Cognitive Sciences in Cybersecurity

Subjects: Computer Science, Cybernetics

Contributor: Roberto O. Andrade, Walter Fuertes, María Cazares, Iván Ortiz-Garcés, Gustavo Navas

Cognitive security is the interception between cognitive science and artificial intelligence techniques used to protect institutions against cyberattacks. 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. In general, cognitive science is being used to understand the behavior of adversaries to minimize the impact of cyberattacks.

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, it was 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].

2. 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, researchers 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 [10].

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 [11]. 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 [12] and diffusion models [13] are used for modeling user response time. Simmons et al. [14] 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. [15] 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.

3. 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 [16][17]. Cognitive science could enhance the processes of perception, comprehension, and projection used by cybersecurity analysts to detect cyberattacks and establish future defense actions [9].

4. Cognitive Process

Currently, information is increasing fast, and the availability of processing data surpasses human capacities. According to [18], 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. [19] 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 [20], 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**).

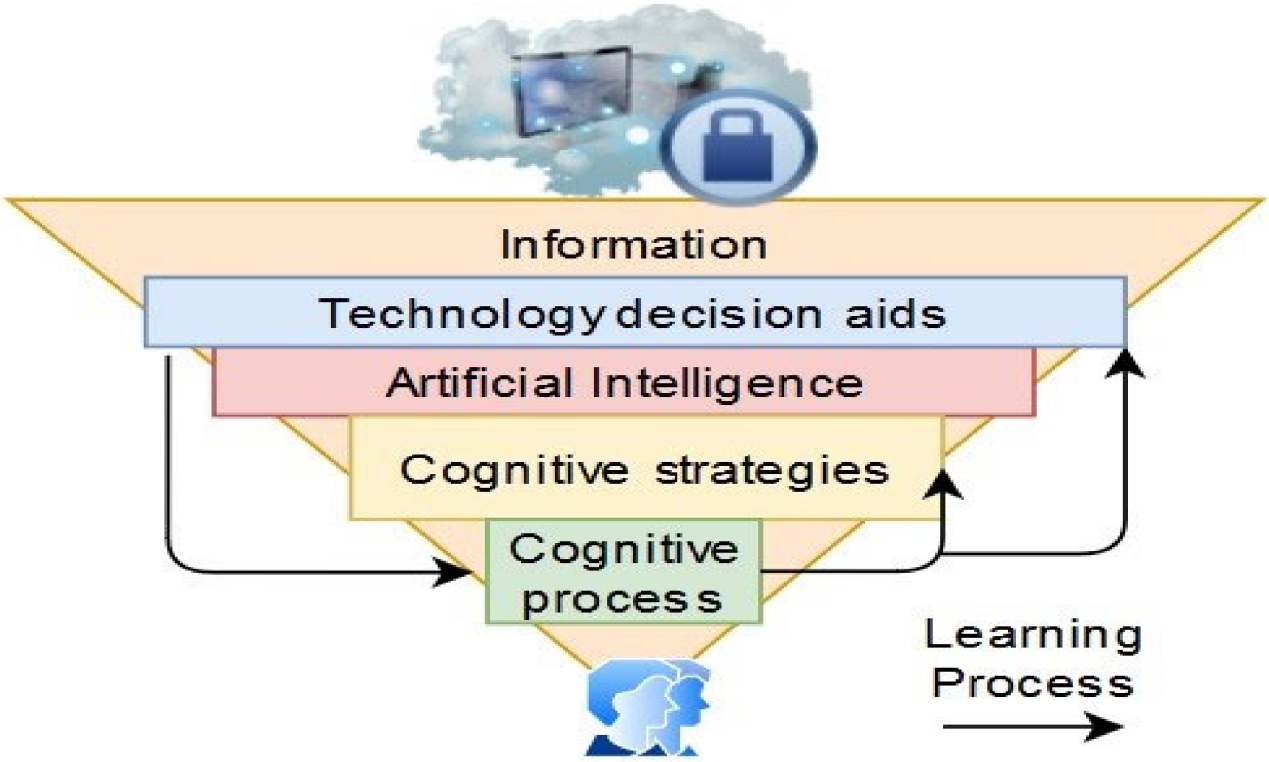

Figure 1. Relation between Information, Technology aids, and Cognitive Processes.

5. 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].

6. Prisma Methodology

The PRISMA methodology is divided into four stages: identification, screening, eligibility analysis, and inclusion [21]. 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 research[22].

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.
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.
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.
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.

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.
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.
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.
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.
10. 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.
11. 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.
12. Orunsolu, A.; Sodiya, A.; Akinwale, A. A predictive model for phishing detection. J. King Saud Univ. Comput. Inf. Sci. 2022, 34, 232–247.
13. Schubert, A.-L.; Frischkorn, G.T.; Hagemann, D.; Voss, A. Trait Characteristics of Diffusion Model Parameters. J. Intell. 2016, 4, 7.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. Cameron, L.; Jago, L. Cognitive Strategies; Springer: New York, NY, USA, 2013; p. 453.
21. Mengist, W.; Soromessa, T.; Legese, G. Method for conducting systematic literature review and meta-analysis for environmental science research. MethodsX 2019, 7, 100777.
22. 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.