Sector

Subjects: Agricultural Economics & Policy

Contributor: Virgínia de Melo Dantas Trinks, Robson de Oliveira Albuquerque, Rafael Rabelo Nunes, Gibran Ayupe Mota

The current international commercial structure places Brazilian Agribusiness in 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.

Keywords: agribusiness ; cyber security ; cyber threat intelligence

1. Introduction

Agribusiness is essential in today's global economy for the 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. This market holds the interests of players that range from powerful governments through large corporations and small building societies [1].

The cattle beef agribusiness chain reached a value of almost USD 40 billion, which account for 15.98% of the Brazilian agribusiness 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 compared with 2019. This demonstrates the primary function of the sector for the Brazilian economy [2].

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 an 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 [2].

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. The value of the meat trade is dominated by beef and veal, but, in terms of quantity, the meat trade is increasingly dominated by poultry [3]. All these points express the importance of the beef supply chain and export revenue to Brazilian economy, food supply, and society.

2. Contemporary Food Supply 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 [4].

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 cause civil unrest and societal tumult.

After the 9/11 attacks, the USA updated its definition of Critical Infrastructure (CI) 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" [5]. According to Ossevorth et al. [6]:

> *"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) [7] 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 [8], and no. 6.703, 2008 [9], 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, which means that physical and operational security needs to be known and monitored in order to ensure the provision of those essential services.

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

In Europe, the OECD classifies six sectors as CI: information and communication technologies, energy, finance, health, transport and water [10]. Food supply appears in a second group of sectors that includes government, chemical industry, or public safety, for about half of the countries. An OECD white paper 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.

In Canada, the National Strategy for Critical Infrastructure [11] 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 a coherent and complementary approach to the 10 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 [12] 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, Japan's regulation affirms that there are also fears of possible future attacks in a global supply chain. In this context, even though food is not nominated as a CI by Japanese authorities, the 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 [10].

2.1. Impact of Technology in Agribusiness and Strategic Supply Chains

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 [4]. 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 [4].

Technological developments bring an infinite horizon of possibilities and uses for beef production, for example, the 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 [4].

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 improves deployment agility, but it also lacks security focus, as evidenced by various Open RAN alliances [4].

Proper security planning and investments 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 cybernetic attacks show that modern production of key products is heavily automated, not only for safety reasons.

2.2. Brazilian Beef Production Chain

The beef production chain starts in the input sector. Then, 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 [13]. Aspects related to foreign trade, macroeconomic evolution, inspection, legislation, product availability, reliability of statistical information, environmental legislation, traceability 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. As a result, the amount of not inspected beef produced dropped from 50% percent to less than 22% [2].

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) [14], 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 [2].

The 2021 edition of the OECD-FAO Agricultural Outlook [3] 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. This explains 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 [15] 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 the Brazilian food sector is central to the world economy and, as such, it is the point of interest of a wide range of actors. It is an international reality that weaponizing CI has become a means to undermine countries capabilities in a contemporary Hybrid Warfare format [16].

3. Threat Intelligence

According to Chismon and Ruks [17], it is relevant to have a clear differentiation between vulnerability information and threat intelligence to produce relevant intelligence. A vulnerability might exist in a product used by the organisation that does not necessarily have 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, and 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 [18]:

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

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 [17]:

> *"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."*

Cyber Threat Intelligence

Even though there is a general awareness of the need for 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 [19]. In this matter, ISO introduced an updated version of the ISO 27001 in 2022, named ISO 27002. 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 [20].

According to Tounsi's work [21], the 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 with the one of TI in the sense that they constitute 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.

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 [22], and thus 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 [21].

With respect to updated cyber security necessities, Agribusiness reality and current CTI production cycles as presented by Borges et al. [23] presented a strategic approach to understand how CTI may assist interested parties to develop long-term cyber security strategies. Thus, intersecting CTI with economic and political components may lead to thorough and updated assessment for the unveiling of potential cyber threats.

Tounsi [21] and Evans [16] provided key definitions on CTI, and how they are currently being used in the kinetic world, through International Relations and warfare. In addition, researchers 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 [24] highlighted 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, 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"*.

4. 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 [25]. The report also recognized that supply chain compromises by state-backed threat actors are not new, and that this type of attack has 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, which sheds doubt on the definitions of cyberespionage and cybercrime operations.

The main spotted trends in the sector showcase that countries with advanced cyber capabilities are using these 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 is not only here to stay, but will be increasingly used for intelligence gathering and critical infrastructure attacks. Thus, 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 [25].

The Guide to Developing a National Cybersecurity Strategy by the International Telecommunication Union (ITU) [26] 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 cybercrime and other cyber-enabled crimes. The ITU guide recognized that:

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

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

In an attempt to understand actors in the sector, a group of researchers at Harvard University came up with the Harvard National Cyber Power Index (NCPI) index [27] that considers that the analysis of cyber power is the product of intent and capability. As a result the top 10 "most comprehensive countries" with the highest level of Intent Ranking by Commercial Objective are as follows [27]:

- China
- Iran
- United Kingdom
- Japan
- Switzerland
- The Netherlands
- Sweden
- Australia
- USA
- Russia

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

The index recognizes countries not normally associated with cyber powers, due to their strong capabilities in certain areas. For example, Sweden is ranked in the top 10 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: it has been found to use industrial espionage, to incentivize 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 cybercrime threat actors increasingly show the same patterns of behaviour [25].

5. Recent Cases of Vulnerabilities Exploitation

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 [1]. In this environment, cyber attacks have become more common. Below researchers present recent cases of cyber attacks against the agribusiness sector, and relevant supply chain providers in chronological order.

5.1. JBS Attack

On 30 May 2021, newspapers all over the world reported on the case of the Brazilian-based meat company called JBS that 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, and damaged the company's image, and a discussion commenced over possible meat shortages and price rises. Only by the beginning of June was the company able to fully recover and put its global IT Systems back in order.

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. 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 4 June 2021, Russia-linked cyber group REvil announced it 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 10 June, 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 16 June 2021, the American and Russian Presidents held a summit in Geneva, where Cyber security was a significant topic of conversation. The American President clearly stated Cyber security was 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.

5.2. 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.

5.3. USAHERDS

In March 2022, 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. The 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.

References

1. CICB (Centro de Inteligencia da Carne Bovina). Qualidade da Carne Bovina. Evaluation, Embrapa. 2022. Available online: https://www.embrapa.br/qualidade-da-carne/carne-bovina (accessed on 8 February 2022).
2. Beef Report–Perfil da Pecuária no Brasil 2021. Available online: http://abiec.com.br/publicacoes/beef-report-2021/ (accessed on 8 February 2022).
3. OECD/FAO. OECD-FAO Agricultural Outlook 2020–2029. Available online: https://www.oecd-ilibrary.org/agriculture-and-food/oecd-fao-agricultural-outlook-2020-2029_1112c23b-en (accessed on 10 February 2022).
4. Goedde, L.; Katz, J.; Ménard, A.; Revellat, J. Agriculture's Connected Future: How Technology Can Yield New Growth; McKinsey & Company: Hong Kong, 2020; Available online: https://www.mckinsey.com/~/media/McKinsey/Industries/Agriculture/Our%20Insights/Agricultures%20connected%20future%20How%20tec connected-future-How-technology-can-yield-new-growth-F.pdf (accessed on 24 July 2022).
5. Baggett, R.K.; Simpkins, B.K. Homeland Security and Critical Infrastructure Protection; ABC-CLIO, LLC: Santa Barbara, CA, USA; Denver, CO, USA, 2018.
6. 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. J. Saf. Sci. Resil. 2022, 3, 39–47.
7. USA. HSPD 7; Homeland Security Presidential Directive 7. Available online: https://www.hsdl.org/?view&did=441950 (accessed on 2 February 2022).
8. Brasil. Decreto nº 10.569, from 9 December 2020. Available online: https://www.in.gov.br/en/web/dou/-/decreto-n-10.569-de-9-de-dezembro-de-2020-293251357 (accessed on 2 February 2022).
9. Brasil. Decreto Nº 6.703, from 18 December 2008. Available online: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm (accessed on 2 February 2022).
10. OECD. OECD-Reviews of Risk Mangement Policies Good Governance for Critical Infrastructure Resilience. Available online: https://www.oecd-ilibrary.org/sites/b1dac86e-en/index.html?itemId=/content/component/b1dac86e-en (accessed on 22 March 2022).

11. Canada. National Strategy for Critical Infrastructure. 2009. Available online: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf (accessed on 2 February 2022).
12. Japan. The Cybersecurity Policy for Critical Infrastructure Protection. Available online: https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf (accessed on 25 February 2022).
13. CICB (Centro de Inteligencia da Carne Bovina). Cadeia Produtiva da Carne Bovina. Evaluation, Embrapa. 2021. Available online: https://www.cicarne.com.br/2020/06/03/cadeia-produtiva-da-carne-bovina (accessed on 10 March 2022).
14. Rojo-Gimeno, C.; van der Voort, M.; Niemi, J.K.; Lauwers, L.; Kristensen, A.R.; Wauters, E. Assessment of the value of information of precision livestock farming: A conceptual framework. Njas-Wagening. J. Life Sci. 2019, 90, 100311. Available online: https://www.sciencedirect.com/science/article/pii/S1573521418302215 (accessed on 20 July 2022).
15. Malafaia, G.C.; de Vargas Mores, G.; Casagranda, Y.G.; Barcellos, J.O.J.; Costa, F.P. The Brazilian beef cattle supply chain in the next decades. Livest. Sci. 2021, 253, 104704.
16. Evans, C.V. Future warfare: Weaponizing critical infrastructure. US Army War Coll. Q. Parameters 2020, 50, 6.
17. Chismon, D.; Ruks, M. Threat Intelligence: Collecting, Analysing, Evaluating; MWR InfoSecurity Ltd.: Basingstoke, UK, 2015.
18. Ramsdale, A.; Shiaeles, S.; Kolokotronis, N. A comparative analysis of cyber-threat intelligence sources, formats and languages. Electronics 2020, 9, 824.
19. Hu, Z.; Khokhlachova, Y.; Sydorenko, V.; Opirskyy, I. Method for optimization of information security systems behavior under conditions of influences. Int. J. Intell. Syst. Appl. 2017, 9, 46.
20. López, A.B. ISO 27002 y Ciberseguridad en la Empresa: Del Control a la Formación del Usuario. 2022. Available online: https://www.seguritecnia.es/tecnologias-y-servicios/ciberseguridad/iso-27002-y-ciberseguridad-en-la-empresa_20220329.html (accessed on 20 June 2022).
21. Tounsi, W. What is Cyber Threat Intelligence and How Is It Evolving? In Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT; Wiley Online Library; 2019; pp. 1–49. Available online: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119618393.ch1 (accessed on 1 July 2022).
22. Cybok. The Cyber Security Body of Knowledge—CyBOK. Evaluation, University of Bristol, Formal Methods for Security. 2021. Available online: https://www.cybok.org/knowledgebase/ (accessed on 10 March 2022).
23. Borges Amaro, L.J.; Percilio Azevedo, B.W.; Lopes de Mendonca, F.L.; Giozza, W.F.; Albuquerque, R.d.O.; García Villalba, L.J. Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data. Appl. Sci. 2022, 12, 1205. Available online: https://www.mdpi.com/2076-3417/12/3/1205 (accessed on 25 February 2022).
24. 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. Comput. Secur. 2020, 92, 101761.
25. EU. Threat Landscape Report 2021. 2021. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (accessed on 2 February 2022).
26. Al-Ghamdi, M.I. Guide to developing a National Cyber Security Strategy. Mater. Today Proc. 2021.
27. Voo, J.; Hemani, I.; Jones, S.; DeSombre, W.; Cassidy, D.; Schwarzenbach, A. National Cyber Power Index 2020; Belfer Center for Science and International Affairs: Cambridge, MA, USA, 2020.