electronics

Article

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] IDEIAGEOCA, Universidad Politécnica Salesiana, Cuenca 010102, Ecuador; mcazares@ups.edu.ec (M.C.); gnavas@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

check for updates

Citation: Andrade, R.O.; Fuertes, W.; Cazares, M.; Ortiz-Garcés, I.; Navas, G. An Exploratory Study of Cognitive Sciences Applied to Cybersecurity. *Electronics* **2022**, *11*, 1692. https://doi.org/10.3390/electronics11111692

Academic Editor: Krzysztof Szczypiorski

Received: 25 April 2022
Accepted: 23 May 2022
Published: 26 May 2022

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.

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

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).

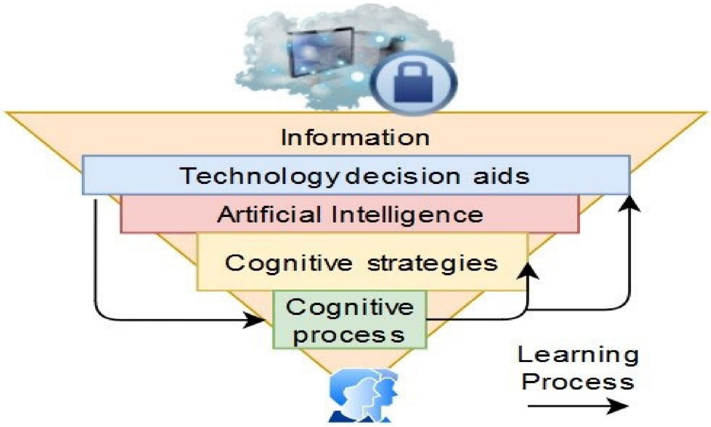

Figure 1. Relation between Information, Technology aids, and Cognitive Processes.

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".

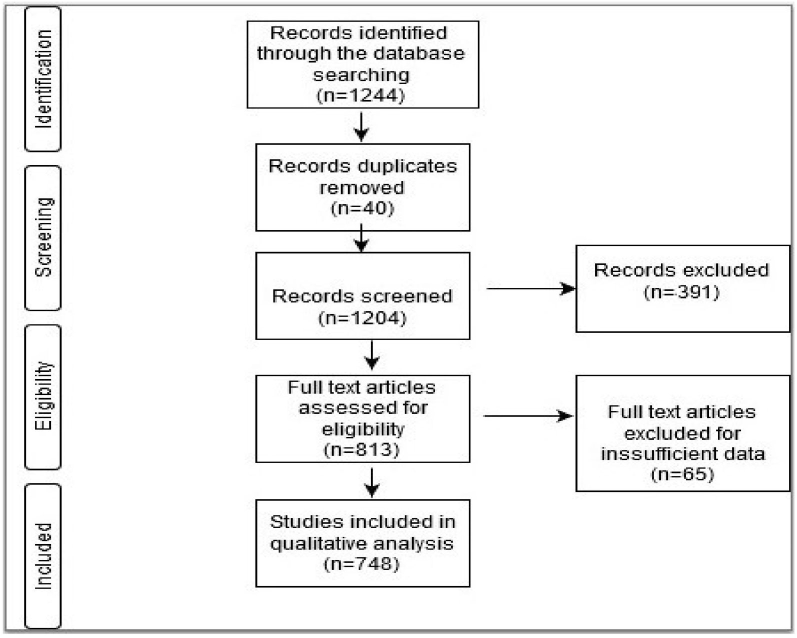

Figure 2. SLR according to Prisma methodology.

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.

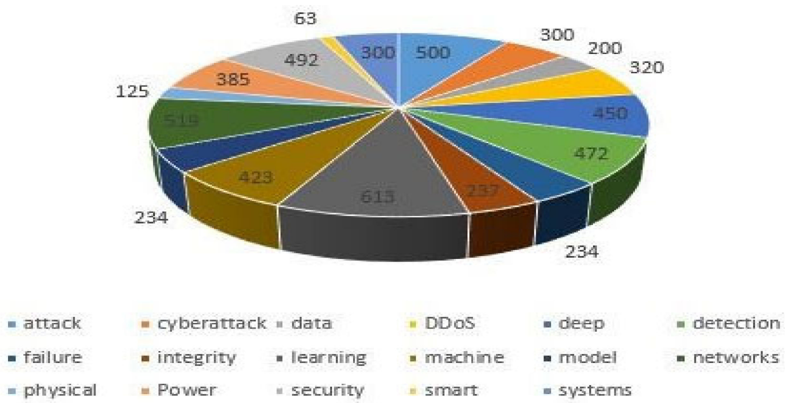

Figure 3. General topics in cybersecurity between 2019 to 2021.

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 tokenization 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.

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

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

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 sex-extort 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 3. Cybersecurity attacks detected in text mining process.

Type	Description	Reference
Phishing	Is a malicious and deliberate attempt of sending fake messages that appear to come from a reputable source	[35–40]
Insider threats	Are encountered in international security, geopolitics, business, trade, and cybersecurity. Insider threats could be considered more damaging than outsider attacks	[41–43]
APT	Are designed to steal corporate or national secrets.	[44–46]
Cybercrime	Criminal activity either targets or uses a computer, a computer network, or a networked device.	[47,48]
Malware	Malicious software designed to infiltrate a device without knowledge	[49,50]
DDoS	Denial of service attack on a computer system or network that causes a service or resource tobe inaccessible to legitimate users	[51–55]
Ransomware	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	[56–60]
Mobile malware	Its name suggests malicious software that targets explicitly the operating systems on mobile phones	[61–64]
Watering hole	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	[65,66]

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.

Attack	Americas	Europa	Asia
DDoS	13%	17%	23%
Ransomware	3%	4%	6%
Mobile malware	15%	15%	25%
Phishing	7%	11%	14%

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).

Type	Human	Machine
Phishing	X	-
Insider threats	X	X
Web Based Attacks	-	X
Advanced persistent threat (APT)	-	X
Spam	X	X
Identity theft	X	X
Data breach	X	X
Botnets	-	X
Physical manipulation	X	-
Cybercrime	X	X
Malware	X	X
DDoS	-	X
Ransomware	-	X
Mobile malware	X	X
Watering hole	X	X
Information leakage	X	X

X represents the affectation 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.

Services	Description	Reference
Financial services	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.	[38]
The energy	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	[51]
Healthcare	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	[52]

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.

Energy Systems	Cybersecurity Scope	Applied Mechanism
Cyber-physical power system (CPPS)	Intrusion detection	Temporal-topological correlation
Distribution systems	Anomaly detection	Multi-agent system
Electric drive system	Attack pattern	Fuzzy feature analysis
Industrial system	Cyberattack monitoring and detection	Frequent pattern tree
Smart distribution networks	Situation awareness	State estimation
Networked control system	Resilience control	Markov chain
Steam turbines	Active defense	k-connected graph
Microgrids	Quantization effect	Ruin probability
Smart grid	Sequential false data injection attacks	
	Power outage	
	Stealthy attack	
	False data injection (FDI)	
	Denial-of-service (DoS)	

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.

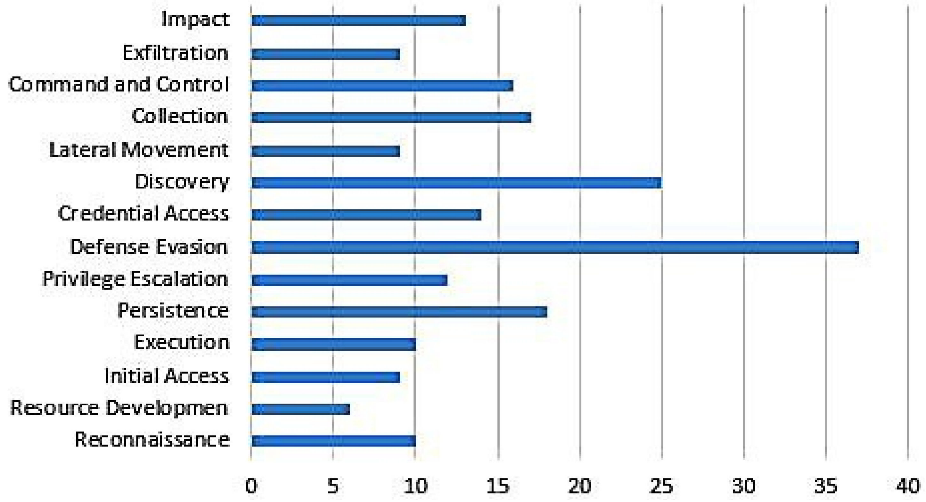

Figure 6. Cybersecurity Techniques according to MITRE.

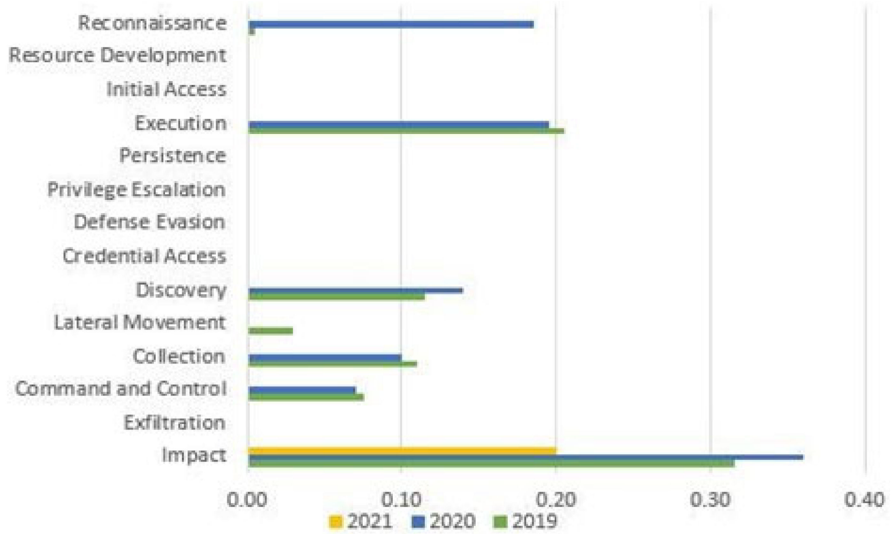

Figure 7. Techniques MITRE identified in works selected in this study.

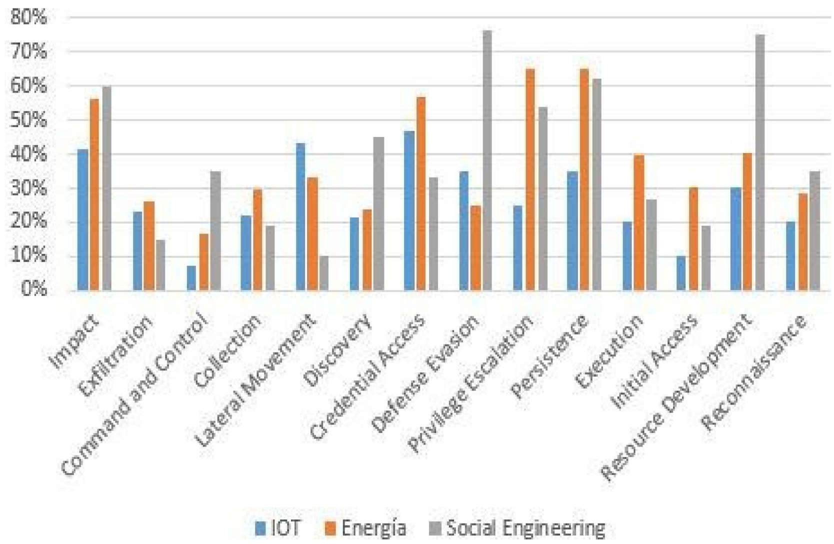

Figure 8. Techniques MITRE used in vertical domains such as Energy, Social Engineering, and IoT.

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.

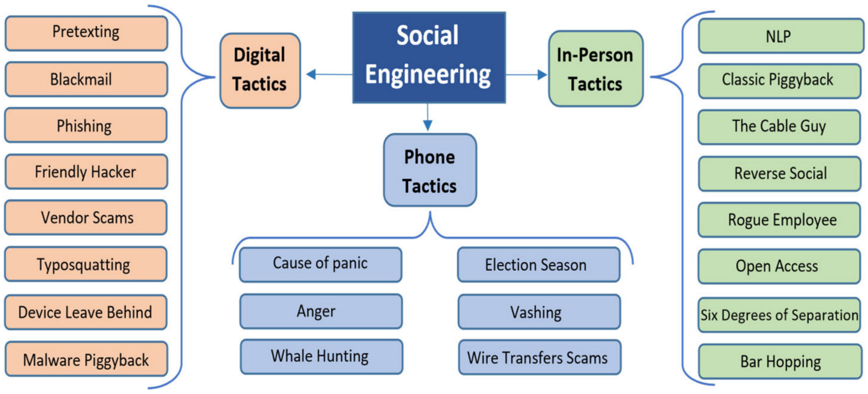

Figure 9. Classification of Social Engineering attacks.

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 8. Cybersecurity topics related to IoT.

The Mechanism Applied Based on	IoT Cybersecurity Context
Data analysis	IoT attack classification
ANN	Attack–defense trees
Graph neural nets	DDoS attacks
Cognitive packet network	Botnet
Random neural networks	Attack countermeasures
	Home security threat
	Identification anomaly

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 earning concepts applied to cybersecurity (See Table 9).

Table 9. Topics related to anomalies.

Cybersecurity Context	Scope	Applied Mechanism
Cyber-physical power system (CPPS)	Behavior pattern	Multiagentsystems (MASs)
Internet of Things	Attack pattern	Honeypots
Connected and automated vehicles (CAVs)	Anomaly detection	Convolution neural network (CNN)
Smart home	Anomaly identification	Dimensionality reduction
Intelligent transportation system (ITS)	Attack pattern	Principal component analysis

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;
3. Deep transfer 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.

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

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.

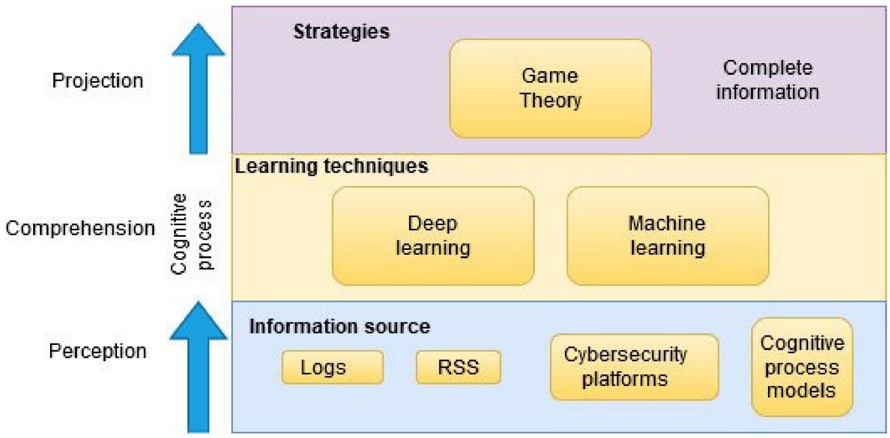

Figure 11. Proposal for a Cognitive Cybersecurity model.

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

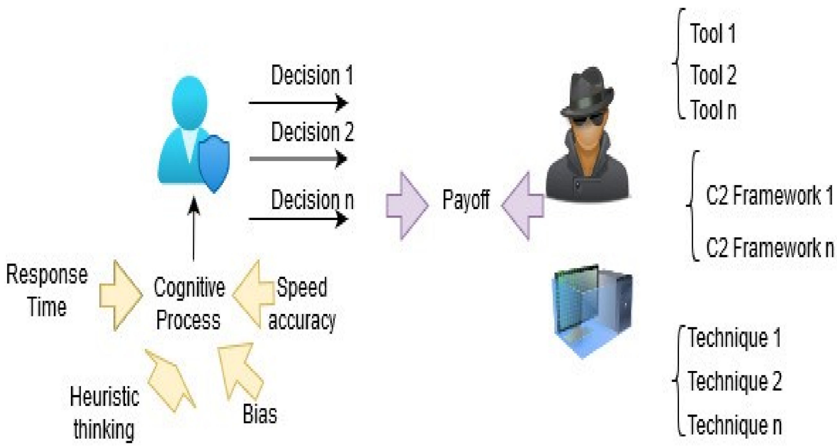

Figure 12. Attack and defense components.

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.

$$Attack = w(T) + w(C2F) + w(T\,h) \quad (1)$$

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.

$$\text{Cognitive Process} = w1(R.T) + w2(H.T) + w3(B) + w4(S.A) \quad (2)$$

where wi 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).

$$\text{Decision}(j) = (\Delta P\ j)\ \text{Cognitive process} \quad (3)$$

where Delta P j is the variation due to weights in cognitive processes.

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

$$\text{Defense} = (\text{Decision } j) + \text{Error} \quad (4)$$

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.

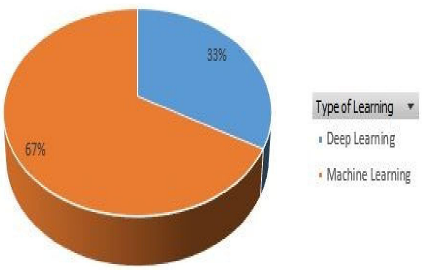

Figure 13. Deep Learning vs. Machine Learning.

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 perid 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. Additionality, 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

1. WEF: Word Economic Forum. The Global Risks Report 2021. Available online: https://www.weforum.org/reports/the-global-risks-report-2021 (accessed on 21 May 2021).
2. Donevski, M.; Zia, T. A survey of anomaly and automation from a cybersecurity perspective. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6. [CrossRef]
3. Yang, Q.; Jia, X.; Li, X.; Feng, J.; Li, W.; Lee, J. Evaluating Feature Selection and Anomaly Detection Methods of Hard Drive Failure Prediction. *IEEE Trans. Reliab.* **2020**, *70*, 749–760. [CrossRef]
4. Alrashdi, I.; Alqazzaz, A.; Aloufi, E.; Alharthi, R.; Zohdy, M.; Ming, H. AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning. In Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 0305–0310. [CrossRef]
5. Andrade, R.; Torres, J. Self-awareness as an enabler of cognitive security. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 701–708. [CrossRef]
6. Leung, H. An integrated decision support system based on the human ooda loop. In Proceedings of the 2018 IEEE 17th International Conference on Cognitive Informatics Cognitive Computing (ICCI*CC), Berkeley, CA, USA, 16–18 July 2018; p. 1. [CrossRef]
7. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Xu, M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access* **2020**, *8*, 222310–222354. [CrossRef]
8. Brückner, M.; Scheffer, T. Stackelberg games for adversarial prediction problems. In Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York, NY, USA, 21–24 August 2011; pp. 547–555. [CrossRef]
9. Andrade, R.; Torres, J. Enhancing intelligence soc with big data tools. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 1076–1080. [CrossRef]
10. Le, D.C.; Zincir-Heywood, N. Exploring adversarial properties of insider threat detection. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020; pp. 1–9. [CrossRef]
11. Rajivan, P.; Gonzalez, C. Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Front. Psychol.* **2018**, *9*, 135. [CrossRef] [PubMed]
12. Andrade, R.; Yoo, S.G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *J. Inf. Secur. Appl.* **2019**, *48*, 102352. [CrossRef]
13. Alqahtani, H.; Kavakli-Thorne, M. Exploring factors affecting user's cybersecurity behaviour by using mobile augmented reality app (cybar). In *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering. ICCAE, Sydney, NSW, Australia, 14–16 February 2020*; Association for Computing Machinery: New York, NY, USA; pp. 129–135. [CrossRef]
14. Kakkad, V.; Shah, H.; Patel, R.; Doshi, N. A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing. *Procedia Comput. Sci.* **2019**, *155*, 680–685. [CrossRef]
15. Andrade, R.O.; Ortiz-Garces, I.; Cazares, M. Cybersecurity attacks on smart home during covid-19 pandemic. In Proceedings of the Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2021; pp. 398–404. [CrossRef]
16. Orunsolu, A.; Sodiya, A.; Akinwale, A. A predictive model for phishing detection. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 232–247. [CrossRef]
17. Schubert, A.-L.; Frischkorn, G.T.; Hagemann, D.; Voss, A. Trait Characteristics of Diffusion Model Parameters. *J. Intell.* **2016**, *4*, 7. [CrossRef]
18. Simmons, C.; Ellis, C.; Shiva, S.; Dasgupta, D.; Wu, C. Avoidit: A cyber attack taxonomy. In Proceedings of the 9th Annual Symposium on Information Assurance (ASIA'14), Albany, NY, USA, 3–4 June 2014.
19. Venkatesan, S.; Sugrim, S.; Izmailov, R.; Chiang, C.J.; Chadha, R.; Doshi, B.; Hoffman, B.; Allison Newcomb, E.; Buchler, N. On detecting manifestation of adversary characteristics. In Proceedings of the MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018; pp. 431–437. [CrossRef]
20. Andrade, R.O.; Yoo, S.G.; Tello-Oquendo, L.; Ortiz-Garces, I. A Comprehensive Study of the IoT Cybersecurity in Smart Cities. *IEEE Access* **2020**, *8*, 228922–228941. [CrossRef]

21. Zambrano, P.; Torres, J.; Tello-Oquendo, L.; Jacome, R.; Benalcazar, M.E.; Andrade, R.; Fuertes, W. Technical Mapping of the Grooming Anatomy Using Machine Learning Paradigms: An Information Security Approach. *IEEE Access* **2019**, *7*, 142129–142146. [CrossRef]
22. Lebiere, C.; Morrison, D.; Abdelzaher, T.; Hu, S.; Gonzalez, C.; Buchler, N.; Veksler, V. Cognitive models of prediction as decision aids. In Proceedings of the 14th International Conference on Cognitive Modeling, University Park, PA, USA, 4–6 August 2016.
23. Cassenti, D.; Veksler, V. Using cognitive modeling for adaptive automation triggering. In Proceedings of the AHFE 2017 International Conference on Human Factors in Simulation and Modeling, Los Angeles, CA, USA, 17–21 July 2017; pp. 378–390. [CrossRef]
24. Cameron, L.; Jago, L. *Cognitive Strategies*; Springer: New York, NY, USA, 2013; p. 453. [CrossRef]
25. Mengist, W.; Soromessa, T.; Legese, G. Method for conducting systematic literature review and meta-analysis for environmental science research. *MethodsX* **2019**, *7*, 100777. [CrossRef]
26. Andrade, R.O.; Yoo, S.G. A Comprehensive Study of the Use of LoRa in the Development of Smart Cities. *Appl. Sci.* **2019**, *9*, 4753. [CrossRef]
27. Antons, D.; Grünwald, E.; Cichy, P.; Salge, T.O. The application of text mining methods in innovation research: Current state, evolution patterns, and development priorities. *R&D Manag.* **2020**, *50*, 329–351. [CrossRef]
28. Lee, C.; Cheng, C.; Zeleke, A. Can text mining technique be used as an alternative tool for qualitative research in education? In Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Las Vegas, NV, USA, 30 June–2 July 2014; pp. 1–6. [CrossRef]
29. Ceron, J.C.A.; Gomez, L.J.P.; Ceballos, H.G.; Cantu-Ortiz, F.J. Twitter data analysis on the topic: Tec de monterrey. In Proceedings of the 2020 3rd International Conference on Computer Applications Information Security (ICCAIS), Riyadh, Saudi Arabia, 19–21 March 2020; pp. 1–6. [CrossRef]
30. USDJ. New York Man Pleads Guilty to Cyberstalking after Harassing and Sextorting Multiple Victims. 2021. Available online: https://www.justice.gov/usao-mdfl/pr/new-york-man-pleads-guilty-cyberstalking-after-harassing-and-sextorting-multiple (accessed on 25 May 2021).
31. CISA. Ransomware Activity Targeting the Healthcare and Public Health Sector. 2021. Available online: https://us-cert.cisa.gov/ncas/alerts/aa20--302a (accessed on 25 May 2021).
32. FBI. Fraudsters Prey on Emotions and Bank Accounts in Money Mule Schemes. 2021. Available online: https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fraudsters-prey-on-emotions-and-bank-accounts-in-money-mule-schemes (accessed on 25 May 2021).
33. Al-Mohannadi, H.; Mirza, Q.; Namanya, A.; Awan, I.; Cullen, A.; Disso, J. Cyber-attack modeling analysis techniques: An overview. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 69–76. [CrossRef]
34. ENISA. Threat Landscape. 2020. Available online: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends (accessed on 12 February 2021).
35. Singh, C. Meenu: Phishing website detection based on machine learning: A survey. In Proceedings of the 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 March 2020; pp. 398–404. [CrossRef]
36. Athulya, A.; Praveen, K. Towards the detection of phishing attacks. In Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184), Tirunelveli, India, 15–17 June 2020; pp. 337–343. [CrossRef]
37. Chapla, H.; Kotak, R.; Joiser, M. A machine learning approach for url based web phishing using fuzzy logic as classifier. In Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 17–19 July 2019; pp. 383–388. [CrossRef]
38. Zubair Hasan, K.M.; Hasan, M.Z.; Zahan, N. Automated prediction of phishing websites using deep convolutional neural network. In Proceedings of the 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), Rajshahi, Bangladesh, 11–12 July 2019; pp. 1–4. [CrossRef]
39. Kunju, M.V.; Dainel, E.; Anthony, H.C.; Bhelwa, S. Evaluation of phishing techniques based on machine learning. In Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 15–17 May 2019; pp. 963–968. [CrossRef]
40. Zheng, K.; Wu, T.; Wang, X.; Wu, B.; Wu, C. A Session and Dialogue-Based Social Engineering Framework. *IEEE Access* **2019**, *7*, 67781–67794. [CrossRef]
41. Joshi, C.; Aliaga, J.R.; Insua, D.R. Insider Threat Modeling: An Adversarial Risk Analysis Approach. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1131–1142. [CrossRef]
42. Duncan, A.; Creese, S.; Goldsmith, M. A combined attack-tree and kill-chain approach to designing attack-detection strategies for malicious insiders in cloud computing. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019; pp. 1–9. [CrossRef]
43. Khan, A.Y.; Latif, R.; Latif, S.; Tahir, S.; Batool, G.; Saba, T. Malicious Insider Attack Detection in IoTs Using Data Analytics. *IEEE Access* **2019**, *8*, 11743–11753. [CrossRef]
44. Alshamrani, A.; Myneni, S.; Chowdhary, A.; Huang, D. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1851–1877. [CrossRef]

45. Su, Y. Research on apt attack based on game model. In Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020; Volume 1, pp. 295–299. [CrossRef]
46. Khosravi, M.; Ladani, B.T. Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection. *IEEE Access* **2020**, *8*, 162642–162656. [CrossRef]
47. Sajal, S.Z.; Jahan, I.; Nygard, K.E. A survey on cyber security threats and challenges in modem society. In Proceedings of the 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 20–22 May 2019; pp. 525–528. [CrossRef]
48. Park, J.; Cho, D.; Lee, J.K.; Lee, B. The Economics of Cybercrime. *ACM Trans. Manag. Inf. Syst.* **2019**, *10*, 1–23. [CrossRef]
49. Cao, M.; Badihi, S.; Ahmed, K.; Xiong, P.; Rubin, J. On benign features in malware detection. In Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering ASE'20, Virtual Event, Australia, 21–25 December 2020; Association for Computing Machinery: New York, NY, USA; pp. 1234–1238. [CrossRef]
50. Samantray, O.P.; Tripathy, S.N.; Das, S.K. A study to understand malware behavior through malware analysis. In Proceedings of the 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 29–30 March 2019; pp. 1–5. [CrossRef]
51. Vishwakarma, R.; Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommun. Syst.* **2019**, *73*, 3–25. [CrossRef]
52. Liang, X.; Znati, T. An empirical study of intelligent approaches to ddos detection in large scale networks. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 821–827. [CrossRef]
53. Priya, S.S.; Sivaram, M.; Yuvaraj, D.; Jayanthiladevi, A. Machine learning based ddos detection. In Proceedings of the 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 12–14 March 2020; pp. 234–237. [CrossRef]
54. Nandi, S.; Phadikar, S.; Majumder, K. Detection of ddos attack and classification using a hybrid approach. In Proceedings of the 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), Guwahati, India, 27 February–1 March 2020; pp. 41–47. [CrossRef]
55. Rohit, M.H.; Fahim, S.M.; Khan, A.H.A. Mitigating and detecting ddos attack on iot environment. In Proceedings of the 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 29 November–1 December 2019; pp. 5–8. [CrossRef]
56. Agrawal, N.; Tapaswi, S. Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3769–3795. [CrossRef]
57. Bijitha, C.V.; Sukumaran, R.; Nath, H.V. A survey on ransomware detection techniques. In *Secure Knowledge Management in Artificial Intelligence Era*; Sahay, S.K., Goel, N., Patil, V., Jadliwala, M., Eds.; Springer: Singapore, 2020; pp. 55–68.
58. Alzahrani, A.; Alshahrani, H.; Alshehri, A.; Fu, H. An intelligent behavior-based ransomware detection system for android platform. In Proceedings of the 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Los Angeles, CA, USA, 12–14 December 2019; pp. 28–35. [CrossRef]
59. Adamov, A.; Carlsson, A. Reinforcement learning for anti-ransomware testing. In Proceedings of the 2020 IEEE East-West Design Test Symposium (EWDTS), Varna, Bulgaria, 4–7 September 2020; pp. 1–5. [CrossRef]
60. Bahrani, A.; Bidgly, A.J. Ransomware detection using process mining and classification algorithms. In Proceedings of the 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Mashhad, Iran, 28–29 August 2019; pp. 73–77. [CrossRef]
61. Shahpasand, M.; Hamey, L.; Vatsalan, D.; Xue, M. Adversarial attacks on mobile malware detection. In Proceedings of the 2019 IEEE 1st International Workshop on Artificial Intelligence for Mobile (AI4Mobile), Hangzhou, China, 24 February 2019; pp. 17–20. [CrossRef]
62. Tahtaci, B.; Canbay, B. Android malware detection using machine learning. In Proceedings of the 2020 Innovations in Intelligent Systems and Applications Conference (ASYU), Istanbul, Turkey, 15–17 October 2020; pp. 1–6. [CrossRef]
63. Mbaziira, A.V.; Diaz-Gonzales, J.; Liu, M. Deep learning in detection of mobile malware. *J. Comput. Sci. Coll.* **2020**, *36*, 80–88.
64. Diaz-Gonzalez, J.; Mbaziira, A.V.; Liu, M. An exploratory deep learning approach to mobile malware detection. *J. Comput. Sci. Coll.* **2019**, *35*, 219.
65. Allen, J.; Yang, Z.; Landen, M.; Bhat, R.; Grover, H.; Chang, A.; Ji, Y.; Perdisci, R.; Lee, W. Mnemosyne: An effective and efficient postmortem watering hole attack investigation system. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, CCS'20, Virtual Event, USA, 9–13 November 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 787–802. [CrossRef]
66. Research CP. CYBER ATTACK TRENDS: 2020 MID-YEAR REPORT—Check Point Research. 2021. Available online: https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/ (accessed on 21 May 2021).
67. Dasgupta, D.; Akhtar, Z.; Sen, S. Machine learning in cybersecurity: A comprehensive survey. *J. Déf. Model. Simul. Appl. Methodol. Technol.* **2020**, *19*, 57–106. [CrossRef]
68. Brewer, J.N.; Dimitoglou, G. Evaluation of attack vectors and risks in automobiles and road infrastructure. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; pp. 84–89. [CrossRef]

69. Li, T.; Wang, K.; Horkoff, J. Towards effective assessment for social engineering attacks. In Proceedings of the 2019 IEEE 27th International Requirements Engineering Conference (RE), Jeju, Korea, 23–27 September 2019; pp. 392–397. [CrossRef]
70. Tandale, K.D.; Pawar, S.N. Different types of phishing attacks and detection techniques: A review. In Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Aurangabad, India, 30–31 October 2020; pp. 295–299. [CrossRef]
71. Badami, C.; Kettani, H. On Malware Detection in the Android Operating System. In Proceedings of the 4th International Conference on Algorithms, Computing and Systems, Rabat, Morocco, 6–8 January 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 45–50. [CrossRef]
72. George, R.; Jalal, R.; Raju, R.M.; Sunny, S.S.; Hari, M. High responsive plug-in for malicious url detection. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 357–359. [CrossRef]
73. Song, X.; Chen, C.; Cui, B.; Fu, J. Malicious JavaScript Detection Based on Bidirectional LSTM Model. *Appl. Sci.* **2020**, *10*, 3440. [CrossRef]
74. Dogaru, D.I.; Dumitrache, I. Cyber security of smart grids in the context of big data and machine learning. In Proceedings of the 2019 22nd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 28–30 May 2019; pp. 61–67. [CrossRef]
75. Spanakis, E.G.; Bonomi, S.; Sfakianakis, S.; Santucci, G.; Lenti, S.; Sorella, M.; Tanasache, F.D.; Palleschi, A.; Ciccotelli, C.; Sakkalis, V.; et al. Cyber-attacks and threats for healthcare—A multi-layer thread analysis. In Proceedings of the 2020 42nd Annual International Conference of the IEEE Engineering in Medicine Biology Society (EMBC), Montreal, QC, Canada, 20–24 July 2020; pp. 5705–5708. [CrossRef]
76. Pilz, M.; Naeini, F.B.; Grammont, K.; Smagghe, C.; Davis, M.; Nebel, J.-C.; Al-Fagih, L.; Pfluegel, E. Security attacks on smart grid scheduling and their defences: A game-theoretic approach. *Int. J. Inf. Secur.* **2019**, *19*, 427–443. [CrossRef]
77. Canaan, B.; Colicchio, B.; Abdeslam, D.O. Microgrid Cyber-Security: Review and Challenges toward Resilience. *Appl. Sci.* **2020**, *10*, 5649. [CrossRef]
78. Tervoort, T.; De Oliveira, M.T.; Pieters, W.; Van Gelder, P.; Olabarriaga, S.D.; Marquering, H. Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review. *IEEE Access* **2020**, *8*, 84352–84361. [CrossRef]
79. Fatima, K.; Nawaz, S.; Mehrban, S. Biometric authentication in health care sector: A survey. In Proceedings of the 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 1–2 November 2019; pp. 1–10. [CrossRef]
80. Kazemi, Z.; Fazeli, M.; Hely, D.; Beroulle, V. Hardware security vulnerability assessment to identify the potential risks in a critical embedded application. In Proceedings of the 2020 IEEE 26th International Symposium on On-Line Testing and Robust System Design (IOLTS), Napoli, Italy, 13–15 July 2020; pp. 1–6. [CrossRef]
81. Kotenko, I.; Saenko, I.; Kushnerevich, A.; Branitskiy, A. Attack detection in iot critical infrastructures: A machine learning and big data processing approach. In Proceedings of the 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Pavia, Italy, 13–15 February 2019; pp. 340–347. [CrossRef]
82. Sen, S.; Jayawardena, C. Analysis of cyber-attack in big data iot and cyber-physical systems—A technical approach to cybersecurity modeling. In Proceedings of the 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 29–31 March 2019; pp. 1–7. [CrossRef]
83. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
84. Gressl, L.; Steger, C.; Neffe, U. Consideration of security attacks in the design space exploration of embedded systems. In Proceedings of the 2019 22nd Euromicro Conference on Digital System Design (DSD), Kallithea, Greece, 28–30 August 2019; pp. 530–537. [CrossRef]
85. Chauhan, V.; Arora, G. A review paper on cryptocurrency portfolio management. In Proceedings of the 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), Greater Noida, India, 18–19 October 2019; pp. 60–62. [CrossRef]
86. Shahnaz, A.; Qamar, U.; Khalid, A. Using Blockchain for Electronic Health Records. *IEEE Access* **2019**, *7*, 147782–147795. [CrossRef]
87. Gong, X.; Liu, E.; Wang, R. Blockchain-based iot application using smart contracts: Case study of m2m autonomous trading. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 781–785. [CrossRef]
88. Chen, Y.-W.; Sheu, J.-P.; Kuo, Y.-C.; Van Cuong, N. Design and implementation of iot ddos attacks detection system based on machine learning. In Proceedings of the 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 15–18 June 2020; pp. 122–127. [CrossRef]
89. Ahmed, Z.; Danish, S.M.; Qureshi, H.K.; Lestas, M. Protecting iots from mirai botnet attacks using blockchains. In Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 11–13 September 2019; pp. 1–6. [CrossRef]
90. Sambangi, S.; Gondi, L. A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression. *Proceedings* **2020**, *63*, 51.
91. Sai, A.M.V.V.; Li, Y. A Survey on Privacy Issues in Mobile Social Networks. *IEEE Access* **2020**, *8*, 130906–130921. [CrossRef]

92. Hijji, M.; Alam, G. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access* **2021**, *9*, 7152–7169. [CrossRef] [PubMed]
93. MITRE. Enterprise Attacks Techniques MITRE. 2021. Available online: https://attack.mitre.org/techniques/enterprise/ (accessed on 25 May 2021).
94. Wankhede, S.B. Anomaly detection using machine learning techniques. In Proceedings of the 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 29–31 March 2019; pp. 1–3. [CrossRef]
95. Wollaber, A.; Peñna, J.; Blease, B.; Shing, L.; Alperin, K.; Vilvovsky, S.; Trepagnier, P.; Wagner, N.; Leonard, L. Proactive cyber situation awareness via high performance computing. In Proceedings of the 2019 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 24–26 September 2019; pp. 1–7. [CrossRef]
96. Iqbal, A.; Gunn, L.J.; Guo, M.; Babar, M.A.; Abbott, D. Game Theoretical Modelling of Network/Cybersecurity. *IEEE Access* **2019**, *7*, 154167–154179. [CrossRef]
97. Zhou, X.; Cheng, S.; Liu, Y. A Cooperative Game Theory-Based Algorithm for Overlapping Community Detection. *IEEE Access* **2020**, *8*, 68417–68425. [CrossRef]
98. Kwiatkowska, M.; Norman, G.; Parker, D.; Santos, G. Prism-games 3.0: Stochastic game verification with concurrency, equilibria and time. In *Computer Aided Verification*; Lahiri, S.K., Wang, C., Eds.; Springer: Cham, Switzerland, 2020; pp. 475–487.
99. Bitzer, S.; Park, H.; Blankenburg, F.; Kiebel, S.J. Perceptual decision making: Drift-diffusion model is equivalent to a Bayesian model. *Front. Hum. Neurosci.* **2014**, *8*, 102. [CrossRef]
100. Dale, S. Heuristics and biases: The science of decision-making. *Bus. Inf. Rev.* **2015**, *32*, 93–99. [CrossRef]
101. Nikolić, J. Biases in the decision-making process and possibilities of overcoming them. *Èkon. Horiz.* **2018**, *20*, 45–59. [CrossRef]
102. Trueblood, J.S.; Holmes, W.R.; Seegmiller, A.C.; Douds, J.; Compton, M.; Szentirmai, E.; Woodruff, M.; Huang, W.; Stratton, C.; Eichbaum, Q. The impact of speed and bias on the cognitive processes of experts and novices in medical image decision-making. *Cogn. Res. Princ. Implic.* **2018**, *3*, 28. [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]
104. Nishiguchi, Y.; Sakamoto, J.; Kunisato, Y.; Takano, K. Linear Ballistic Accumulator Modeling of Attentional Bias Modification Revealed Disturbed Evidence Accumulation of Negative Information by Explicit Instruction. *Front. Psychol.* **2019**, *10*, 2447. [CrossRef]
105. Quayyum, F.; Cruzes, D.S.; Jaccheri, L. Cybersecurity awareness for children: A systematic literature review. *Int. J. Child Comput. Interact.* **2021**, *30*, 100343. [CrossRef]
106. Cheung, K.-F.; Bell, M.G.; Bhattacharjya, J. Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transp. Res. Part E: Logist. Transp. Rev.* **2021**, *146*, 102217. [CrossRef]
107. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
108. Wang, Z.; Zhu, H.; Sun, L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access* **2021**, *9*, 11895–11910. [CrossRef]
109. Rahman, A.U.; Williams, L. Software Security in DevOps: Synthesizing Practitioners' Perceptions and Practices. In Proceedings of the 2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED), Austin, TX, USA, 14–15 May 2016; pp. 70–76.
110. Maglaras, L.; Drivas, G.; Chouliaras, N.; Boiten, E.; Lambrinoudakis, C.; Ioannidis, S. Cybersecurity in the Era of Digital Transformation: The case of Greece. In Proceedings of the 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), Zhenjiang, China, 27–29 November 2020; pp. 1–5. [CrossRef]
111. Sharma, R.; Dangi, S.; Mishra, P. A Comprehensive Review on Encryption based Open Source Cyber Security Tools. In Proceedings of the 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 7–9 October 2021; pp. 614–619. [CrossRef]