17th International Conference on Space Operations, Dubai, United Arab Emirates, 6 - 10 March 2023.

SpaceOps-2023, ID # 123

THE COGNITIVE OPERATIONS IN SPACE : MANAGE THE BRAINS IN THE NEW DATA CONTEXT

Djamel Metmati

[a] *Department of Cyber, Thales*, djamel.metmati@thalesgroup.com

Abstract

The New Space denes itself by an extension of the actors and the technologies applied in Space. The consequences of New Space mean the increasing of data available for any topics about the Space operations. In regard of the Space industry development through the services delivered to the ground and towards the Deep Space, the operational data needs a method to be correctly collected, organized, and interpreted by the machines and the interface with human. The cybersecurity offers the way to secure the data networks. Nevertheless, the integrity of data shall be checked to secure and protect the brain. Indeed, its construction doesn't come for Space environment, even if it owns an ability to adapt on it. The cognitive cybersecurity provides the toolbox to design a correct representation of data for any kinds of maneuver in Space or from the ground to the Space. As data is the key control, the understanding of cognitive bias from the brain secures the mission process. Moreover, the brain is faced with the machines errors. The training from data model corrects them through the simulation. Despite of that, the brain undergo the effects of the predictive model in which the no-comprehensive and intelligible data can produce both the wrong decision making, the unexpected maneuvers and the observation errors.

Keywords: cognitive, cybersecurity, data, networks

1-Introduction

The objectives of this work is to demonstrate from the cybersecurity cognitive requirements the key parameters to manage Space operations according the conditions of New Space.

2-Method

The method holds on the neural framework with the counter-intuitive inputs. These inputs come from the quantum technology applied to the way to understand the reality at the moment where the brains undergo the huge data flow.

3-Results

3.1 Mitigate the predictive model from neural framework

The exchange machine to machine and the intelligence artificial techniques use the flow processing from the datasets. The quality of the intelligence artificial depends on the way of the data structure. Then, the data engineering produces the predictive models which display on the screen to support any operational action, to give the inputs of the system status. It means that the vulnerabilities of the predictive models exist at the moment where they use the biais of the brain to orient the click action or to confirm the biais between the human and the machine. It exists also for the exchange machine to machine for the datasets could be corrupted in the processing. To mitigate the predictive model by data poisoning, the intelligence artificial algorithm shall use the human cognition parameters in the data building for the predictive model and for the displaying the key element on a screen. The purpose is to be closer of the reality and understand what it really happens. The tools to apply this methodology is neural framework once the datasets is ready and cleaned from the sources don't connect with the process measured.

The neural framework [5] is the last step before the datas are recorded in the database for requests from the network. To be useful, the conditions of neural framework shall be taken account by identifying the targets of the data, the sources of the data, the digital humanities context, the geometric structure of the networks and the potential biais that the framework provide to mitigate the vulnerabilities of datas expression. Through this methodology, the data of New Space shall give the high value expected for the operational management and the training for people on the ground and Space segment.

4-Discussion

4.1 Space data processing vulnerabilities

The Space data is common of the one on the ground except the interpretation needs to understand the way of the data displaying on the screens.

All Space missions depends on the data and the sensors behaviour to provide the status of a system from Spacecraft, materials, and people in Space. Moreover, the Space as the services through Cloud providers provide the capacity to use the satellites and store data in a data-center. In this context, the processing of data changes to show the vulnerabilities specific applicable for Space domain. It concerns the Space networks, the payload on Orbit, the command and control to manage them.

Above all, it exists the organizations with theirs own satellites fleet including the ground segment and the Space segment. Then, the new generation of satellites [1] like CubeSat, SmallSat, NanoSat owns the functionalities.

The Space data became a tool to manage the ground and to support the human activities for an operational purpose. As well, the point is to ensure the availability and the integrity of the data in order to be use for the ground. Its use concerns the Space exploration too for the assets begins to be launched outer the Earth orbit for permanent mission. The process of data shall be ensure in terms of integrity and availability to provide the right measures or the observation of sensors in Deep Space. At last, the crew ans the teams on the ground should be trained to follow this Space data processing to manage correctly the the work flow of these informations.

The Space systems are vulnerable for all support concerned by the digital signal in transit : the ground station, the object on orbit, the relay, the machine-human gateway. With a cyberspace extension in the vacuum of space, the cybersecurity ensures the satellite functionalities for the execution of many services : GPS for navigation, the transports, the imagery and detection for the ground, and above all the Internet full access potential from Space thanks to Starlink constellation, OneWeb system and the VSAT networks. As a Space command was created in many countries getting the Space skills : The United States, India, China, France, Russia, the United Arab Emirates, the space cybersecurity spreads out on the other topics. Since the first Apollo mission, the human kind is faced to face with its own image, with the Earth observation capabilities, the Artemis programme [2] with private contractors, the solar system exploration, the embedded cybersecurity system for all orbital objects. In addition to the risks linked to the Space territory, the main vulnerabilities are connected with the encryption, the password policies, the insecure protocol and the misconfiguration software. Moreover, the orbital position are concerned too by these vulnerabilities. Indeed, satellites next to the equator with a low inclination get an advantage on the others. As potential target, they may be more vulnerable_against the cyberattacks. In the purpose to give the value of the available services from Space, the data and the signal must be secured.

Thanks to data to make allowing public or private decision, the signal analysis shows the potential of action and the hardening solution to improve the signal security. The first point is the properties of cyberspace to be considered : the signal transmission and reception crosses several context with the use of C and K band frequencies : the Ether, the atmosphere, the Earth electromagnetic field, the Space itself, the gravitation, and the space meteorology.

One more point is the others conditions which appear in the Space Telecommunication Architecture for a system.

The Starlink Internet service [3], with 600 hundreds satellites in low orbit for 42000 planned, with 12000 satellites authorized for launch in 2020, a signal test reaching a bandwidth of 60,24 Mbits/s down and 17,64 Mbits/ up with 20ms latency announced, demonstrates an innovative network for the applying of security standard : roaming check, satellite move towards the receivers, satellite laser synchronization, data packets with ground station, between the satellites, signal double jump. Concerning the 0,48 meters receivers antenna, a jamming and man-of-the-middle attack could be launched. The second point deals with the network vulnerability when there is a transmission and reception signal between orbital objects and the ground station.

The command and control system works with the protocols which are not unknown. The computer design is the same, the input and the ouput as Ethernet gateway, Shell, UDP, TCP, Wireshark and in more Red Team Hackers and Green Team owning materials as DVB card, transponder, antenna. Following this general process, the IP and UDP datagram analysis highlights the ID, the type of encryption, the satellite orbit, the frequency, the polarisation, the synchronization. The 3D visualization provides the right time to connect to the satellite. Then, the "US catalog of space objects" use gives some information about satellite orbital data too. The globalized economy, through the space networks, needs an embedded space cybersecurity. This cybersecurity describes the embedded digital system inside the shuttle, the modules, the rockets, and the satellites for most of them. The cybersecurity framework applying for the satellites and the Space communication in generally is sitll to be built in a strong digitalization context. The satellites own a weight, a height control, the solar panels for the electric power, an orbital period, an inclination, an antenna, the instruments on board. And to execute the automatic process from the crew and the

ground station, each command answers with a specific action for which a computer on board or printed circuit do a computation. At the last Hack-a-Sat organized by the Air Force and the Digital Defense service in 2020, the hack of "Stars tracker" mechanism provoked an orientation change of the solar panels to the sun. Some examples exist since the year 2000.

This type of cybersecurity gets the machine-human gateway where the cognitive security studies the correct data understanding from the computer to mitigate the action in the ground station or in Space. During the Apollo 11 mission, some alarms switched on from the computer on board at the moment the module started its move toward the lunar ground. The crew report mentioned an alarm that only the ground station could understand. It means that the 1201 and 1202 alarms had been simulated by the engineer Jack Garman and Steves Bales, a flight officer. The crew was too concentrate and its approach of the ground submitted at "the shuttle effect". The point was the computation of landing radar and the accelerator command algorithm. And the 72 Ko memory from the computer had some difficulties to interprate the data incoming. The space cybersecurity introduces a methodology and the add-on extensions at the web environment. At least, the first quantum signal between satellites turns on closely a space cybersecurity to the particle physics.

4.2 The cognitive cybersecurity

Cognitive cybersecurity is a posture that allows us to understand artificial human behavior through the operation of cognitive functions drawn from human-machine interfaces. It is based on a type of cognition that designates the way in which artificial systems acquire data by producing representations, and by transforming them into knowledge by algorithms based on the functionalities of the brain in order to implement them in the activities, the behaviors of a system. Cognitive functions are integrated in the functioning of applications and frameworks in artificial intelligence, such as the IBM Watson IOT platform [4], which allows to introduce other parameters in the methods of intrusion of the target system. Also, while they allow cognitive hacking of individuals and organizations, there are cognitive security countermeasures.

Cognitive hacking involves self-learning systems that use the availability and exploration of sensitive and non-sensitive data, the recognition of deterministic patterns that systems use, the processing of natural language in the construction of different types of algorithms: K-means, DBSCAN, KNN, WARD, Weka. It takes as its target the cognitive functions embedded in the operation of a system or application. On March 22, 2016, the attack against the Vinci stock price relied on the content of an email based on the fabrication of a sense of urgency to bypass the first level of security control. It also attacks the cognition of individuals targeted within organizations. The main vector of this hacking is linked to data access, so that CISOs, security managers, and people in charge of management are potential disseminators. Its effect is all the more destructive during crisis phenomena or in a_non-peaceful human context: attacks, health crisis, jealousy, frustration, poor organization, deterministic education, uncontrolled ego, undefined private-public boundary, absence of professional ethics or healthy organizational culture, excessive surveillance.

It is defined by an ability to detect and remedy a cognitive hacking process produced by the construction of artificial ecosystems of data interpretation that stimulate behavior leading to a wrong decision. The algorithms of high-frequency trading caused, on October 5, 2012, is a sharp drop in the NIFTY index followed by a bullish recovery as strong. It is involved in defining threat awareness, detecting anomalies in the behavior of systems and organizations, and responding to incidents. In each of its phases, cognitive security is a countermeasure to the specific vulnerabilities of data that determine each organization and individual. At the data level, the application of these parameters are, for example, applicable to the model of validated data that is then used by the business thanks to the predictive model of Machine Learning. This technology is defined by the ability of a machine to calculate, in a short period of time, the processing of different types of data for operational purposes. At the individual level, behavioral anomalies are the most visible signs of detection. And the encouraging factors are more related to the psychiatric history of each individual and the way in which their cognitive functions process information. Cognitive remediation, in its function of repairing alterations caused by a new situation, takes the form of cybersecurity where sensors are produced to build a value chain through: an algorithm oriented on natural language with the "Chatbot COVID 19" and the implementation of the "Robert" protocol in the form of an application whose coordination level is placed at the pan-European level. The COVID 19 Bot is based on a series of questions/answers from natural language processing and automatic text generation. The Bot queries a knowledge base to enable it to answer the identified object. The "ROBust and privacy preserving proximity Tracing" protocol is characterized by an architecture based on Bluetooth technology and the use of pseudonyms ("crypto-identifiers").

A server assigns temporary pseudonyms. These are exchanged to keep a history of the people crossed in the server. The application checks whether the alias is in the list of infected persons and alerts in case of a positive response.

5. Conclusions

The cognitive cybersecurity is linked with the presence of the machines and their capacities to provide information thanks to the quantity of data. With the Space requirements, the ability to manage data need the neural framework where in addition the exchange machine-to-machine, the one marked by machine-to-human shall be understood to consider the safety and the security of operations.

References

List of references

Reference to a journal publication:
[1] Alessio Botta, On the performance of new generation satellite broadband internet services, 2014, IEEE Communications magazine, Electrical and Electronic Engineering.
[5] Dr. James Crowder, The Artificial Cognitive Neural Framework, 2012, Raytheon Intelligence and Information Systems Division16800 E. Centretech Parkway, Aurora, Colorado 80011.
[4] Luca De Nardis, Alireza Mohammad, Giuseppe Caso, Usman Ali, Maria-Gabriella Di Benedetto, Internet of Things Platforms for Academic Research and Development : Critical Review, 2022, MDPI AG.

Reference to a book:
[2] Andrew S Thompson, Artemis Program, 2020, Nasa's Lunar Exploration Program Overview.
[3] Shkelzen Cakaj, The parameters comparison of the Starlink LEO Satellites constellation for different orbital shells, May 2021, Universiteti Politeknik I Tiranës.

.