An Exploratory Study of Cognitive Sciences Applied to Cybersecurity

Roberto O. Andrade 1, Walter Fuertes 2, María Cazares 3, Iván Ortiz-Garcés 4,* and Gustavo Navas 3

1 Facultad de Ingeniería en Sistemas, Escuela Politécnica Nacional, Quito 170525, Ecuador; roberto.andrade@epn.edu.ec
2 Department of Computer Sciences, Universidad de las Fuerzas Armadas ESPE, Sangolquí P.O. Box 17-15-231B, Ecuador; wmfuertes@espe.edu.ec
3 IDEAGEOCA, Universidad Politécnica Salesiana, Cuenca 010102, Ecuador; mcazares@ups.edu.ec (M.C.); gnava@ups.edu.ec (G.N.)
4 Facultad de Ingeniería y Ciencias Aplicadas, Escuela de Ingeniería en Tecnologías de la Información, Universidad de las Américas, Quito 170125, Ecuador
* Correspondence: ivan.ortiz@udla.edu.ec

Abstract: Cognitive security is the interception between cognitive science and artificial intelligence techniques used to protect institutions against cyberattacks. However, this field has not been addressed deeply in research. This study aims to define a Cognitive Cybersecurity Model by exploring fundamental concepts for applying cognitive sciences in cybersecurity. For achieving this, we developed exploratory research based on two steps: (1) a text mining process to identify main interest areas of research in the cybersecurity field and (2) a valuable review of the papers chosen in a systematic literature review that was carried out using PRISMA methodology. The model we propose tries to fill the gap in automatizing cognitive science without taking into account the users’ learning processes. Its definition is supported by the main findings of the literature review, as it leads to more in-depth future studies in this area.

Keywords: cognitive security; cybersecurity; cyberattacks

1. Introduction

Cybersecurity attacks have been relevant since the appearance of the first computers. However, their evolution due to the level of techniques and tools has converted them into the world’s main risk. The World Economic Forum [1] has classified cyberattack as one of the top ten worldwide risks. Its impact is considered more significant than a food crisis due to its scope in modern society and its probability of occurrence. Reactive solutions focus mainly on attack alleviation processes, while proactive solutions could predict possible cyberattacks and generate self-protection systems. This scenario has motivated companies and researchers in the cybersecurity field to look for alternatives for replacing reactive solutions with proactive ones. One approach used by specialized firms and researchers is to establish anomaly detection processes that discover possible attack patterns and identify attackers’ behaviors. In the last three years (2019–2021), several contributions to anomaly detection have been developed in different domains such as SCADA systems, smart grids, smart cities, critical infrastructures, and Cyber-Physical Systems (CPS) [2].

The anomaly detection process requires identifying features or components that differ from typical behaviors [3]. In the initial phase of this anomaly detection process, modeling cybersecurity expert knowledge and cognitive processes are relevant for building better proactive solutions. However, the large volume of data generated by the different interconnected devices in the digital world makes the identification process more challenging to implement [4]. Several alternatives have been defined for supporting analysts’ cognitive processes (i.e., augmented cognition) by using computational models that simulate the
cognitive processes performed by cybersecurity experts. The identification of security risk patterns based on the analysts’ cognitive processes can be approached through the Observe–Orient–Decide–Act model (OODA) or the Monitor–Analyze–Plan–Execute model (MAPE-K) [5].

Researchers have proposed the automation and support of the cognitive processes defined in the OODA and MAPE-K models through different machine learning techniques [6]. In the same research line, we found that several works from 2019 to 2021 used convolution networks, K-means, or deep learning for detecting phishing, ransomware, and even attacks against smart grids [7].

Researchers have identified that the possible actions or strategies of adversaries can be studied using game theory models with incomplete information based on Stackelberg’s proposals [8]. This approach could support identifying a possible future attack and the possible strategies used by the adversary. In this way, cybersecurity research’s central objective is to expand security analysts’ cognitive capacity through data analysis, machine learning techniques, and game theory in cybersecurity [9].

Researchers have proposed a more in-depth approach to improve the cybersecurity proposals, focused on the adversary to identify their behavioral characteristics that lead them to decide on a specific attack strategy [10]. Furthermore, this allows for identifying the techniques that the adversary could select and how to use them. This approach could enable cybersecurity analysts to anticipate and establish a more optimal defense mechanism. Research has included the psychological perspective to analyze the adversaries’ behavior [11]. Incorporating Artificial Intelligence, Machine Learning, data analytics, and psychology, among other fields related to cognitive sciences in cybersecurity, has generated a new cybersecurity approach called cognitive security [12]. This approach goes one step ahead of security intelligence to propose the best defensive strategies and take advantage of both cognitive processes: cybersecurity analysts and adversaries [13].

This study aims to identify the fundamental concepts related to the application of cognitive sciences in cybersecurity for establishing defense strategies to minimize the impact of cyberattacks. For this reason, we developed an exploratory study based on two stages:

- A text mining process to identify challenges in the field of cybersecurity and analyze the impact of cyberattacks and the future direction of cybersecurity solutions based on cognitive science;
- A Systematic Literature Review (SLR) to identify the contributions of applied cognitive sciences in cybersecurity as alternatives for proactive strategies. The main contribution of this study is the definition of a cognitive cybersecurity model supported by the findings of a literature review in this research area based on the PRISMA methodology.

This study is structured as follows. Section 2 introduces and describes the theory that explains the components of the research problem under research. Section 3 provides the methodological procedure applied to judge the validity of the results of this study. Section 4 presents a proposal for a cognitive cybersecurity model. Finally, the Section 6 describes the main findings and the lines of future work.

2. Background

2.1. Adversarial and User Analysis

In cyberattack scenarios, a competitive advantage by the adversary could exist in the first instance. Table 1 shows the adversary has valuable information such as personal user information, type of operating system, and user applications. Additionally, the adversary has information about the types of security vulnerabilities that can be exploited. The adversary has been trained in several cybersecurity areas, such as ethical hacking, vulnerability analysis, and reverse engineering. In this context, a user has a clear disadvantage, and from the perspective of game theory, we are faced with a game scenario with incomplete information from the user’s side. The user does not know information related to the adversary, such as the type of cyberattack it could perform, which techniques will be used.
to execute the attack, and which kind of resources are available. Establishing an optimal defense/security attack strategy requires more information from a user perspective [14].

Table 1. Comparative of resources adversarial versus user.

<table>
<thead>
<tr>
<th>Role</th>
<th>Techniques</th>
<th>IT Resources</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Empirical Knowledge</td>
<td>Office or Home Desktop</td>
<td>No or low information related to adversaries. Adversaries could use VPN or deep network to hide their information and maintain anonymity.</td>
</tr>
<tr>
<td>Organization</td>
<td>Tactics, Techniques, and Procedures (TTP) Offensive/Defensive approaches</td>
<td>Perimetral security (Firewall, IPS, IDS) Security Event Management (SIEM)</td>
<td></td>
</tr>
<tr>
<td>Adversaries</td>
<td>Offensive approaches (hacking, vulnerability scans, deep network) MITRE ATT&amp;CK defines 245 techniques of attacks, distributed in 14 categories.</td>
<td>Vulnerability tools Exploit tools Obfuscation tools Lateral Movement Frameworks Remote access trojans</td>
<td>Data from Social networks (Facebook, Instagram, twitter) Data from personal or enterprise blogs or web pages. Data for deep network.</td>
</tr>
</tbody>
</table>

Alternatively, another drawback for the user is the stimulus that affects his/her decision criteria. For example, the COVID-19 pandemic has created a scenario where adversaries interact with web pages with drug procurement for the virus or access to free entertainment platforms [15]. In this context, the response time window in which the user must decide between clicking or abstaining from clicking is critical. For gathering information related to the adversary, pattern recognition techniques are used [7]. Meanwhile, decision-making models based on Bayesian networks [16] and diffusion models [17] are used for modeling user response time. Simmons et al. [18] propose the characterization of cyberattacks based on five major classifiers: attack vector, operational impact, attack target, defense, and informational impact. The adversary’s characterization is based on two aspects: Risk adverseness and Experience level. Venkatesan et al. [19] propose that the modeling of the adversary behavior considers at least the following aspects:

- Cultural characteristics;
- Behavior patterns;
- Types of attacks.

At this point, incorporating cognitive sciences can improve the development of proactive cybersecurity solutions.

2.2. Cognitive Sciences

Research on cognitive sciences applied to cybersecurity acknowledges the importance of the human factor in cybersecurity; this is particularly relevant with the challenges generated by the growth of technologies such as cloud, mobile, IoT, and social networks [20,21]. Cognitive science could enhance the processes of perception, comprehension, and projection used by cybersecurity analysts to detect cyberattacks and establish future defense actions [9].

2.3. Cognitive Process

Currently, information is increasing fast, and the availability of processing data surpasses human capacities. According to [22], cognitive architectures and models have primarily been developed using Artificial Intelligence to serve as decision aids to human users. Analyzing the rational cognitive process can allow the design of the computational level of cognitive prediction. Cassenti et al. [23] mention that by using technology based on adaptive aids, the user’s cognitive state can be obtained and difficulties detected at any stage of cognition. Additionally, Cassenti mentions that one missing element in technology models concerns the human learning process, providing feedback that allows technology to adapt to the user and accomplish goals. According to Cameron [24], cognitive strategies are mental processes developed by humans to regulate the thought processes inside the mind to achieve goals or solve problems (See, Figure 1).
2.4. Cognitive Security

Cognitive security is the ability to generate cognition for efficient decision-making in real-time by modeling human thought processes to detect cybersecurity attacks and develop defense strategies. Specifically, it responds to the need to build situational awareness of cybersecurity related to the environment of technology systems and the insights about itself. In addition, cognitive security allows programmers to develop defense actions by analyzing structured or unstructured information using cognitive sciences approaches, for instance, by incorporating Artificial Intelligence techniques such as data mining, machine learning, natural language processing, human-computer interaction, data analytics, big data, stochastic processes, and game theory. These emulate the human thought process for generating continuous learning, decision making, and security analysis [5].

2.5. Prisma Methodology

The PRISMA methodology is divided into four stages: identification, screening, eligibility analysis, and inclusion [25]. The identification stage includes the development of the following phases: study selection, inclusion and exclusion criteria, manual search, and duplicate removal. The screening stage consists of choosing papers according to relevant titles and abstracts. Next, the eligibility analysis stage includes the process of reading the full texts that accomplished the screening criteria. Finally, the inclusion stage consists of the relevant data extraction from full papers [26].

2.6. Text Mining

In this work, we applied text mining to execute the data analysis of selected papers. Text mining can be defined as mathematical analysis to deduce patterns and trends in the data. A classic exploration can detect these patterns because the relationships are very complex or large amounts of text where repetitive patterns, trends, or rules that explain the text’s behavior are discovered. Text Mining’s objective, an essential part of Data Science, is to help understand the content of a set of texts through statistics and search algorithms related to Artificial Intelligence [27]. In the text mining process, we obtain information from large amounts of text, with unstructured information and the context in which it was written, intending to extract non-obvious information. Text mining could conduct a qualitative research project with a large sample size similar to a quantitative research study [28].

3. Methods

Cognitive sciences applied to cybersecurity; an exploration based on PRISMA.

The methodology used in this study was the development of a systematic literature review based on the PRISMA methodology, which includes four stages: identification, screening, eligibility analysis, and inclusion (see Figure 2). Study selection was based on
a systematic review following the Prisma Guidelines [21]. In the identification stage, we found works in the following databases: Springer, Scopus, IEEE, Association for Computing Machinery (ACM), Web of Science, and Science Direct, in the last three years, 2019 to 2020, to identify the trends in cybersecurity. The search queries established were the following:

- “Cybersecurity” AND “Attacks” AND “Trends”;
- “Cybersecurity” AND “Trends” AND “Challenges”.

Figure 2. SLR according to Prisma methodology.

The inclusion criteria were: (i) documents published on the scientific database from 2019 to 2021. The exclusion criteria included: (i) documents not related to cybersecurity and (ii) documents out of the research period (2019–2021). Figure 3 shows the screening and eligibility process of the 1244 studies. Then, based on the review of papers’ titles and abstracts using a web application, Rayyan, created for the systematic review process, we removed the papers that did not comply with the inclusion criteria. At the end of the screening process, 813 articles were selected for full-text reading. Finally, we removed studies without clear proposals in the cybersecurity field, excluding 748 papers.

Figure 3. General topics in cybersecurity between 2019 to 2021.

**Qualitative analysis using text mining technique.**

Text mining, which is considered another field in cognitive science, is essential for qualitative cybersecurity research. However, text mining requires text cleaning and tok-
enization as prerequisites. In this way, the cleaning process of text, within the scope of text mining, consists of eliminating everything that does not provide information on its subject, structure, or content from the corpus. It should be noted that there is no single way to do this step. It depends on the purpose of the analysis and the text source. We applied a text mining analysis using R software to all 748 studies obtained in the included stage of PRISMA methodology. Thus, we eliminated non-informative patterns (web page URLs), punctuation marks, and single characters. We generated the text tokenization, which divides the text into the units for the analysis in question. We proceeded to store the tokenized text. Each element of the tokenized_text column is a list with a character vector containing the generated tokens. However, there has been a significant change when doing the tokenization process. Before the text’s division, the study elements (observations) were the titles and keywords of selected papers. Each one was in a row, thus fulfilling the condition of tidy data: one observation per row. When performing the tokenization, the study element has become each token (word), thus violating the condition of tidy data. Thus, each token list must be expanded to recover the ideal structure, doubling the other columns’ value as many times as necessary [29]. We carried out the analysis for the years 2020–2021, obtaining the results in Table 2 and Figure 3.

Table 2. General topics in cybersecurity between 2019 to 2021.

<table>
<thead>
<tr>
<th>5G</th>
<th>Cloud Security</th>
<th>Microgrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC microgrids</td>
<td>Data integrity attack (DIA.)</td>
<td>Multistate model</td>
</tr>
<tr>
<td>Advanced metering</td>
<td>Deep learning</td>
<td>Offensive Security</td>
</tr>
<tr>
<td>Artificial intelligence (AI)</td>
<td>Distributed resilient control</td>
<td>Open software</td>
</tr>
<tr>
<td>Battery pack</td>
<td>DevOps Security</td>
<td>Plug-in electric vehicles</td>
</tr>
<tr>
<td>Blockchain</td>
<td>Digital transformation</td>
<td>Robust algorithm</td>
</tr>
<tr>
<td>Call detail record (CDR)</td>
<td>Event-triggered mechanism</td>
<td>Smart contract</td>
</tr>
<tr>
<td>Cybersecurity awareness</td>
<td>Energy security</td>
<td>Smart sensor</td>
</tr>
<tr>
<td>Cyberattacks</td>
<td>False data injection attacks</td>
<td>Smart meters</td>
</tr>
<tr>
<td>Cyberattack detection</td>
<td>Human Security</td>
<td>Smart City</td>
</tr>
<tr>
<td>Cyber-physical systems (CPS.)</td>
<td>Internet of Things (IoT)</td>
<td>Software-defined architecture</td>
</tr>
<tr>
<td>Cyber power network</td>
<td>Machine learning</td>
<td>Supply chain management</td>
</tr>
</tbody>
</table>

We included the studies of all the works that evidenced the development of strategies and structures in cybersecurity. Furthermore, we considered articles referring to models developed for learning defense against a cyberattack.

Then, we developed a word cloud process to obtain more detail on scientific studies’ contributions in the cybersecurity domain. Algorithm 1 shows the R script used to determine the cybersecurity topics, and Figure 4 shows the word cloud results.

Algorithm 1: Pseudo-code of R script to word cloud process

```r
wordcloud <- function(group, df)
  print(group)
  wordcloud(words = df$token, freq = df$frequency,
            max.words = 400, random.order = FALSE,
            rot.per = 0.35, color = brewer.pal(8,"Dark2"))
```
Figure 4. Results of a word cloud of 748 papers.

**Cybersecurity attacks and their impact**

According to the World Economic Forum [1], cyberattacks were considered a fifth of the worldwide risks above food crisis in 2020. Adversaries developed several cyberattack scenarios. For instance, the United States Department of Justice discloses public information about scams perpetrated through websites, social networks, emails, and robocalls, among other means. All these related to fake news about COVID-19 vaccines, treatments, protective equipment, and obviously, about criminals who conducted fake businesses to steal identities or file fraud cite the USDJ. Another cybersecurity scenario covered by the United States Department of Justice is when adversaries send text messages using fictitious phone numbers and social media accounts to harass, intimidate, cyberstalk, and attempt to sextort women [30]. On the other hand, CISA mentions that adversaries use Bots to conduct credential harvesting, mail exfiltration, crypto mining, point-of-sale data exfiltration, and the deployment of ransomware [31]. According to the FBI, from 2015 to 2019, reports about fraud in the FBI’s Internet Crime Complaint Center (IC3) went from USD 1.1 billion to USD 3.5 billion [32]. Establishing the most appropriate cybersecurity defense solution is necessary to identify the characteristics of cyberattacks [33]. There are currently a great variety of cyberattacks [34]; Table 3 shows those that are the most recurrent among the selected papers for this study.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>Is a malicious and deliberate attempt of sending fake messages that appear to come from a reputable source</td>
<td>[35–40]</td>
</tr>
<tr>
<td>Insider threats</td>
<td>Are encountered in international security, geopolitics, business, trade, and cybersecurity. Insider threats could be considered more damaging than outsider attacks</td>
<td>[41–43]</td>
</tr>
<tr>
<td>APT</td>
<td>Are designed to steal corporate or national secrets.</td>
<td>[44–46]</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>Criminal activity either targets or uses a computer, a computer network, or a networked device.</td>
<td>[47,48]</td>
</tr>
<tr>
<td>Malware</td>
<td>Malicious software designed to infiltrate a device without knowledge</td>
<td>[49,50]</td>
</tr>
<tr>
<td>DDoS</td>
<td>Denial of service attack on a computer system or network that causes a service or resource to be inaccessible to legitimate users</td>
<td>[51–55]</td>
</tr>
<tr>
<td>Ransomware</td>
<td>A type of malicious program that restricts access to certain parts of files of the infected operating system and demands a ransom in exchange for removing this restriction</td>
<td>[56–60]</td>
</tr>
<tr>
<td>Mobile malware</td>
<td>Its name suggests malicious software that targets explicitly the operating systems on mobile phones</td>
<td>[61–64]</td>
</tr>
<tr>
<td>Watering hole</td>
<td>Refers to a tactic used during targeted attack campaigns where the APT is distributed through a trusted website that is usually visited by employees of the target company or entity</td>
<td>[65,66]</td>
</tr>
</tbody>
</table>
We contrasted this result with an international organization related to cybersecurity. We found that some of them were considered the most relevant cyberattacks in the year 2020, according to The European Union Agency for Cybersecurity (ENISA) [34]. Additionally, we compared this result with the report of a specialized cybersecurity firm. We found that four out of nine attacks documented in our study had a growth rate of between 7 and 25 percent in 2020 in America, Europe, and Asia (see Table 4). According to [67], a classification of cyberattacks is based on the effects they cause against a system or its architecture: misuse of resources; user access compromise; root access compromise; web access; malware; and denial of service.

Table 4. Growth rate percentage of cyberattack 2020.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Americas</th>
<th>Europa</th>
<th>Asia</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS</td>
<td>13%</td>
<td>17%</td>
<td>23%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>3%</td>
<td>4%</td>
<td>6%</td>
</tr>
<tr>
<td>Mobile malware</td>
<td>15%</td>
<td>15%</td>
<td>25%</td>
</tr>
<tr>
<td>Phishing</td>
<td>7%</td>
<td>11%</td>
<td>14%</td>
</tr>
</tbody>
</table>

Other cyberattacks use machines as attack vectors [68], while others focus on human behaviors [69]. In the case of phishing, attackers seek to exploit human vulnerabilities resulting from factors such as solidarity, desperation, or authority control to carry out their attack [70]. In contrast, Ransomware attacks exploit vulnerabilities in operating systems or applications to encrypt users’ or organizations’ sensitive information [71]. Within this context, Watering hole attackers use exploit kits with stealth features and seek to compromise a specific group of end-users by infecting websites [65]. A malicious URL attacker defines a link created to distribute malware or facilitate a scam [72]. Form hacking is a type of cyberattack where hackers inject malicious JavaScript code into legitimate website payment forms [73]. Table 5 shows a classification of attacks based on an adversary’s resource (machine or human).

Table 5. Attacks adversary’s targets (machine or human).

<table>
<thead>
<tr>
<th>Type</th>
<th>Human</th>
<th>Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Insider threats</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Web Based Attacks</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Advanced persistent threat (APT)</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Spam</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Identity theft</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data breach</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Botnets</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Physical manipulation</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Malware</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DDoS</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ransomware</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mobile malware</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Watering hole</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Information leakage</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

X represents the affection of target due to attack.

Another way to classify cyberattacks could be based on the target, such as energy, healthcare, and transportation [74,75]. Table 6 shows some services considered targets by adversaries. An exciting fact obtained from text mining analysis is that most research works focus on cybersecurity in the energy domain. False data injection is the most famous attack in energy services because it focuses on modifying forecasted demand data [76]. The main issue with energy services, such as smart grids, is connected to network infrastructure and smart meters, which could have some vulnerabilities. This aspect increases the probability
of cyberattacks on smart grid infrastructures [77]. Research focuses on preventing and overcoming cyberattacks by using machine learning techniques, such as artificial neural networks, to solve cybersecurity challenges, especially with the considerable volume of data on power systems [74].

Table 6. Classification of cybersecurity attacks based on target services.

<table>
<thead>
<tr>
<th>Services</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td>Financial institutions are exposed due to their network dependence. Financial services include payment systems or trading platforms. An example of an attacker on financial services is accessing SWIFT credentials to send fraudulent payment orders.</td>
<td>[38]</td>
</tr>
<tr>
<td>The energy</td>
<td>The energy sector is vulnerable to attacks because they need real-time operations. Cyberattacks can generate failure or breakdown of generation, transmission, distribution, or substation systems</td>
<td>[51]</td>
</tr>
<tr>
<td>Healthcare</td>
<td>The prime target is the theft of medical information. Cyber-criminals’ medical information is more valuable than personal financial information. Ransomware attacks are growing on medical devices</td>
<td>[52]</td>
</tr>
</tbody>
</table>

Table 7 shows topics related to cybersecurity in energy facilities. Healthcare is another domain of interest for adversaries for sensitive and personal information [75]. In healthcare, one relevant issue is legacy software [78]. It is difficult for some hospitals or medical centers to migrate their medical records to new systems, e.g., for factors such as budget, data format, or time; this could be a disadvantage from a cybersecurity perspective. Some research is focused on improving authentication methods to reduce this gap [79], following the topics related to healthcare cybersecurity:

- Physical security, two-way authentication, security protocol, and privacy;
- Security medical devices and legacy software.

Adversary takes advantage of vulnerabilities in different domains, such as [80]:

- Hardware failure;
- Software failure;
- Data encryption;
- Loss of backup power;
- Accidental user error;
- External security breach;
- Physical security;
- Accidental user error;
- External security breach.

Table 7. Cybersecurity topics related to energy facilities.

<table>
<thead>
<tr>
<th>Energy Systems</th>
<th>Cybersecurity Scope</th>
<th>Applied Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-physical power system (CPPS)</td>
<td>Intrusion detection</td>
<td>Temporal-topological correlation</td>
</tr>
<tr>
<td>Distribution systems</td>
<td>Anomaly detection</td>
<td>Multi-agent system</td>
</tr>
<tr>
<td>Electric drive system</td>
<td>Attack pattern</td>
<td>Fuzzy feature analysis</td>
</tr>
<tr>
<td>Industrial system</td>
<td>Cyberattack monitoring and detection</td>
<td>Frequent pattern tree</td>
</tr>
<tr>
<td>Smart distribution networks</td>
<td>Situation awareness</td>
<td>State estimation</td>
</tr>
<tr>
<td>Networked control system</td>
<td>Resilience control</td>
<td>Markov chain</td>
</tr>
<tr>
<td>Steam turbines</td>
<td>Active defense</td>
<td>k-connected graph</td>
</tr>
<tr>
<td>Microgrids</td>
<td>Quantization effect</td>
<td>Ruin probability</td>
</tr>
<tr>
<td>Smart grid</td>
<td>Sequential false data injection attacks</td>
<td></td>
</tr>
<tr>
<td>Power outage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stealthy attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>False data injection (FDI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial-of-service (DoS)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The growth of new electronic services and technologies such as IoT, big data, and artificial intelligence have allowed the development of new attack vectors [81,82]. IoT has generated interest by adversaries in carrying out security attacks due to its lack of advanced security and great coverage [83]. IoT solutions are very attractive for attackers because of the variety of attacks that can be performed on different components of IoT, among which we can mention the following [84]:

- Mobile devices;
- Embedded systems;
- Consumer technologies;
- Operational systems.

The growth of crypto-currency and distributed authentication architecture is driving the use of blockchain architecture [85]. Another use of blockchain is in healthcare organizations to improve data integrity, authentication, and privacy issues, especially those with sensitive features such as medical records [86]. On the other hand, IoT is growing in different domains such as healthcare, smart city, and smart home [26]. Establishing authentication such as PKI architectures for IoT ecosystems could be expensive for many IoT devices, so smart contracts based on blockchain architecture are an alternative [87].

Following, we outline the topics related to blockchain and cybersecurity in papers selected in this work, which were developed between 2019 to 2021:

- Energy trading;
- Cryptocurrency, crypto-jacking, money laundering;
- Public organization;
- Decentralized consensus decision-making (DCDM);
- Fuzzy static Bayesian game model (FSB-GM);
- Internet of Things, smart contracts;
- Electronic health records.

Some cyberattacks take advantage of new technologies such as 5G, IoT, and the cloud to perform DDoS attacks [88]. The growth of IoT devices with limited computational resources and lack of security configurations make them vulnerable to different cyberattacks. For instance, Mirai Botnet malware exploited the vulnerabilities of an estimated 600,000 IoT devices, resulting in massive Distributed Denial of Service (DDoS) attacks [89]. Cloud computing services are used to launch Distributed Denial of Service (DDoS) attacks. However, adversaries are focusing on low-rate DDoS attacks because they are more challenging to detect due to their stealthy and low-rate traffic [58].

On the other hand, using the hijacked Connection-less Lightweight Directory Access Protocol, an attacker could perform DDoS attacks at 2.3 terabytes per second [90]. Social media platforms have achieved relevance for interaction and social information exchange. However, the attackers have used them to deceive people and make them victims of attacks [91]. An adversary has found a striking attack target in humans because they can be deceived through persuasion techniques [15]. Attacks based on human vulnerabilities, called social engineering, have grown in recent years [66]. Figure 5 shows a word cloud of topics related to social engineering. We can observe that human factors are relevant in this kind of attack. The pandemic has created tremendous pressure on cybersecurity aspects. During the COVID-19 pandemic, the social engineering attacks carried out were phishing, spamming, and scamming. These attacks were combined with socio-technical methods such as fake emails, websites, and mobile apps [92]. The need to work remotely has changed the attack surface of organizations. Attacks on VPNs, hijacking of video meetings, fake news campaigns, and phishing attacks have increased during the COVID-19 pandemic [15]. According to the text mining process, we identified the following topics related to COVID-19 and cybersecurity:

- Malicious web pages;
- Malicious Mobil Apps;
- Malicious Emails messages;
• Misinformation and fake news;
• Security and privacy.

Figure 5. Word cloud of topics related to Social Engineering.

Challenges in cybersecurity solutions
To face cyberattacks, organizations have established cybersecurity mechanisms that could be physical, software-oriented, or procedural. Below, we show some of the most common defense mechanisms:

• Security intelligence systems;
• Perimeter controls;
• Encryption technologies;
• Data loss prevention;
• Governance risk;
• Automated policy management.

The mechanisms described above are the most common solutions for cyberattacks. However, it is possible to define specific defense mechanisms for each type of cyberattack in some cases. For instance [67], the two defense techniques against phishing attacks are:

• Software-based defense approaches;
• User education.

However, MITRE [93] has defined 245 techniques that the attacker could use for executing cyberattacks. The techniques are distributed in 14 stages; each stage is associated with the attackers’ process of executing cyberattacks. Figure 6 shows the number of techniques associated with each stage. Figure 7 shows the frequency of MITRE techniques included in the works selected in this study, which were developed between 2019 and 2021. Our text mining analysis found that the most relevant techniques are reconnaissance, discovery, lateral movement, collection, command-control, and impact. On this point, it is important to mention that the absence of frequency in other techniques, such as initial access or privilege escalation, is not an indicator that these techniques are not used in cyberattacks. The information shown in Figure 8 reveals that researchers are more focused on the result of one specific technique in their study. However, for the review made, we can observe that not all selected works considered the cycle of a cyberattack; this aspect is relevant for developing a good defense strategy. We found that most of the techniques mentioned in the selected studies focused on gathering information, such as reconnaissance, discovery, and collection.
Figure 6. Cybersecurity Techniques according to MITRE.

Figure 7. Techniques MITRE identified in works selected in this study.

Figure 8. Techniques MITRE used in vertical domains such as Energy, Social Engineering, and IoT.
Figure 8 shows the relation between cybersecurity techniques and domain attacks: energy, IoT, and social engineering. We observed that the relevance of a specific technique depends on the type of cyberattack. For instance, the most relevant techniques in social engineering are reconnaissance, resource development, persistence, and defense evasion. On the other hand, the most relevant techniques in IoT attacks are credential access, lateral movement, and collection. This number of techniques could be a challenge because cybersecurity analysts need to have the capability to detect them in real-time when they are used in cyberattacks to select the best defense strategy.

Figure 9 shows some variants of cybersecurity attacks based on social engineering, which show the incredible versatility of attacks, which can vary depending on the attack techniques used digitally, in person, or by phone.

![Figure 9. Classification of Social Engineering attacks.](image)

Cybersecurity solutions require adapting to new challenges:
- The heterogeneity of IoT solutions;
- The expansion of the attack surface by IoT and Machine Learning;
- Attacks on Cloud infrastructures;
- Cognitive hacking.

Cybersecurity firms and researchers have been developing some alternatives by mainly focusing on anomaly detection. Inside the anomaly detection process, the objective is to detect some pattern, behavior, or component used by attackers [94]. Table 8 shows topic development from 2019 to 2021 related to anomaly detection. Cybersecurity companies and researchers in the field have moved on from reactive solutions to proactive ones [95].

<table>
<thead>
<tr>
<th>The Mechanism Applied Based on</th>
<th>IoT Cybersecurity Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data analysis</td>
<td>IoT attack classification</td>
</tr>
<tr>
<td>ANN</td>
<td>Attack–defense trees</td>
</tr>
<tr>
<td>Graph neural nets</td>
<td>DDoS attacks</td>
</tr>
<tr>
<td>Cognitive packet network</td>
<td>Botnet</td>
</tr>
<tr>
<td>Random neural networks</td>
<td>Attack countermeasures</td>
</tr>
<tr>
<td></td>
<td>Home security threat</td>
</tr>
<tr>
<td></td>
<td>Identification anomaly</td>
</tr>
</tbody>
</table>

Cybersecurity research is trying to stay one step ahead and take advantage of cybersecurity analysts’ cognitive capabilities to define proactive cybersecurity defense strategies. So, several research types are focused on incorporating cognitive models to generate these proactive solutions. In the selected period (2019–2021), several studies included artificial intelligence and machine learning concepts applied to cybersecurity (See Table 9).
Table 9. Topics related to anomalies.

<table>
<thead>
<tr>
<th>Cybersecurity Context</th>
<th>Scope</th>
<th>Applied Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-physical power system (CPPS)</td>
<td>Behavior pattern</td>
<td>Multiagent systems (MASs)</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>Attack pattern</td>
<td>Honeypots</td>
</tr>
<tr>
<td>Connected and automated vehicles (CAVs)</td>
<td>Anomaly detection</td>
<td>Convolution neural network (CNN)</td>
</tr>
<tr>
<td>Smart home</td>
<td>Anomaly identification</td>
<td>Dimensionality reduction</td>
</tr>
<tr>
<td>Intelligent transportation system (ITS)</td>
<td>Attack pattern</td>
<td>Principal component analysis</td>
</tr>
</tbody>
</table>

The use of supervised machine learning such as Decision Tree (DT), Support Vector Machine (SVM), Naïve Bayes (NB), Random Forest (RF), and unsupervised algorithms such as K-nearest neighbor (kNN) and Artificial Neural Network (ANN’s) for building intrusion detection systems (IDS), or anomaly pattern detection, are the most exciting topics in cybersecurity. A relevant fact observed in the selected papers was the growing number of studies related to deep learning applications. Researchers have considered deep learning a good alternative for facing different cybersecurity issues. How can deep learning be applied to detect IoT attacks, APT, DDoS, malware, and anomaly detection? An interesting fact is that there are three variants of deep learning:

1. Deep learning;
2. Deep reinforcement learning;

Table 10 shows topics identified from papers in the text mining process related to security in IoT. Research focus on defense solutions to face DDoS include the use of cognitive sciences approaches such as [88]:

- Deep learning;
- Machine learning;
- Deep Convolutional Neural Network (CNN);
- Genetic algorithms;
- Game theory;
- PCA;
- Large-Scale System (LSS.)

Table 10. Machine learning applied to cybersecurity.

<table>
<thead>
<tr>
<th>Learning Techniques</th>
<th>Cybersecurity Application Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision Tree</td>
<td>Cryptojacking</td>
</tr>
<tr>
<td>k-nearest neighbors</td>
<td>Internet of things</td>
</tr>
<tr>
<td>Random Forest</td>
<td>Advanced persistent threat</td>
</tr>
<tr>
<td>Naïve Bayes</td>
<td>Collaborative attacks</td>
</tr>
<tr>
<td>Recurrent Neural Networks (RNNs)</td>
<td>Traffic flow monitoring</td>
</tr>
<tr>
<td>Generative adversarial networks</td>
<td>Distributed denial-of-service attacks</td>
</tr>
<tr>
<td>Deep learning</td>
<td>Malicious javascript detection</td>
</tr>
<tr>
<td>Deep reinforcement learning</td>
<td>Intruder detection</td>
</tr>
<tr>
<td>Deep transfer learning</td>
<td></td>
</tr>
</tbody>
</table>

Below there are some approaches of studies between 2019 and 2021 with solutions based on machine learning and deep learning for identifying malicious URLs or sentiment analysis in social media:

- Deep learning for word embedding;
- Natural language processing and sentiment analysis on online social networks.
Game theory is another alternative of cognitive sciences applied to cybersecurity. Its objective is to try to guess the next step for adversaries during cyberattacks. Figure 10 shows a word cloud with topics related to game theory. We identified that game theory could be applied to different domains such as energy, investment, cyber-physical systems, and computer security. Additionally, game theory research shows approaches in defense mechanisms, information dissemination, and decision making. Game theory uses computational modeling to take advantage of security analysts’ cognitive processes and adversaries to improve decision-making based on information analysis to face attacks [96]. Game theory is mostly used in the economy field, which is responsible for studying optimal decisions and strategies for given situations. According to the definition of Nash equilibrium, the strategy or set of strategies of each player responds to the other players’ actions to maximize each player’s profit. The player’s strategy is a specific action at a particular moment of the game [96]. A game is defined as interacting with two or more participants seeking a reward. During the game, participants develop strategies to maximize their profit. Players do not necessarily represent people; they can be organizations or groups. There are two classic games in-game theory: cooperative games and non-cooperative games. There are two ways for the mathematical representation of a game: a standard form using matrices and an extensive form using decision trees. A cooperative game is based on the players’ interaction reaching agreements to establish the decision-making that each player will carry out, achieving the objective of reaching coalitions, and determining how to distribute the rewards [97]. However, in non-cooperative games, each player must decide what decision to make without knowing the rest’s decisions. These are more subject to the reality of what happens in the cybersecurity domain. Complete information games are those in which each player knows all the events in the game’s course from the beginning, especially when making a decision. A classic example of a complete information game is the game of chess. Incomplete information games, in most cases, are simultaneous decision-making games, so each player knows something that the others do not. Interactions between an adversary and the user could be modeled based on two players’ stochastic game. Using a non-linear program is possible to compute Nash equilibrium to define the best response strategies for players [98]. Developing games that consider cost, time, reward, and performance could define effective game strategies.

Figure 10. Game theory research topics.

4. Results and Discussion
Cognitive Cybersecurity Model

Our text mining process found that the works selected in this study do not consider indirect cognitive processes or cognitive models such as OODA or MAPE-K. Including
game theory in cybersecurity can lead to strategies to minimize cyberattacks from a cognitive perspective. A complete information model is the most appropriate to obtain the best decision from the game theory approach. Big network environments are very complex scenarios for developing detection and protection cybersecurity solutions. The integration of machine learning and deep learning with game theory techniques could improve proactive security solutions. Concerning Figure 2, Cassenti et al. [23] mention that technology does not consider the user learning processes. From our perspective, the game theory approach could be a solution to this because it validates the user’s decision-making processes based on a set of experiences and patterns. From the game theory perspective, if the user (player) improves the learning process or the decision-making process based on cognitive processes, the probability of winning the game increases. In this sense, we propose in Figure 11, a cognitive cybersecurity model based on integrating cognitive process and machine learning, deep learning, and game theory approach applied in cybersecurity. As shown in Figure 11, we structured the model into three layers. The first layer of the cognitive model addresses the aspects of perception related to the cognitive processes. It associates them with sources of information that can be analyzed to establish patterns of anomalies based on space-time criteria. The second layer establishes the association of the understanding processes with machine learning (ML) techniques or deep learning (DL) that can be used for the anomaly detection processes. This association must have bi-directional feedback between analysts and technology to improve ML or DL algorithms’ training processes. The way towards the analysis allows us to generate perspicacity about cybersecurity situation awareness. Additionally, this feedback should support the improvement in the analyst’s cognitive processes to detect cyberattacks.

Finally, the third layer associates the cognitive projection process with game theory techniques. At this level, the decision-making processes to establish the best defense strategy must be supported by the information obtained from the ML and DL processes carried out in the lower layer. The bidirectional relation, in one sense, is the computational model of the game theory component. In another sense, it should improve the cognitive decision-making processes. However, establishing the proposed model is complex without obtaining all the information from the analyst and adversary (See Figure 12). Modeling the adversary’s characteristics would allow analysts to have a complete vision to establish a better decision. For instance, they knew that the adversary could use a combination of tools (T), techniques (Th), and procedures (C2F). However, the list of tools and procedures can be extensive and varied. Below is a list of the most widespread RATs:

- OSSEC is an open-source HIDS for data gathering;
- Snort is an intrusion Prevention System (IPS) to detect malicious network activity;
- Suricata is an open-source system for real-time intrusion detection (IDS) and intrusion prevention (IPS);
• Security Onion is open-source used for threat hunting, security monitoring, and log management;
• OpenWIPS-NG is an intrusion prevention system (IPS), preferred for wireless packet tracking;
• Fail2ban is a software that scans log files and bans IPs that show malicious activity. Procedures used for adversaries could be based on Command and Control (C2) frameworks. Following, we list some C2 frameworks:
  ■ FudgeC2 is a campaign-orientated Powershell C2;
  ■ Callidus is an open-source C2 framework that leverages Outlook, OneNote, Microsoft Teams for command and control;
  ■ APfell is a cross-platform, OPSEC aware, red teaming, post-exploitation C2 framework;
  ■ DaaC2: is an open-source C2 framework that makes use of Discord as a C2;
  ■ Koadic is an open-source for post-exploitation;
  ■ TrevorC2 is a client/server model for masking command and control through web browsers

Figure 12. Attack and defense components.

We represent in Equation (1) the attack as the combination of tools (T), procedures (C2F), and techniques (Th), where w represents the weights based on the tool, procedure, and technique used by the adversary.

\[
\text{Attack} = w(T) + w(C2F) + w(Th)
\]  

On the other hand, cybersecurity analysts developed a set of cognitive processes to establish the defense process. From a macro vision, the analyst must decide if a possible event could be an attack or not, based on the cognitive process of perception. Bitzer et al. [99] mention that perceptual decision making is applied to two-alternative forced-choice tasks to judge perceptual feature differences. According to Bitzer, drift-diffusion models have been used to quantitatively analyze behavioral data, i.e., reaction times and accuracy. In the same vein, Dale et al. [100] mention that the cognitive analysis of vast amounts of data requires the application of the heuristics process and that people often mistakenly judge the likelihood of a situation by not taking all relevant data into account. However, according to Nikolić et al. [101], the application of heuristics as mental strategies and certain deformations in the thoughts and perceptions of decision makers affect their attitudes and approach to problem solving. Trueblood et al. [102] mention that we need to understand how people make perceptual decisions to improve training to minimize misdiagnoses in the medical field. So, let us adapt this approach to cybersecurity: the defense strategy must be oriented toward the factors associated with the cognitive process; this is described in Equation (2), where: R.T is the Response Time associated with the time
for executing a defense action by a cybersecurity analyst; $H.T$ is the heuristic thinking associated with the process of selecting a decision; $B$ is the Bias related to human thinking, and $S.A$ is the speed accuracy in the decision-making process.

$$\text{Cognitive Process} = w_1(R.T) + w_2(H.T) + w_3(B) + w_4(S.A)$$

(2)

where $w_i$ is the weight assigned to each variable.

Once the cognitive process has been carried out, the best decision is made considering the weight of each variable in the cognitive process, expressed in Equation (3).

$$\text{Decision}(j) = (\Delta P_j) \cdot \text{Cognitive process}$$

(3)

where $\Delta P_j$ is the variation due to weights in cognitive processes.

Therefore, the defense strategy is expressed as Equation (4).

$$\text{Defense} = (\text{Decision}(j)) + \text{Error}$$

(4)

However, analysts in the cybersecurity decision-making process could be affected by factors such as Bias and speed accuracy. Bias ($B$) effects and speed-accuracy effects are ubiquitous in experimental psychology. Bias effects arise when the two stimulus alternatives occur with unequal frequency or have unequal rewards attached to them. Speed-accuracy ($SA$) effects arise as the result of explicit instructions emphasizing speed or accuracy [103]. Computational models of decision making present a solution to this problem. In particular, we choose Response Time (RT) models such as the drift-diffusion model (D.D.M.), proposed by Ratcliff [103], and the linear ballistic accumulator (LBA) model, proposed by Brown [104]. Accumulator models assume that evidence is accumulated over time until a threshold amount is reached for a commitment to that response option. These models contain four primary parameters related to different psychological components of simple decisions: caution, Bias, stimulus processing, and motor sense.

5. Discussion

In this study, a literature review for the period 2019 to 2021 was carried out. Text-mining was used to determine the most addressed topics in chosen papers in the area of cybersecurity. This exploratory analysis focused on the most relevant used words in the content. The words we found included security, attack, detection, networks, machine learning, and power. This result made us deduce that cybersecurity research has been related to detecting cyberattacks on electricity grids through machine learning in recent years. Another finding in our literature review was that the mainstream research has been dedicated to implementing proactive cybersecurity. Cognitive science is being applied for this purpose. We actually found relevant contributions in which machine learning and deep learning-based solutions were proposed. Figure 13 shows the percentage of works that use machine learning and deep learning, respectively, from the papers included in the literature review that we carried out.

![Figure 13. Deep Learning vs. Machine Learning.](image)

The period 2019 to 2021 was atypical in the way some activities were carried out worldwide due to it being in the context of a pandemic driven by COVID-19. In this context,
the reasoning in some sectors has to consider the greater use of technological resources, such as tele-education, tele-health, government, and private electronic services. From the perspective of the digital transformation of organizations and cities, the pandemic was an essential accelerator in the adoption of technologies in specific sectors. It made organizations and people more dependent on technological resources. However, this context generated the need to address essential aspects of cybersecurity. For example, children increased their availability of internet connections, increasing their exposure to online risks [105]. Organizations based their logistics and supply chain processes on internet-based technologies, expanding the attack surface [106]. The inclusion of IoT for data collection and process automation increases the need to acquire an end-to-end secure IoT environment [107]. The use of social engineering attacks based on the human need to obtain information about the pandemic increased their probability of accessing fake news or being a victim of social engineering attacks [108].

During the same period, 2019–2021, even within the context of the pandemic, there was no reduction in attacks on organizations’ information systems or the impact on people through social engineering attacks. The literature review carried out for the period 2019–2021 showed that the financial, energy, and healthcare services were the most attacked, and the fastest-growing attacks were DDoS, Ransomware, Mobile malware, and Phishing. This context highlighted the need for organizations to strengthen their cybersecurity strategies concerning:

- Security intelligence systems;
- Perimeter controls;
- Encryption technologies;
- Data loss prevention;
- Governance risk;
- Automated policy management.

While from a user perspective, it highlighted the need to generate more awareness concerning:

- Malicious web pages;
- Malicious Mobile Apps;
- Malicious Email messages;
- Misinformation and fake news;
- Security and privacy.

Faced with this continuous growth of cybersecurity attacks and the need to improve security strategies to protect people and organizations, the literature review carried out shows that research has promoted the use of learning techniques as a resource to strengthen their security strategies, specifically to automate activities such as behavior pattern, attack pattern, anomaly detection, and anomaly identification. The most-used learning techniques in the cybersecurity domain correspond to Decision Tree, k-nearest neighbors, Random Forest, Naive Bayes, Recurrent Neural Networks (RNNs), generative adversarial networks, deep learning, deep reinforcement learning, and deep transfer learning, and you can see a growing interest in what corresponds to deep learning. Although game theory is not new in its application to cybersecurity, it has had significant growth in recent years, especially in improving decision-making processes related to cybersecurity in the financial, energy, and critical infrastructure sectors.

This finding encourages future work to understand how security organizations and specialists are preparing to adopt cognitive techniques based on learning as a security strategy. It has also proposed a possible future analysis of how our organizations can have their learning capacity (situational awareness and self-awareness) capable of establishing that it is being attacked and can establish a level of resilience. From the user’s perspective, it highlights how these learning techniques can be used to strengthen cognitive processes in detecting security attacks, especially those based on social engineering techniques.
The design of cognitive models applied in cybersecurity compared to traditional security methods is based on obtaining or abstracting information from the user’s cognitive processes, organization, and adversary roles, for which a cognitive model could define the following steps:

1. Implementation of infrastructure for handling a large volume of data;
2. Incorporation of cognitive sciences in security strategies such as artificial intelligence, machine learning, data analytics, and psychology;
3. Cognitive model design based on:
   A. Cognitive processes Observe–Orient–Decide–Act model (OODA);
   B. the Monitor–Analyze–Plan–Execute model (MAPE-K).
4. Identification of cognitive processes:
   A. Users’ or analysts’ cognitive processes;
   B. The adversary’s behavioral characteristics.

6. Conclusions

The literature review found that much attention has been paid to proactive cybersecurity solutions, acceptable cybersecurity practices, and cybersecurity hygiene strategies for mitigating cyberattacks. In this context, the use of cognitive science techniques has grown significantly. Answers in this area are being proposed, and they mainly look for the improvement of the response time of cyberattacks’ countermeasures that work in real-time.

In general, cognitive science is being used to understand the behavior of adversaries to minimize the impact of cyberattacks. In this context, machine learning and deep learning are the techniques that are used the most. The model we propose tries to fill the gap that exists in automatizing cognitive science without considering the users learning processes. Our opinion is that incorporating game theory represents a significant contribution to bringing cognitive sciences to decision-making processes. A set of heuristic, Bias, and quantitative perception measures was defined as part of the cognitive cybersecurity model we have proposed. These measures make it possible to integrate machine learning and deep learning techniques with game theory. We conclude that social and psychological analysis in cybersecurity may improve the process of obtaining information that helps in the decision-making processes.

The present work, investigating the period 2019–2021, understands the evolution of cybersecurity under an atypical context such as a pandemic. Work carried out during the year 2022 has not been considered because it is a period still in progress and has had a change based on the progressive return of activities. Therefore, we believe that future complementary work would be to analyze how this new change has affected cybersecurity processes.

This work was based on the literature review of scientific bases. It would be interesting to extend it with a study of different organizations and their perspective on the inclusion or management of cognitive techniques applied to cybersecurity, including understanding how these techniques can provide security in the requirements analysis, and by performing security configurations in the context of DevOps [109] and Digital transformation [110], in addition to how cognitive techniques tie in with Open-source tools, which are widely used to maintain network security, endpoint security, and system security [111]. Although our literature review does not show them explicitly, these are very relevant topics in cybersecurity today. This leads us in future work to propose new search strings that allow us to expand our study to these topics.

Author Contributions: Conceptualization, R.O.A. and W.F.; methodology, R.O.A.; validation, W.F.; formal analysis, R.O.A.; investigation, M.C.; data curation, I.O.-G.; writing—review and editing, I.O.-G. and G.N.; funding acquisition, I.O.-G. and G.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.
Acknowledgments: The authors would like to thank the Universidad de las Fuerzas Armadas ESPE of Sangolquí, Ecuador, for the resources granted for the development of the research project entitled: “Detection and Mitigation of Social Engineering attacks applying Cognitive Security, Code: PIC-ESPE-2020-SE”. The author also acknowledges the Universidad de Las Américas of Ecuador and his Engineer degree in Information Technology for support in this work. Additionally, we want to thank the members of the group IDEIAGEOCA for all their support in the research.

Conflicts of Interest: The authors declare no conflict of interest.

References


73. Song, X.; Chen, C.; Cui, B.; Fu, J. Malicious JavaScript Detection Based on Bidirectional LSTM Model. Appl. Sci. 2020, 10, 3440. [CrossRef]


91. Sai, A.M.V.V.; Li, Y. A Survey on Privacy Issues in Mobile Social Networks. IEEE Access 2020, 8, 130906–130921. [CrossRef]


103. Smith, P.; Ratcliff, R. An introduction to the diffusion model of decision making. In *An Introduction to Model-Based Cognitive Neuroscience*; Springer: New York, NY, USA, 2015; pp. 49–70. [CrossRef]


