Journal of Information Security and Applications 48 (2019) 102352

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Cognitive security: A comprehensive study of cognitive science in cybersecurity

Roberto O Andrade*, Sang Guun Yoo

Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito, Ecuador

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Cognitive security
Cognitive science
Situation awareness
Cyber operations

ABSTRACT

Nowadays, IoT, cloud computing, mobile and social networks are generating a transformation in social processes. Nevertheless, this technological change rise to new threats and security attacks that produce new and complex cybersecurity scenarios with large volumes of data and different attack vectors that can exceeded the cognitive skills of security analysts. In this context, cognitive sciences can enhance the cognitive processes, which can help to security analysts to establish actions in less time and more efficiently within cybersecurity operations. This works presents a cognitive security model that integrates technological solutions such as Big Data, Machine Learning, and Support Decision Systems with the cognitive processes of security analysts used to generate knowledge, understanding and execution of security response actions. The model considers alternatives to establish the automation process in the execution of cognitive tasks defined in the cyber operations processes and includes the analyst as the central axis in the processes of validation and decision making through the use of MAPE-K, OODA and Human in the Loop.

1. Introduction

The United Nations Organization, in the United Nations Development Program [49] and International Telecommunication Union's [18] Connect 2020 Agenda, highlights that the information society empowered by an interconnected world accelerates the economic and social development of society in different countries. Technologies such as IoT, cloud computing, Big Data and mobile enhanced the information society through the access to different data sources, large amount of data and the collaboration of people from anywhere in the world; and millions of devices are connected every year to meet this goal. According to [13], in the year 2017 there were 8.3 billion of connected devices, 11.19 billion of devices were quantified in the year 2018, and by 2020 approximately 20.4 billion of devices will be connected. Statista [35] - projects 30.73 billion of connected devices by year 2020 and 75.44 billion by year 2025, while Forbes [12] indicates that investment in IoT devices will present a growth of 215 billion in the year 2018 to 835 billion by year 2020. The interconnection of all (people, things and processes) and the access to large amount of information are changing the way we work, learn and socialize [10]; generating new models of urban management and development such as smart cities [50] or sensitive cities [17]. Smart cities establish a sensorization layer [41] and data exchange layer [21] in order to generate knowledge for decision making process in aspects such as mobility, transportation, consumption of natural resources or environment changes. At home, connected devices such as televisions, refrigerators, lights, and support virtual assistants like Siri, Alexa or Google Assistant changes the social interactions of people. In this context, a person has the ability to open a door from a mobile device or request a song from computer and play it on speakers located in different places in the house. Today toys are also interconnected to the Internet, IBM presented a cognitive toy, which consists on a dinosaur connected to its Watson cognitive platform that can interact with a child based on structured dialogues with the ability to learn with each interaction. However, this interconnected world raise new threats and risks within cyberspace [34] where the human is a key element in the dynamics of cybersecurity; for instance, one user who opens an email infected by malware, an attacker that analyze the vulnerabilities and gaps to build the attack, the security analyst that find mechanisms for detect and contain attacks or the Chief Information Security Officer (CISO) that must make decisions based on analysis of security risk. This context motivates us in this work define our research proposal in two topics:

1. Aspects of human behavior within the context of cybersecurity operations.
2. Establishment of Cybersecurity Situation Awareness (CSA) to understand the security procedures, operational tasks

* Corresponding author.
E-mail addresses: roberto.andrade@epn.edu.ec (R.O. Andrade), sang.yoo@epn.edu.ec (S.G. Yoo).

https://doi.org/10.1016/j.jisa.2019.06.008
2214-2126/

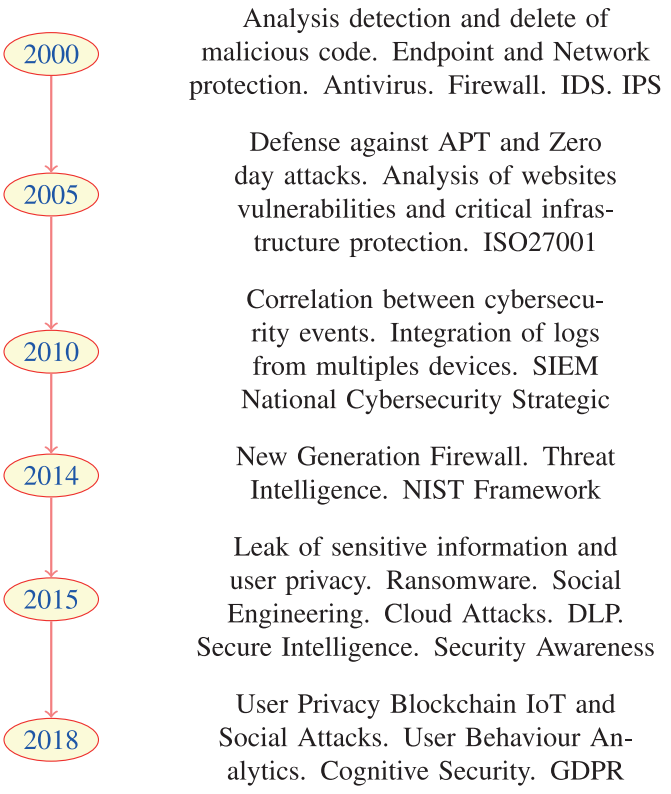

Fig. 1. Timeline in cybersecurity, challenges and road-map.

and the knowledge generated from historical cybersecurity events that permit define defensive strategies.

The interdisciplinary scientific study of psychology, computational science, linguistics, philosophy and neuroscience to understand the human mind has been defined as cognitive sciences [32]. The application in the field of cybersecurity allows an interrelation between the procedures, security practices, the knowledge generated by computer systems, security blogs, vulnerability bulletins and the experience of security specialists based on the tasks they perform daily, generating a cognition (awareness or insight) about cybersecurity situation. The collaboration between humans and machines, the application of statistical methodologies, the use of machine learning and Big Data could allow enhanced or extended the cognitive skills of security specialists at Security Operations Centers (SOC) or Security Incident Response Teams (CSIRT), raising the interest of research on the application of this solutions focused on cybersecurity processes.

The Fig. 1, we present the evolution of cybersecurity regarding the processes of detection of malicious behavior focused on the protection of information in critical infrastructures and users. Although technology plays an important role in cybersecurity the human is the key player in the dynamics in cyberspace in their different roles: as user, attacker or defender. The security analyst must focus on the situation of cybersecurity of the organization through the use of cognitive sciences, which could improve the cybersecurity processes for detection and response of security incidents.

2. Background

2.1. Challenges in cybersecurity

Technology and social changes are generating new challenges for security specialists in commercial and academic environments. According to projections by Forbes and Gartner, Government organizations such as NSA, NIST and European Commission, some challenges in cybersecurity are:

- Algorithms in Artificial Intelligence (AI), uses organizational or personal data to generate predictions, this data may be sensitive, so is necessary to enhanced the mechanisms of protection of information especially for personal data. In AI, attackers could tamper data affecting the results obtained, for that is necessary to ensure the integrity of the data. Misuse of AI could be possible too, and be used to attack systems or even people like as the slaughterbots, which are drones that use AI to search and kill politicians. Some challenges in cybersecurity about the use of artificial intelligence are:
  - Privacy of information used in AI.
  - Integrity of information used in AI.
  - Misuse of AI.
- Ransomware, has become a powerful weapon of cybercrime. Since 2012, there have been several attacks of ransomware such as reventon, cryptolocker, cryptowall, wannacry. However, they are not the only ones, between 2014 and 2017 there have been identified 327 families of ransomware, which have generated a total of 184 million attacks. Statista (2017) estimates for year 2019 losses of 11.5 billion dollars for product of ransomware attacks. Some challenges in cybersecurity about this aspect are:
  - Identify ransomware patterns.
  - Establish contention processes to prevent ransomware distribution.
  - Define data protection schemes.
- Blockchain, the use of crypto-currency is potentially considered as an option to optimize the electronic transfer processes in banking, health or business. However, there are some challenges at the security level:
  - Improve recovery time in case of failure by decentralized administration.
  - Assurance the correct functioning of intelligent contracts.
  - Assurance the infrastructure that supports blockchain.
- IoT security, according to Gartner [13] by year 2020 investment of 2.9 billion dollars and approximately 20 billion connected devices generate IOT to worldwide. Attacks of IoT Bonet increased by 600 % since 2016, being the best known Mirai Bonet that affected sites like CNN, Netflix, Reddit, and twitter. Is necessary to face the following challenges in IoT related to cybersecurity:
  - Secure communications between IoT devices.
  - Authorization and authentication of devices.
  - Privacy and data integrity.
  - Device updates management.
  - Identity theft of devices.
- Serverless Apps security, containers in the cloud allows reduce the operative cost and accelerate the delivery times to the user, when use service models available in the cloud to implement applications and services some security considerations are:
  - Authentication broken.
  - Unsecured serverless configurations.
  - Inadequate monitoring.
  - Dependencies of the insecurities of the third parties.

Complementary to analyze the security challenges from the academic perspective, we conducted an analysis of 30 conferences held between 2016 and 2018 with the sponsor of universities, ACM and IEEE. A compiled of research topics are present in the Table 1 grouped within the three levels of action in the cybersecurity field: Strategic, Tactical and Operational. From the academic and com-

Table 1
Research topics in cybersecurity.

Level	Research topic
Strategic	Real-time situation awareness
	Knowledge representation
	Measuring the impact of threats
	Risk modeling
	Decision making for security
Tactical	Measuring the impact of threats Automated security aids
	Collaborative defense approach Information assurance
Operational	Computer Forensics
	Spam detection
	Botnet detection
	Anomalous behavior detection
	Detection of adversarial attacks
	Decision making for security
	Vulnerability testing
	Threat detection
	Zero-day attack

mercial perspectives there is a wide scope of research and development in the field of cybersecurity for the coming years.

2.2. Security incidents response

Although technological solutions for the protection of cybersecurity have been improved, is necessary consider the establishment of proactive defense strategies, even more with the large number of variants of threats and attacks in continuous expansion with the use of emerging technologies and the change of human social interaction. Some of the attacks that organizations face daily are:

- Attacks on IoT industrial systems.
- Malware propagation.
- IoT botnet.
- DDoS and remote attacks.

The goal of security incidents response is to reduce or contain the impact of a security attack that allow the organization return to a security state defined as acceptable [51]. Some organizations define as strategy to handle security incidents established security incident response teams called CSIRT, CERT or SIRT [19]. Additionally, security incident response allow to organizations complies with other aspects like:

- Improve compliance with regulations or standards.
- Rapid threat detection and remediation.
- Reduction of the risk of exploiting vulnerabilities.
- Simplify efforts in security operations.

Triange. Organizations faces different security attacks simultaneously for that in the security incident process the activity of *triange* is defined to prioritize the attention of security incidents based on a categorization previously made in function of the risk impact of cybersecurity attacks. In order to carry out the triange process the organization must previously establish the following steps [37]:

1. Identification of the incident,
2. Incident registration,
3. Categorization of the incident,
4. Prioritization of the incident,
5. Early Diagnosis,
6. Escalation of the incident,
7. Resolution of the incident, and
8. Closure of the incident.

In an adequate triange process, security analysts must understand the situation awareness of cybersecurity in the organization to identify, and predict threats or security attacks. To achieve this situation awareness analysts, need to process large amounts of information and correlate them in time and space variables. This activity requires great concentration and cognitive skills of the security analyst that can be affected by different factors:

- High stress,
- High false alarm rate,
- Low situation awareness,
- Little experience,
- Unstructured tasks,
- Non-standardized methodology to identify and respond to attacks,
- Large amounts of data and information,
- Uncertain sources of information, and
- Lack of performance metrics from analysts and Security Operation Center (SOC) or CSIRTs

2.3. Cognitive sciences in cybersecurity

The perspectives in the field of cybersecurity regarding cognitive sciences are find solutions to enhanced the capacities related to the human factor, especially in complex systems that are generated with the use of technologies such as cloud, mobile, IoT and social networks that produce large amounts of information. Nowadays, in the scientific field becomes imperative analyze the contributions of cognitive sciences to augmented human capacities for the execution of cybersecurity tasks that require the use of cognitive skills. Cognitive science could contribute to enhanced the processes of perception, comprehension and projection that are part of the self-learning of the human, as shown in Fig. 2.

Psychology and Cybersecurity. Awareness is one concept defined from the field of psychology as the capacity of one human to generate understanding about his life, based on his experiences (Baker, 1987). This concept has been adapted by many researchers to the field of engineering and computer systems, for example Lewis et al. (2016) [27] defines self-awareness of a computational system as the ability to obtain knowledge about itself based on internal and external events. In the work of Camara [8] self-awareness is defined as the capacity of autonomy, social capacity and pro-activity that a computer system can has to generate knowledge about itself and its environment and determine the actions that will be executed according to that knowledge. In addition, Kounev et al. [22] and Lewis et al. (2011) [26] define self-awareness of computational system such as the process or capability of a computer system to acquire the following three properties at the time of execution:

- Auto-reflective: has the awareness of its software architecture, hardware infrastructure and execution environment to achieve its operational objectives.
- Auto-predictive: has the ability to predict the effect due to a dynamic change resulting from possible adaptation actions.
- Self-adaptive: can adapt proactively to the environment to continue achieving its operational objectives.

2.4. Weakness of cognitive systems

The capability of generated levels of cybersecurity awareness in an organization allows determining the type of threats and attacks, maintaining adequate levels of security, and defining proactive strategies to face present and future attacks or threats. The proposed cognitive security model seeks to integrate different solutions to improve cybersecurity operations; however, it still presents weaknesses associated with the inherent weaknesses of each component.

In the case of use artificial intelligence in cybersecurity, a knowledge base is generated by the security analyst and this is

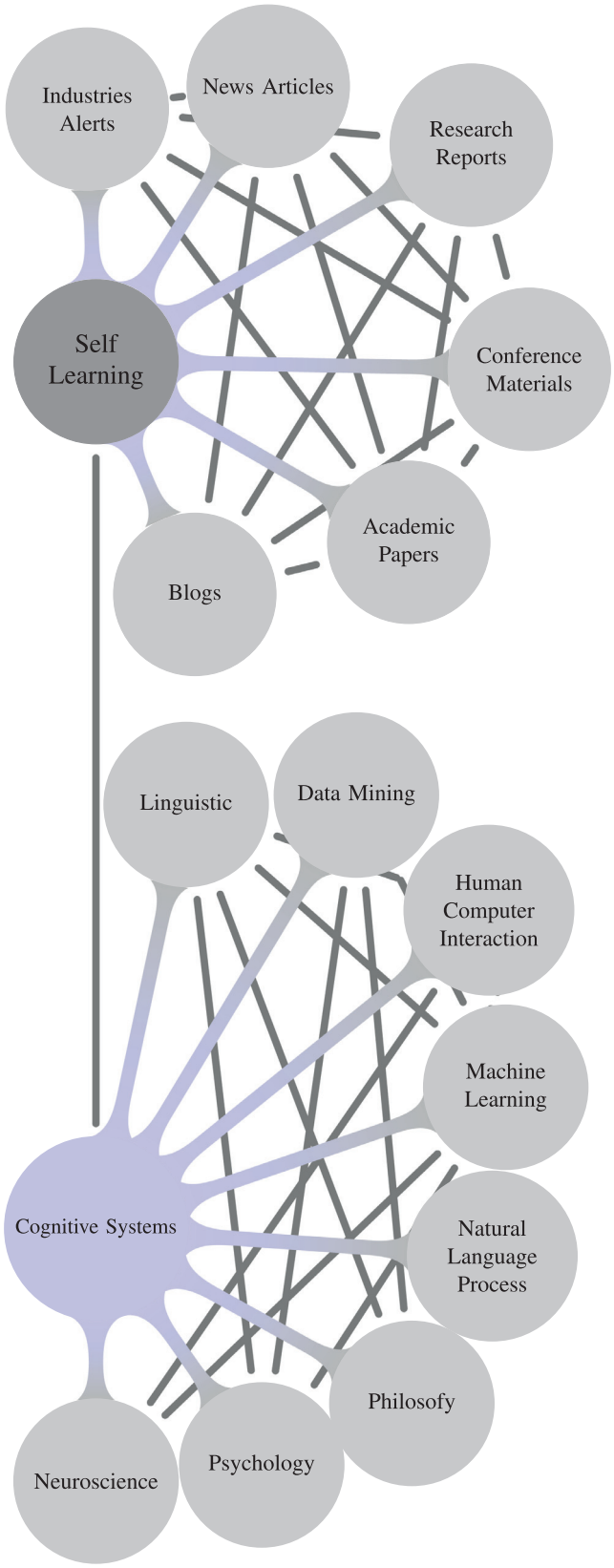

Fig. 2. Cognitive tasks and process in cyber-sec operations.

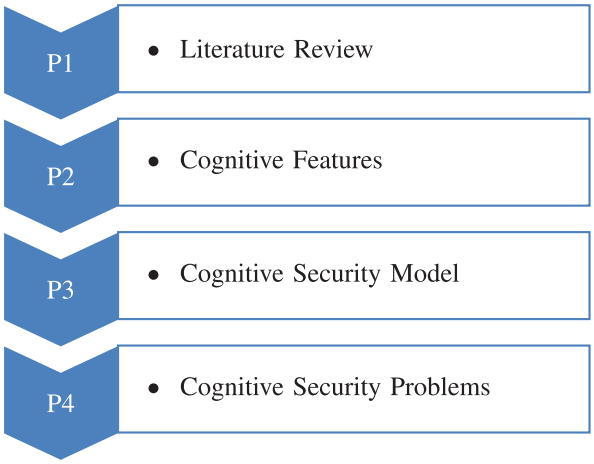

Fig. 3. Research approach for analyze the contribution of cognitive sciences.

used to establish the best decision for respond to attacks; if the incident has not been previously cataloged or if the knowledge base is limited, or if the specific tasks are not clearly defined, the solution will not be able for respond adequately.

This situation known as “narrowness" can produce unpredictable actions that can be dangerous in critical environments such as smart grids and nuclear plants. In the case of the data analysis components such as Big Data, if data quality is not considered, the security analyst could make decisions based on inaccurate information; this situation can cause unpredictable actions in the organization. Follow are the minimum characteristics that should ensure for a quality data:

- Consistency
- Accuracy
- Completeness
- Auditability
- Orderliness

Considering the importance of how Big Data and Artificial intelligence are integrated in the cognitive system, we propose to consider the CRISP-DM methodology to maintain an adequate data quality. This methodology also allows to establish a modeling process based on data analysis; It could be considered in the layers of pre-processing, processing and modeling of the cognitive model proposed in this work. Cognitive systems still lack a state of self-awareness, so they are not able to understand by themselves about positive or negative state of an event, so it is not advisable to implement in a 100% automation level. The components of a cognitive system can also be susceptible to attacks that can manipulate the data and induce negative decision making. The proposed cognitive security model considers the aforementioned weaknesses and includes control techniques such as MAPE-K, keeping the analyst as part of the model through of OODA and HITL, and proposal of a layered model that allows data quality analysis.

3. Research approach

For analyze the contribution of cognitive sciences in the field of cybersecurity, this study has developed four phases show in Fig. 3. In the first phase we present a literature review about of cybersecurity, then in the second phase we identify the main features that distinguish the contribution of cognitive science to cybersecurity strategies, then in the third phase we integrate the features by proposing a conceptual model of cognitive security and finally we discuss about problems that will face cognitive security.

4. Literature review

To maintain information security, organizations establish focal points for cybersecurity and defense operations known as Security Operations Centers (SOCs) or Security Incident Response Teams (CSIRTs). To deal with cybersecurity problems, the SOC or CSIRT establish daily operations or activities that are executed by security analysts. Most of them consist on:

1. Establishment of security situation awareness,
2. Identification of attacks or threats,
3. Security incident response,
4. Process of lessons learned.

According to MITRE [30], since 1990 several events have changed the way that SOC operates; among them:

- The growth of Advanced Persistent Threat (APT)
- The consolidation of IT and cloud-based computing.
- The growth of mobile technologies.
- The transition from attacks to the network towards attacks on the client side.

Different technological solutions are currently available for the protection and detection of security threats in cyber infrastructures. Nevertheless, humans are still the weakest link in the security chain. SOC or CSIRT must not only face the problems that arise from technology but also those related to people and processes. This is a research topic that has generated interest is the study of cognitive science to understand and enhanced the processes and cognitive tasks of security analyst. The integration of cognitive theories with methods and models applied in the field of cybersecurity can improve decision-making processes of the actors involved in cyberspace. The research methodology proposed in this work includes a literature review according to the operational activities of the SOC that allows us to understand the contribution of cognitive sciences in cyber-defense strategies. In Fig. 4, we show the topics considered in our literature review. We started by investigating the concepts of situation awareness in cybersecurity, followed by an analysis of attacks and threats arising from the use of emerging technologies that generate new challenges for security specialists, then a study on cognition in security operations, subsequently exploring cognitive activities or tasks to identify skills of cognition required by security analysts.

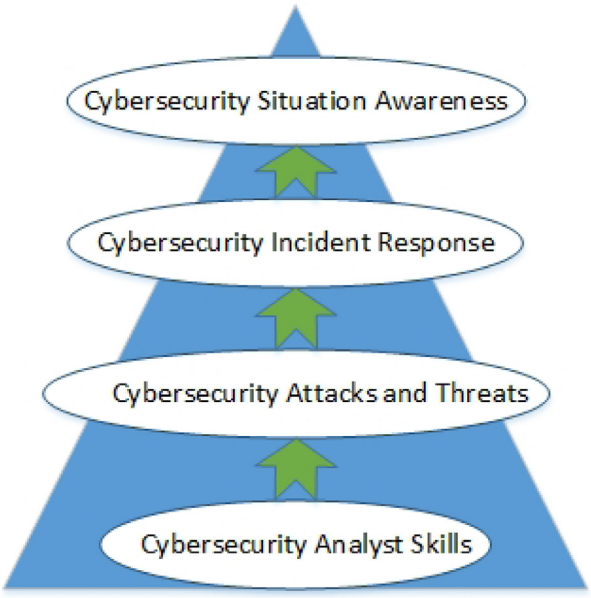

Fig. 4. Literature review cybersecurity topics.

Table 2
OODA cognitive phases.

Phase	Process	Products
Observe	Perceiving	Features
	Feature Matching	Structured Objects
Orient	Comprehending	Cause-Effect links
	Projecting	Mental Models
Decide	Recalling	Prototype Actions
	Evaluating	Pros & Cons

4.1. Cybersecurity situation awareness (CSA)

The concept of situation awareness (SA) describes the current situation of the organization about threats and attacks, the impact of a possible attack and the identification of the attacker and user behavior Timonen et a. (2015) [48]. All of these allow to project a state of the organization in the near future Scott [43]. The establishment of situation awareness is the main activity of the SOC. In the context of cybersecurity, situation awareness is defined in three levels by [47]:

1. Perception, generated by the information of the elements within cyberspace like firewall, SIEM or security news.
2. Comprehension, determines the current status of the situation based on the analysis of an attack depending on the level of threat or risk.
3. Projection, establishes a prediction of the types of vulnerabilities, threats or attacks.

The analyst must understand the security situation and determine the likelihood of impact. In the military field, the USAF pilots determined that a situation awareness can be established based on the four phases of the OODA loop proposed by Colonel John Boyd. The OODA proposal is based on the observation and understanding of the environment for the decision-making process. The OODA loop has two critical aspects: time constraint and information uncertainty, for which researchers have proposed variants, among which we can mention:

- Extended OODA loop
- Iterative OODA loop
- CECA model
- OODA loop adapted to Network Centric Warfare
- OODA loop adapted to Effect Based Operation
- Modular OODA loop
- Cognitive OODA loop

The cognitive OODA loop proposed by Breton and Rousseau (2018) [6] is based on the cognitive processes of perception, comprehension and projection. The Table 2 shows the relationships between cognitive phases, cognitive processes and products generated according to Brenton's proposal.

To establish the self-awareness capability of a computational system the following techniques can be used [26]:

1. Techniques based on feedback control,
2. Metric optimization with restrictions,
3. Techniques based on automatic learning,
4. Portfolio programming,
5. Reconfiguration of the self-conscious architecture, and
6. Stochastics performance models.

In 2001, IBM proposed a technique based on feedback control for computer systems known as MAPE-K [3]. Fig. 5 shows the five phases of MAPE-K: Monitoring, Analysis, Planning, Execution and Knowledge.

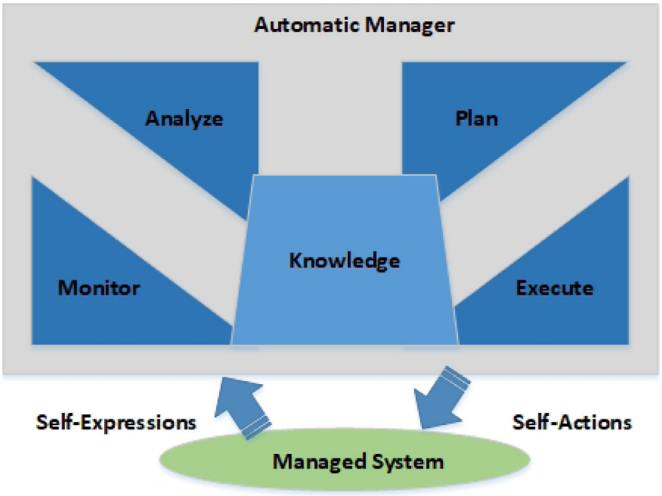

Fig. 5. MAPE-K [7].

Table 3
Cyber cognitive situation awareness.

Process	Attribute
Perception	Identification of relevant data
Comprehension	Interpretation of data Conversion in knowledge
Projection	Prediction futures events Evaluation possible impacts

4.1.1. Cyber-cognitive situation awareness (CCSA)

To establish the cybersecurity situation awareness of the organization we could rely on cognitive aspects oriented to the support of decision-making processes. Adapted to cyberspace the cognitive processes of perception, comprehension and projection, we would have the relationships shown in Table 3.

4.2. Cybersecurity attacks and threats

Security attacks can generate the failure of an electrical system, the collapse of a banking system, or problems in traffic control. Some attacks are caused by natural events, while others are supported by terrorist states or groups. MITRE [30] mentions that technological changes and variants of threats are factors that modify the form of operation of the SOC.

For this reason, we consider pertinent analyze the threats that arise from the use of technologies such as: IoT, cloud and Big Data. This analysis is the second fundamental activity of the SOC. In relation to IOT, Alaba [2] presents a survey of attacks and threats related to hardware, software or technologies used such as bluetooth, zigbee and rfid, while Zhou [53], mentions the challenges and new security threats in IOT. Mirza [31], presents different threats and attacks based on a study on IoT security in smart homes, medical devices and industrial applications. Yazan [52] presents a review of attacks and threats in Big Data and Amara [1] mentions attacks and threats in cloud infrastructure. In Tables 4–6, we present a compendium of attacks and threats security in Big Data, IoT, and cloud, based on the review made from scientific databases; business reports of technology and security made by CISCO, IBM, Kaspersky, Symantec, CheckPoint; international organizations such as: NIST, NSA, SANS and; reports from consulting companies such as: Gartner and Forbes. In the information presented in the tables a threat can be associated with different attacks, there is not a direct threat attack relationship presented.

Table 4
Cybersecurity IoT attacks and threats.

Technology	Attacks	Threats
IoT	Eavesdropping	Tracking
	Counterfeiting	Flooding
	Key exchange	Rogue access points
	Scapy	Manipulation of data
	KillerBee	Misconfiguration
	Car Whisperer	Insider misuse
	Bluebugging	Unintentional action
	Jamming	Packet manipulation
	Tampering	Lack system defense
	Collisions	IoT botnets
	Man in the middle	privacy leak
	Imitation	Remote attack
	Blocking	Privacy leak
	Routing diversion	Trespass Falsification

Table 5
Cybersecurity cloud attacks and threats.

Technology	Attacks	Threats
Cloud	XDOS	Xmltags
	HDOS	Http Flooder
	DNS Attacks	Meltdown
	XSS Attacks	Specter
	Wrapping	Insecure APIs
	Cookie Poisoning	Abusive Use
	Hypervisor Attacks	Unknown Profile
	Data Loss	Insufficient Compliance
		Data breaches

Table 6
Cybersecurity cloud attacks and threats.

Technology	Attacks	Threats
Big data	Data lake	Unauthorized data access
	Spamming	Re-identification
	Spoofing	Privacy threats
	Data mining attacks	Flooding
	Phishing	Data breaches

4.3. Cybersecurity incident response

The third operational activity of SOC considers to establish processes of security incidents response that allow to maintain an adequate state of security in the organization facing attacks. To carry out this activity security specialist must analyze large amounts of logs, in order to determine possible anomalies that allow detecting threats and attacks that may negatively affect the organization. Solutions such as SIEM correlates logs and events, which facilitates this activity for analysts. Another alternative is the use of statistical techniques or data mining to determine patterns of attacks or threats, which are not easily detected. However, although the advances in technology allow the automation of responses, actions are not always implemented due to the impact that a normal temporal event could cause being classified as false alert and thus generating the interruption of valid connections. The complexity and size of the networks and the dynamic nature of the behavior of the attackers can generate a high rate of false positives. According to [39], around 20,000 hours are used to test false alarms, in this sense the need for the decision criterion based on experiences and believes of the human is needed within the process of automation (Human in the loop).

4.3.1. Incident management process

The incident management process establishes a set of phases that allow to determine the mechanisms to detect a security incident and to define a recovery action to maintain an adequate state

Table 7
Incident response references.

Organization	Topics	Year
CERT	Organizational model Incident handling process CSIRT services	2003
ENISA	Incidents handling phase Roles Polices Workflows	2010
SANS	Incident handling process	2011
ISO	Guidelines incident response	2011
NIST	Incidents handling phase	2012

of cybersecurity in case of a negative impact due to attacks. NIST (2012) establishes a set of four phases:

1. Preparation,
2. Detection and analysis,
3. Containment, eradication and recovery, and
4. Post-incident activity

The process of handling incidents has been addressed by several organizations, in Table 7, we present a consolidated list of the organizations and guidelines proposed.

4.3.2. Automated Incident response

The operational activities of an incident response process are generally long, tedious and require of cognitive skills from cybersecurity analysts. Human limitations to process large amounts of data and factors that affect the human cognition like stress and emotions, can reduce security incident response accuracy and effective. Some alternatives to support the process of incident response through the automation of tasks could solved this limitation. In the Diagram 1 we present a consolidation of the security incident response automation strategies.

***Dynamic models*:** The limitation of the static models in security incidents response is that are based on a set of possible responses predefined by the security analyst, so if there is a variation of the attack, the model cannot predict a possible response action. Then, the main advantage of dynamic models is their adaptability to change in the digital environment.

***Cognitive map models*:** The cognitive map is based on the creation of valence matrices according to a consensus of the security team, depending on the different alternatives analyzed regarding on how to solve an incident [20]. The steps established in the proposal include:

- Generate attack scenarios.
- Build probabilistic incident response options to generate cognitive maps.
- Select the most appropriate answer.

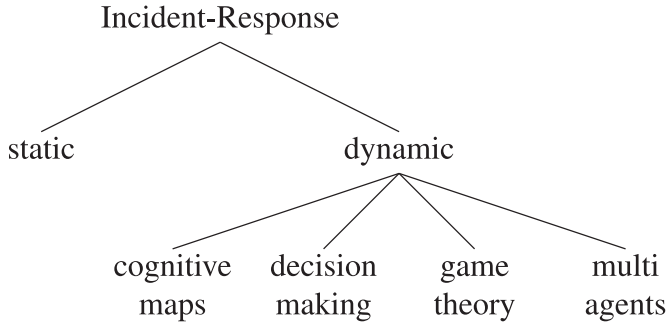

Diagram 1. Automated incident response models.

***Decision-making models*:** The model of decision making is based on an axiom that validates a condition and based on its accomplishment, an action is executed. The selection of the condition to be evaluated can be based on different criteria, some proposed decision-making models are:

- Fuzzy decision making and risk assessment [5].
- Ontologies-based [24].
- Planning the hierarchical task network [9].
- Tolerance to risk impact [44].
- Cost of attack damage [45].
- Markov decision [16].

***Game theory model*:** The use of game theory is based on establishing two attacks and defense roles to predict possible sequences of attacks that can be executed. For the implementation of game theory, the proposals are based on:

- Nash in equilibrium strategies [54].
- Stochastic models [23].
- Bayesian learning [28].

***Multi-agent models*:** The multi-agent system (MAS) executes tasks to solve problems related to the handling of incidents. The objective of the multiple agents is to provide an autonomous and decentralized architecture that is based on the following activities [25]:

- Identification and registration.
- Categorization and prioritization.
- Diagnosis and scaling.
- Resolution and recovery of items.
- Closure of incident.

The proposal defines different roles of the agents:

- User agent: is the user of the system who can see the details of the incident.
- Administrator agent: is responsible for the administration of the system.
- Supervisor agent: is responsible for monitoring IT services to detect possible anomalies or problems.
- Incident agent: is responsible for handling the incident. Its tasks consist of: storing incident information, validating similar incidents in the incident database, notifying in case of finding the solution; and notify if the incident is new for the related information
- Diagnostic agent: responsible for evaluating the impact of the incident based on the Service Level Agreement (SLA).
- Support agent: works in coordination with the incident agent when there is no solution and has information grouped by hardware, software or network.

4.3.3. Cybersecurity analyst skills

The security analyst integrates experience and practical knowledge to evaluate and interpret the observations, in order to generate hypothesis about the events that can be possible attacks. For this, it is required to process multiple sources of data and information and to establish a correlation between them and the digital environment. A security analyst should be responsible for the following activities:

- Monitor the network.
- Identify threats.
- Fix vulnerabilities.

To execute these activities, the analyst performs the following cognitive processes:

- Identification,

Table 8
Cognition in cybersecurity layers.

Layer	Cognition-Attribute
Attacks & threats	Cognitive Hacking
Cyber Operations	Cognitive Techniques
Incident Response	Cognitive Tasks
Analyst Skills	Cognitive Skills
Cyber Strategic	Cognitive Situation Awareness

- Observation,
- Generation of hypothesis,
- Research of hypothesis.

At the RSA (2017) conference in 2017, IBM [40] presented the cognitive tasks that a security analyst must perform in the investigation of one security incident, shown below:

1. Identification
   - TC-1. Review incident data.
   - TC-2. Review the events by aspects of interest.
2. Observation
   - TC-3. Pivot in the data to find atypical values or outliers.
   - TC-4. Expand the search to find more data.
3. Generation of hypothesis.
   - TC-5. Investigate the threat to develop experience.
   - TC-6. Discover new threats.
   - TC-7. Determine indicators of commitment in other sources.
4. Research of hypothesis.
   - TC-8. Apply intelligence to investigate the incident.
   - TC-9. Discover IPs potentially infected.
   - TC-10. Qualify the incident based on the knowledge generated depending on the investigation of the threat.
   - TC-11. Prescriptive analysis in base of attack profile.
   - TC-12. Analysis of lessons learned based on the dispersion map of the attack.

The cognitive abilities required by the security analyst to perform cognitive tasks include:

- Thinking strategies
- Troubleshooting
- Inventive thinking
- Decision making.
- Learning.

To enhanced the cognitive abilities of the analyst, there are several alternatives:

- Hands-on practice.
- Experience with tools.
- Simulation environments.
- Workflows based on situation awareness.

The digital age and the sophistication of threats and attacks have increased in severity and occurrence generates millions of data that require a high processing capacity. At the different levels of cybersecurity, the role of the human is an important factor, which cannot be minimized only through the implementation of automation solutions, but also require to enhanced the cognitive abilities of the security analyst. In Fig. 6, we present a consolidation of the components of cognitive security based on our literature review.

From our analysis we consider that cognitive attributes should be transversal to cybersecurity layers related to the detection of attacks and threats, cybersecurity operations, handling of incident response and the decision making from a strategic vision to improve the security of the organization. In Table 8, we present the application of cognition in the different layers of security proposed in this work.

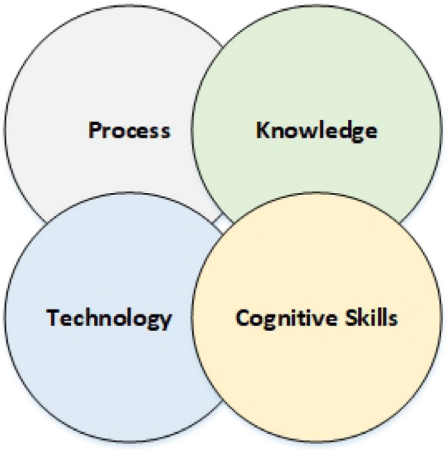

Fig. 6. Cognitive security components.

5. Cognitive features

The proposed cognitive security model considers the different roles: attackers, defenders and users, in the following way:

***Attacker*:** The security analyst evaluates the cognitive or behavioral aspects of the attacker i.e. their motivations, types and patterns of attacks to get competitive advantage. According to Sample [42], the modeling of attacks can be complex due to cultural characteristics, preferences of the attackers and geographical location. The proposed cognitive model considers the use of big data, machine learning and natural language processing to make geographic referencing, analysis of the attacker's feelings, and detect attack patterns for establish an attacker's profile. Regarding the motivations of attackers, Meyers [29] establishes a classification of adversaries which is shown in Table 9.

Regarding the type of attacks, Simmons [46] proposes the characterization of the nature of an attack based on five major classifiers: attack vector, operational impact, attack target, defense, and informational impact. The characterization of the attackers is based on two characteristics: Risk-adverseness and Experience level, proposal by Venkatesan [50].

The modeling of the attackers should consider at least the following aspects:

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

***User*:** The proposed model considers the cognitive and behavioral aspects of the user. The work proposed by Sample [42] mentions that victims of attacks have associated cultural aspects; and social engineering attacks/cognitive hacks are based on these char-

Table 9
Adversary class according attacker's motivation.

Adversary Class	Motivations
Script kiddies	Curiosity
Hacktivist	Defacement for political reasons
Cyber punks	Engage in malicious attacks
Insiders	Disgruntled employees
Coders	Write automated tools
White hackers	Test new programs
Black hackers	Organized crime
Cyber terrorists	Against enemy nations

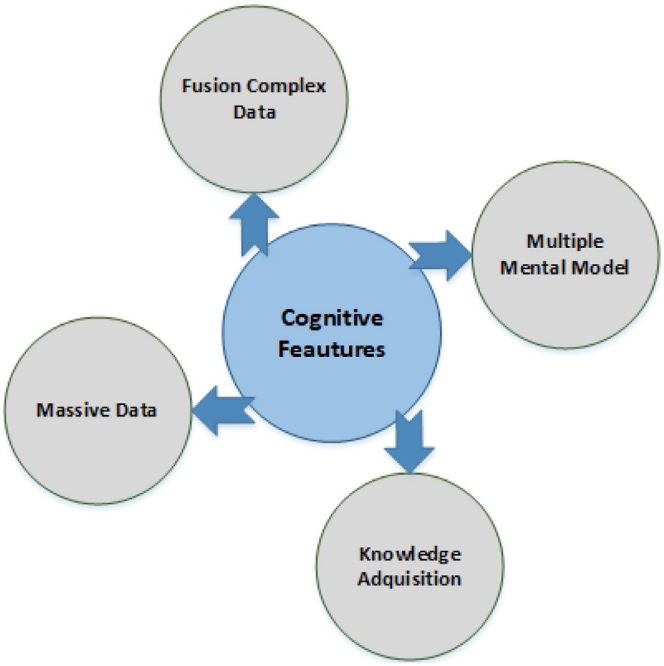

Fig. 7. Relations of cognition with data and knowledge.

acteristics. Therefore, it is important that the analyst could determine patterns that allow them detect that a user is victim of an attack or not. The work presented by Gratian [14] shows how personal factors such as age, gender, extraversion, neuroticism and openness can influence cybersecurity behaviors. The modeling of user behavior could consider at least the following aspects:

- Normal traffic schedules,
- Recurring applications,
- Devices,
- Networks,
- Geo-referencing.

For the modeling of behavior of users and attackers, the system could consider the cultural framework proposal by Hofstede [15] that indicates six dimensions:

- Power Distance Index (pdi),
- Individualism versus Collectivism (ivc),
- Masculine versus Feminine (mvf),
- Uncertainty Avoidance (uai),
- Long-term orientation versus Short-term orientation (lvs),
- Indulgence versus Restraint (ivr).

***Security Analyst*:** The proposed cognitive security model considers the security analyst as the central axis and base their effectiveness on the automation of cybersecurity cognitive tasks. Based on our literature review, we present in Fig. 7, the elements that generates the cognitive features for the processes, tasks and skills of security analyst which are identified previously in the Table 8.

According to the OODA model, four phases are established:

- Observation, refers to the data collection process
- Orientation, the fusion of information to build situation awareness
- Decision, process of establishing a final decision based on the analysis of all the hypotheses.
- Action, defines the process of analytical reasoning.

In the Fig. 8, we present the three-phase workflow to establish a cybersecurity situation awareness that security analyst can develops based on the cognitive tasks (D'Amico, 2005) [11].

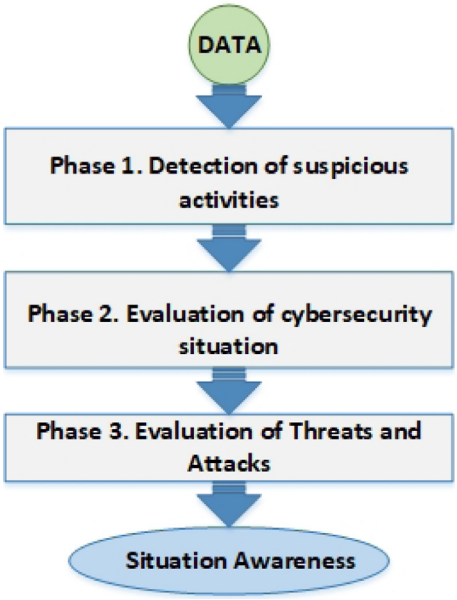

Fig. 8. Relations of cognition with data and knowledge.

1. Detection, the analyst inspects and associates data to detect suspicious activities. Convert data into information.
2. Situation evaluation, the analyst extracts characteristics of the data to establish a state of organizational security. Convert information into knowledge.
3. Evaluation of threats, the analyst correlates the threats to identify the enemy's identity, motivation and support. Convert the information into knowledge and prediction.

For the generation of knowledge, the analyst can use different sources of information:

- Threat database
- Security reports
- Vulnerability reports
- Security websites
- Security events
- User activity
- Information configuration
- Vulnerability results
- System and application logs

Association between cognitive tasks and the cognitive processes according to the OODA model, adapted to cybersecurity operations is show in the Table 10.

Table 10
Cognitive tasks and process in cyber-sec operations.

Cognitive tasks	Cognitive Process
TC-1.	Perception
TC-2.	Perception
TC-3.	Comprehension
TC-4.	Projection
TC-5.	Comprehension
TC-6.	Projection
TC-7.	Comprehension
TC-8.	Projection
TC-9.	Comprehension
TC-10.	Comprehension
TC-11.	Comprehension
TC-12.	Comprehension

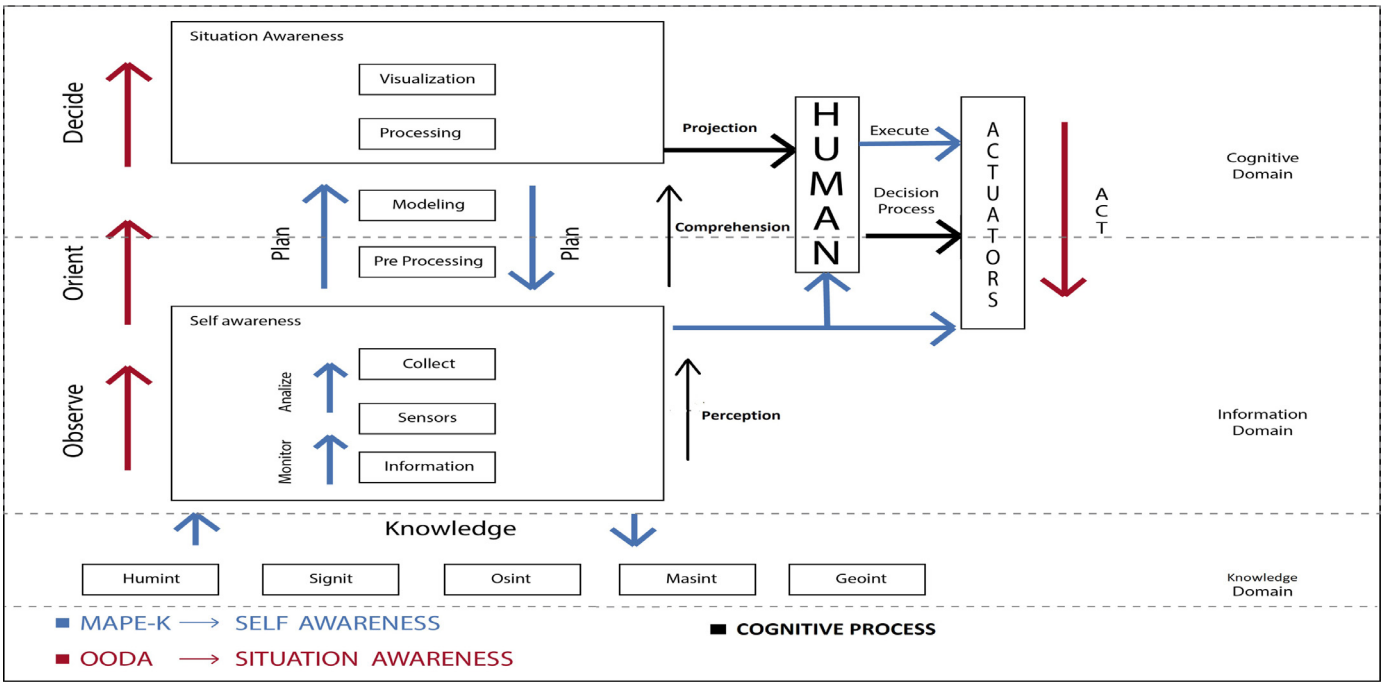

Fig. 9. Cognitive security model extended.

6. Cognitive security model

Cybersecurity situation awareness allows to organizations establish their current state related with cybersecurity such as: risks, vulnerabilities, attacks and gaps, based on this knowledge the organizations can projects the condition of their state in the near future. There are two possible levels of cybersecurity situation awareness [38], the low level where raw data is processed and is most common to find technological solutions that allow its automation; the high level that allows to establish strategic decisions based on information abstraction processes; high levels of situation awareness are performed usually by humans manually, this is work-intensive, time-consuming, and error-prone. Technological solutions in the field of cybersecurity that could enhanced the cognitive abilities of the security analyst for establish proactive security strategies are distributed in different fields: Visualization for cybersecurity, Artificial intelligence in cybersecurity or big data in cybersecurity. Our objective in this work is to present a cognitive model that integrates the different contributions of cognition at the different levels of cybersecurity for aids to security analyst to establish cybersecurity situation awareness.

The proposal security cognitive model is show in the Fig. 9, and we denominated NOTAS-MH by the inclusion of the following methodologies and components: Newstrom, OODA, Technologies, Acquisition, Situation Awareness, MAPE-K and Human in the loop. The proposal model defines three layers: Knowledge, Information and Cognitive, and it tries support the process of modeling of mental maps, the generation of knowledge, the fusion of data and the handling of massive data related with cybersecurity events. The final objective of the proposed model is can determine a level of cybersecurity situation awareness and the tasks automation development by the security analyst. The analyst can use different sources of information for generate knowledge related with each task and then define the automation process and establish security defense strategies.

The generation of this knowledge and execution of tasks require of methodological, repeatable, measurable and formal process. In the field of cybersecurity, collaborative work is important, for this

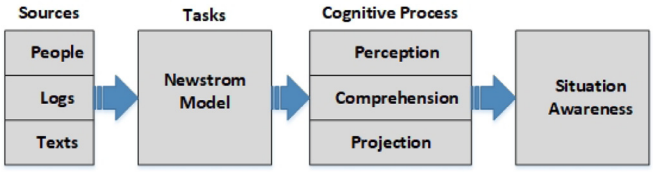

Fig. 10. Cognitive tasks and process for cybersecurity awareness.

reason we consider the model proposal by Newstrom and Davis [36] for establish the organizational structure of the execution of the tasks and subsequently can measure their effectiveness. The security analyst to establish the cybersecurity situational awareness will follow the stages shown in the Fig. 10, in which the sources of information, the organization of tasks and the execution of cognitive processes are related. The knowledge domain of security cognitive model considers the different source of information to establish a situation awareness (Scott, 2017):

1. HUMINT, is generated by humans from interviews, conversations or forums.
2. SIGINT, is produced by the interception of signals generated by computer equipment, network equipment or telecommunications equipment.
3. OSINT, is derived from open sources and include news, social media and commercial databases. It also considers technical information from platforms such as WHOIS.
4. MASINT, is produced by data obtained from sensing instruments. Sensors may be used tactically or strategically for generate this kind of information.
5. GEOINT, is produced from geo-spatial systems and can be derived entirely of any satellite or aerial imagery.

The amount of information may exceed the analysis capabilities of security specialists, for which the use of Recommendation Systems (RS) or expert Decision Support Systems (DSS) can support the decision-making processes. To analyze large amounts of information we propose the use of different technological solutions such as: Sensors, big data and Machine learning; in the work

Table 11
Layers of cybersecurity cognitive model.

Domain	Layer	Application Field	Approach
Knowledge	Knowledge	Cyber Operations	Humint, Osint, Geoint, Sigint, Masint
Information	Information	Systems information	Organization information theory
Information	Sensor	Autonomic computing	Self-healing Self protecting
Information	Collect	Big Data	ELK
			Spark
			Hadoop
		Data Mining	ANN
			Association rules
			Clustering
			Decision Tree
		Machine Learning	HMM
			SVM
			Naive Bayes
			Inductive Learning
Cognitive	Pre-processing	Self-Awareness	MAPE-K
		Situation Awareness	OODA
Cognitive	Modeling	Threat model	Cognitive maps
		Attack model	Game theory
		Planning model	Fuzzing
		Risk model Impact model	Ontologies
Cognitive	Processing	Decision Support System	Intelligence driven
			Data driven
		Recommender System	User driven Goal driven
Cognitive	Visualization	Security Visualization	Geo-maps
			Traffic flow
		Big Data Analytics	Time series
			Correlation graphs
			Forensic events
Cognitive	Human	Human in the loop	Human computer interaction Natural processing language
			Learning models
			Mental models
			User Behavior Analytic

"Management of information security indicators under a cognitive security model" [4] we present a model that is composed of seven layers that integrate the different technological solutions that could enhance the cognitive skills of the security analyst.

1. Information Source Layer: This layer considers the different data sources generated by equipment servers, networking equipment, perimeter security equipment and user devices.
2. Sensor Layer: This layer establishes the homogenization of security sensors communications distributed among multiple locations.
3. Collect Layer: In this layer data management process is done. The data management process includes: Data validation, Data cleansing, Outlier removal, Data conversion and Data aggregation and; data partition.
4. Pre-processing Layer: In this layer patterns of anomalous behavior are established on the basis of which the existence of possible attacks can be determined. The patterns are established based on the correlation of network traffic data, user behavior, established connections, and network addresses used.
5. Modeling Layer: In this layer it is necessary to carry out the modeling of the information gathered, to describe the data flows and to establish the most common types of interaction that exist inside the network.
6. Processing Layer: This layer also uses machine learning solutions with the aim of analyzing the anomalous behavior or parameters in visualization layer. In this layer the visualization of the information generated by the processing layer is presented as sources that are neither corrupted nor manipulated
7. Decision Layer: In this layer the visualization of the information generated by the processing layer is presented. Recommender systems or Decision Support Systems can be used.

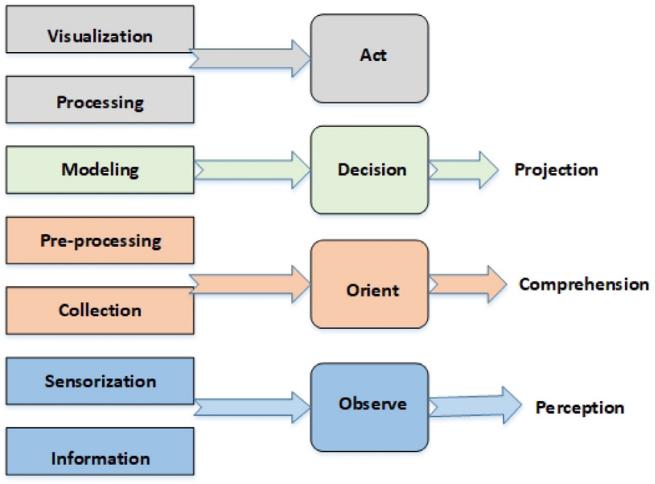

Fig. 11. Relations between technologies and cognitive process.

We present in Table 11, the relationships between technological solutions that could enhanced cognitive processes of security analysts, and the fields of study that could contribute to the application of the cognitive security model proposed.

Using the OODA loop determines patterns that are identified through the analysis of the data for generating mental models in base of profiles of attacks, threats, behavior of users and attackers that allow to establish the situation awareness of the organization, and define the projecting actions to maintain the cybersecurity state. OODA shares the knowledge to the security analyst through the recommendation systems or decision support systems. The Fig. 11 shows the relations between each of the technological

layers and each one of the cognitive processes of the security analyst.

Continuous monitoring of cybersecurity state is based on the application of *MAPE-K*; the control variable is the state of cybersecurity situation awareness in the modeling layer. The data intake in the data sources in the information, sensorization and collecting layers then pass to pre-processing and modeling layers for analyze it; according to cybersecurity indicator pre-establish some specific actions are executed.

The proposal of the cognitive model considers the inclusion of the human model in the loop (HITL) to solve the human interaction with the technological solutions of the different layers, this approach allows to create machine understanding models for the training and automation of the solutions of artificial intelligence and autonomic computing that allow to generate knowledge and enhanced the cognitive abilities of the security analyst. The HITL allows to control the generation of false alerts by controlling the indicators of commitment. HITL also executes the control of the actuators who are in charge of executing automated incident response actions to avoid actions that could negatively affect the computer systems, especially when they are the product of false alerts.

7. Cognitive security problems

The first problem or challenge that cognitive security faces are that for the predictive analysis the data sources have not been manipulated or corrupted, for which it is necessary to establish data quality processes and security mechanisms that avoid the alteration of the data sources. If an attacker altered the data, it could lead to data mining, machine learning or Big Data solutions to generate erroneous analyzes that could induce the analyst to make an incorrect decision.

A second problem is the limitation of cognitive solutions to get the ability of the human to establish a common sense to handle dilemmas or show compassion. MIT developed a project called Moral Machine that establishes the dilemmas that cognitive solutions can face in automated systems [33].

Finally, a third problem is that cognitive solutions still lack the capacity for generalization and abstraction that allow humans solve problems and analyze the possible impact of decisions made. Based on this criterion, not every process is automatizable due to the risk of the existence of false positives. In case of full automation, a false positive can cause the complete shutdown of a critical system which is why it is necessary to maintain models such as human in the loop.

8. Conclusions and future work

Awareness is a concept widely defined in the field of psychology and several researchers have analyzed how to translate its principles into the field of cybersecurity. To achieve this sense of awareness in cybersecurity is necessary to evaluate the parameters of itself (self-awareness) and its environment (situation awareness) based on security indicators that allow us to understand the current state of cybersecurity and project security risks, possible attacks, actions to be executed and the possible impacts of executing a certain action in a future time.

The use of cognitive sciences in the field of cybersecurity allows us to address the contributions of psychology, artificial intelligence, linguistics and human computer interaction to improve the cognitive processes of security analysts in order to improve times of response and effectiveness in decisions about actions to detect, contain or mitigate a security attack. Cognitive security considers four components: processes, knowledge, technology and cognitive abilities, to establish mental maps, complex data fusion, the handling of massive data and the maintenance of knowledge.

To manage the security operations in the SOC or CSIRT they must focus on four macro processes: Cybersecurity situation awareness, Cybersecurity attacks and threats, Cybersecurity incident response and skills of security analysts. The generation of a cognition in situation awareness can be achieved based on the application of the three cognitive processes: perception, comprehension and projection. For this process, we identify relevant data, then data is interpreted and correlated and then future events are evaluated and predicted.

We should consider that not every task or process is automatized because the impact of executing an action may affect more negatively than the security attack. For this aspect, it is important to keep the human at the center of decision making for the execution of cybersecurity actions or tasks.

To establish a continuous monitoring about the information from different sources that allow the generation of cognition and decision-making process, is necessary use control techniques. In the field of computer science and cybersecurity some proposals have been applied such as MAPE-K, OODA and Human in the loop. The security cognitive model proposal in this work integrates technological solutions with cognitive process and control techniques that allows to provide a complete vision of the cybersecurity situation awareness.

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Amara N, Zhiqui H, Ali A. Cloud computing security threats and attacks with their mitigation techniques. International conference on cyber-enabled distributed computing and knowledge discovery (CyberC); 2017. doi:10.1109/cyberc.2017.37.
[2] Alaba F, Othman M, Hashem I, Alotaibi F. Internet of things security: a survey. J Network Comput Appl 2017;88:10–28. doi:10.1016/j.jnca.2017.04.002.
[3] Amoud, M., and Roudies, O. MAPE-K-based approach for security @ runtime, 2016. pp. 138–140, doi:10.1109/SWSTE.2016.28.
[4] Andrade R, Torres J, Flores P. Management of information security indicators under a cognitive security model. In: 2018 IEEE 8th annual computing and communication workshop and conference (CCWC); 2018. p. 478–83. doi:10.1109/CCWC.2018.8301745.
[5] Berenjian S, Shajari M, Farshid N, Hatamian M. Intelligent automated intrusion response system based on fuzzy decision making and risk assessment. In: IN:2016 IEEE 8th international conference on intelligent systems (IS); 2016. p. 709–14. doi:10.1109/IS.2016.7737389.
[6] Breton R, Rousseau R. THE C-OODA: a Cognitive Version of the OODA loop to represent C2 activities. Topic 2018.
[7] Brun Y, Desmarais R, Geihs K, Litoiu M, Lopes A, Shaw M, Smit M. A design space for self-adaptive systems. In: Software engineering for self-adaptive systems II: international seminar. Dagstuhl Castle, Germany: Springer Berlin Heidelberg; 2010. p. 33–50. October 24-29. doi:10.1007/978-3-642-35813-5-2.
[8] Camara J. and Kounev S. and Kephart J. and Milenkoski A. and Zhu X. Self-aware computing systems: related concepts and research areas, 2017, doi:10.1007/978.3.319.47474.8.2.
[9] Chengpo M, Yingjiu L. An intrusion response decision-making model based on hierarchical task network planning. J Expert Syst Appl 2010;37(3):2465–72.
[10] Cisco., 2018. Cisco internet of everything. https://www.cisco.com.
[11] D'Amico A, Whitley K, Tesone D, O'Brien B, Roth E. Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts. Proceedings of the human factors and ergonomics society annual meeting 2005;49:229–33 doi:10.1177/154193120504900304.
[12] Forbes., 2017. Press Releases. https://www.forbes.com.
[13] Gartner., 2017. Press Releases. https://www.gartner.com.
[14] Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A. Correlating human traits and cyber security behavior intentions. Comput Secur 2018;73:345–58. doi:10.1016/j.cose.2017.11.015.
[15] Hofstede G. Attitudes, values and organizational culture: disentangling the concepts. Org Stud 1998;19(3):477–93.
[16] Iannucci S, Abdelwahed S. Model-based response planning strategies for autonomic intrusion protection. ACM Trans Auton Adapt Syst 2018;13(1):1–23.
[17] IEEE., 2016. Smart cities, big data, and the internet of things. https://www.standardsuniversity.org

[18] ITU., 2016. Connect 2020 Agenda. https://www.itu.int.
[19] Killcrece G, Kossakowski, K.-P., Ruefle, R., and Zajicek., 2003. State of the practice of computer security incident response teams. https://resources.sei.cmu.edu/library/.
[20] Krichene J, Boudriga N. Incident response probabilistic cognitive maps. In: 2008 IEEE international symposium on parallel and distributed processing with applications; 2008. p. 689–94. doi:10.1109/ISPA.2008.33.
[21] Krylovskiy, A. Jahn, M. and Patti, E. Designing a smart city internet of things platform with microservice architecture. In: Proceedings of the 2015 3rd international conference on future internet of things and cloud. 2015 doi:10.1109/FiCloud.2015.55.
[22] Kounev S, Zhu X, Kephart J, Marta Z Kwiatkowska. Model-driven algorithms and architectures for Self-aware computing systems. In: Dagstuhl Seminar 2015;5:164–96 DOI: 10.1109/FiCloud.2015.55.
[23] Kundu A, Ghosh SK. Game theoretic attack response framework for enterprise networks. In: Distributed computing and internet technology; 2014. p. 263–74.
[24] Lanchas V, Gonzalez VV, Bueno F. Ontologies-based automated intrusion response system. In: Computational intelligence in security for information systems, 2010; 2010. p. 99–106.
[25] Latrache A, Nfaoui H, Boumhidi J. Multi agent based incident management system according to ITIL. In: 2015 intelligent systems and computer vision (ISCV; 2015. p. 1–7. doi:10.1109/ISACV.2015.7105552.
[26] Lewis P, Chandra A, Parsons S, Robinson E, Glette K, Bahsoon R, Torresen J, Yao X. A survey of self-awareness and its application in computing systems. In: Fifth IEEE conference on self-adaptive and self-organizing systems workshops; 2011. p. 102–7. doi:10.1109/SASOW.2011.25.
[27] Lewis, P.R. and Chandra, A. and Parsons. Self-awareness and self-expression: inspiration from psychology. In: Self-awareness computing systems. Natural computing series. Springer, Cham 2016 doi:10.1007/978.3.319.39675.0.2.
[28] Luo Y, Szidarovszky F, Al-Nashif Y, Hariri S. A fictitious play-based response strategy for multistage intrusion defense systems. J Secur Commun Network 2014;7(3):473–91.
[29] Meyers, A. and Powers, S. and Faissol, D., 2009, Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches, 2016, doi = 10.2172/967712.
[30] MITRE.: MITRE Security Vulnerabilitys. https://www.mitre.org.
[31] Mirza A, Muhammad A, Sajid H, Saleem U. Security issues in the internet of things (IoT): a comprehensive study. Int J Adv Comput Sci Appl 2017;8(6).
[32] MIT. Cognitive science. MIT Department of Brain and Cognitive Sciences; 2018 https://bcs.mit.edu/research/cognitive-science.
[33] MIT. Moral machine. Massachusetts Institute of Technology; 2018 http://moralmachine.mit.edu.
[34] Mosenia A, Jha N. J IEEE Trans Emerg Top Comput 2017;2017:586–602. doi:10.1109/TETC.2016.2606384.
[35] Statista., 2017. Press Releases. https://www.statista.com.-
[36] Newstrom, J. W. and Davis, K., 2019., Comportamiento humano en el trabajo NIST.:computer security incident handling guide. https://csrc.nist.gov/publications.
[37] Nugraha A, Legowo N. Implementation of incident management for data services using ITIL V3 in telecommunication operator company. In: 2017 international conference on applied computer and communication technologies (ComCom); 2017. p. 1–6. doi:10.1109/COMCOM.2017.8167093.
[38] Pino R, Kott A, Shevenell M. Cybersecur Syst Hum Cognit Augment 2014. doi:10.1007/978-3-31910374-7.
[39] Ponemon Institute. Eliminating cyber security false positives within the SOC. 2017. https://www.ponemon.org.
[40] IBM.: Applied cognitive security complementing the security analyst. https://www.rsaconference.com.
[41] Santana E, Chaves A, Gerosa M, Kon F, Milojicic D. Software platforms for smart cities: concepts, requirements, challenges, and a unified reference architecture. ACM Comput Surv 2017;50:1–37. doi:10.1145/3124391.
[42] Sample, C. and Hutchinson, S. and Maple, C. and Karmanian, A. (2018). Cultural observations on social engineering victims.
[43] Scott J, Rebekah B. Intelligence driven incident response. O Reilly books; 2017.
[44] Shameli-Sendi A, Dagenais M. ARITO: vyber-attack response system using accurate risk impact tolerance. Int J Inf Secur 2014;13(4):367–90.
[45] Shameli-Sendi, Louafi H, Cheriet M. Dynamic optimal countermeasure selection for intrusion response system. IEEE Trans Dep Sec Comp 2018;15(5):755–70.
[46] Simmons, C.B., S.G. Shiva, H.S. Bedi and D. Dasgupta. AVOIDIT: a cyber attack taxonomy. (2014).
[47] Thomas W, Manz D. Research methods for cybersecurity. Elsevier; 2017.
[48] Timonen J. Improving situational awareness of cyber physical systems based on operator's goals. In: 2015 international conference on cyber situational awareness, data analytics and assessment (CyberSA); 2015. p. 1–6. doi:10.1109/CyberSA.2015.7166121.
[49] United Nations., 2016. Sustainable Developments Goals, 2016 http://www.undp.org/content.
[50] Venkatesan S, Sugrim S, Izmailov R, Chiang CYJ, Chadha R, Doshi B, Buchler N. On detecting manifestation of adversary characteristics. MILCOM 2018 - 2018 IEEE military communications conference (MILCOM); 2018. doi:10.1109/milcom.2018.8599754.
[51] Wiik Johannes, 2005, Limits to effectiveness in computer security incident response teams. https://resources.sei.cmu.edu/library.
[52] Yazan A, Yong W, Raj K. Big data lifecycle: threats and security model. Journal 21st Americas conference on information systems, In: emerging issues in information security; 2015.
[53] Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Int Things J 2018;6(2):1606–16. doi:10.1109/JIOT.2018.2847733.
[54] Zonouz S, Khurana H, Sanders W, Yardley T. RRE: a game-theoretic intrusion response and recovery engine. J IEEE Trans Parallel Distrib Syst 2014;25(2):395–406.