Gyancity Journal of Electronics and Computer Science,
Vol.5, No.1, pp. 76-90, March 2020
ISSN: 2446-2918 DOI: 10.21058/gjecs.2020.51008

Digital Threat Detection Model to Mitigate Cybersecurity Risks in Organizations

Felix Eloy Jimenez Chuque
Escuela Universitaria de Posgrado, UNFV-EUPG, Lima, Peru
colcabamba@gmail.com

Abstract

Cybersecurity is a fundamental aspect of networks, computers, software, and data. The objective is to establish a Digital Threat Detection Model to mitigate cybersecurity risks in organizations by evaluating the influence of cybersecurity infrastructure on the global cybersecurity index. *Without sufficient security, these assets are vulnerable to malicious threats (Xiong & Lagerström, 2019). The technological platforms located in the data centers of the organization itself or through service providers locally or in the cloud make available communications services, databases, application servers, and managed security services, among others. Multiple times we find that the published services are compromised by different types of digital threat that compromises the operational continuity of the organization or even its reputation. Digital services must be permanently attended even more if we have users who permanently consult the services offered on the platforms. Every service published on the Internet is always attacked by different forms or digital variants that violate or paralyze the applications that serve the public. In this sense, it is important to understand ways and ways to identify a digital threat; the criteria used to differentiate correct traffic from another that violates or intends to violate our platforms, as well as knowing how our digital services are organized, the technological infrastructure, both network architecture, and security.*

Keywords: *Cybersecurity, technology platforms, data centers, service providers, threats.*

1. Introduction

When the cybersecurity architecture is established, we must have a clear understanding of the type of services we are going to protect, what are the criteria to

use, what protection tools do we have, what are the capabilities of the collaborators who are part of the digital security team. Threats have a different level; they are of a different type, and also of different intensity how we approach a problem of this nature, what are the steps to follow to understand the problem of the other and that a specialist with sufficient capabilities can correctly address a digital threat.

In this sense, it is necessary to mitigate cybersecurity risks. Risk mitigation is a conceptual framework of the form and manner in which this research is approached, and considers it important to establish the following in the first place:

- Identify digital threats.
- Diagnose the organization's capabilities in terms of digital security.
- Establish policies for attention and mitigation of risks in cybersecurity.
- Strengthen the capabilities of the technological infrastructure.
- Manage protection assets in digital security

There is a dispersion of events in each digital service published on the internet, as well as incidents that are registered in each server, database, application servers, as well as the security infrastructure that exists in each organization.

Digital threats in their different variants maintain behavior patterns with random dispersion of existing records or databases, be they virus signatures, system updates, or others, as well as peripheral devices or IoT (Internet of Things) devices. In other cases, we have threat mitigation scenarios of Firewalls, IPS, IDS, WAF, and other analysis tools, but these maintain a linear behavior or under supervised learning schemes, but they do not necessarily identify the incoming threat in a scaled way.

1.1 The security platform

In the corresponding case of this study, consider the integration of learning machines in the analysis of the behavior of users and IOT teams that are used at the level of trusted data centers, as well as end users who use them in an authorized way—the digital platforms of any organization. The design of a computer security architecture allows us to provide improvements in the protection of the assets of any organization integrated into the security platform and guarantee the continuity of digital online services. Global threats are aspects that should always be considered throughout the organization's digital platform, because there is an integration between the different services available and the interaction with other platforms are located within the organization, or outside it. The dynamics of communications seriously affect any program or digital system. In these scenarios, it is important to consider that global threats always affect organizations and their digital services. Internal threats are the most frequent in the entire network infrastructure, mostly affecting the services that manage the accesses and the internal network. Considering that there are different sources where the services are affected, be they USB ports, emails, or Internet browsing, how does a Digital Threat Detection Model influence the mitigation of problems of cybersecurity risks of

organizations? The objective is to establish a Digital Threat Detection Model to mitigate cybersecurity risks in organizations by evaluating the influence of cybersecurity infrastructure on the global cybersecurity index, determining the existing relationship in organizations with cybersecurity certifications and its impact on the global cybersecurity index and the existing relationship of security incident response teams and the global cybersecurity index, so that if the Digital Threat Detection Model is implemented, then it influences the mitigation of cybersecurity risks in organizations.

2. State of the art

Currently, digital threats have seriously affected the daily work of existing computing platforms and services. Cybersecurity is the means where we can give attention to these threats and be able to mitigate them using different ways and thus guarantee the continuity of the corresponding service. The current interpretation of the behavior of users and computer equipment in pre-established behaviors, in the face of unforeseeable threats, generates a more significant problem, in that sense, having unidentified threats according to existing patterns generates a mitigation problem. The teams dedicated to networks and security have events where we can integrate and centralize them to organize and present structured information, and based on this, we can make decisions. Also, users have ways to make queries to certain systems. A system records recurring events; Any event that escapes the baseline pattern of its behavior can then, in the presence of pre-existing records, we can then consider that the user has behavior outside the established parameters. It is evident that, in emerging economies, there is a growing demand for digital services, which is why it is necessary to guarantee its continuity and operability, the information obtained from this work will allow us to develop new forms and models in the way we have to manage resources. computer science of an organization. In this way, we will also be able to identify cybersecurity problems in organizations so that we can mitigate strategically through relevant tools and solutions. The study will also allow projecting new research around the cybersecurity problem, the existing reality of the technological infrastructure in computer security, the limitations of professional capacities due to the expertise demanded by the sector. This document establishes a baseline of the corresponding indicators and infrastructure for security, threats, and vulnerabilities. Thus, it also allows identifying a classification of the operational units in the digital security of organizations. This research is important since it guarantees the operational continuity of the organization. This digital threat detection system will prevent online systems from being attacked, and the continuity of digital services is not affected. It is evident that it will allow timely warning of massive attacks on different digital services and will facilitate security officers to establish more immediate communication with the organization's security and network managers.

2.1 Theoretical Bases

ISSN: 2446-2918 DOI: 10.21058/gjecs.2020.51008

The existence of different models to detect digital threats allows any organization to adopt protection schemes for its critical assets, guaranteeing the continuity of its digital operations. The proposed Business Cybersecurity Management model (Donaldson, Siegel, Williams, & Aslam, 2018) allows us to have a vision of what every organization should assume as a role within the strategy of detecting digital threats and how to prevent them. Cybersecurity is a fundamental aspect of networks, computers, software, and data (Xiong & Lagerström, 2019); without sufficient security, these assets are vulnerable to malicious threats. There are different points of view around cybersecurity, considering specialists in cybersecurity, vulnerability scanning, virus filtering in emails, protection of personal information, prevention of cybersecurity, data protection service, all these aspects should be considered in a threat detection model (Thakur, Qiu, Gai, & Ali, 2016). The integrity of the data is another important aspect to consider, the damage to integrity causes more serious problems than the existing gaps in its storage (Gheyas & Abdallah, 2016). Attacks on data integrity seriously affect critical infrastructure systems. The digital assets of an organization, as well as the critical assets of a nation, are affected if the existing vulnerabilities are not addressed in the corresponding time frames. There is a cost incurred for not paying attention to cybersecurity infrastructure needs (Johnson, 2015). APT attacks, Persistent Advanced Threats are sophisticated network attacks where the attacker seeks to gain information and not be detected for a certain time, acquiring a large amount of information and knowledge of the violated infrastructure. APT attacks are not designed to cause damage but to obtain and modify data. (Johnson, 2015). Currently, there are various types of digital threats, whether internal or external, considering intrusions and vulnerabilities, malware. The way to identify them depends on the criteria to be used and the tools to be used. Be these honeypots, security systems, ethical hacking services, as well as honeypots for collecting zero-day malware.

- Threat detection techniques
- Threat detection systems and techniques
- An approach based on patterns and related techniques.
- The approach based on behaviors, behavior.
- (Risk and Security of the Internet)
- Cybersecurity is a fundamental aspect of networks, computers, software, and data

The fundamental basis of threat modeling is to identify, communicate, and manage digital security weaknesses. This is accomplished by understanding the possible threats and attacks that the system must resist and the corresponding countermeasures (controls) for those threats.

2.2 Cyber attacks generations

- Generation 1 - Late 1980s, virus attacks on stand-alone PCs affected all businesses and drove the rise of anti-virus products.
- Generation 2 - Mid 1990s, attacks from the internet affected all business and drove the creation of the firewall.
- Generation 3 - Early 2000s, exploiting vulnerabilities in applications affected most businesses and drove the rise in intrusion prevention systems (IPS) products.
- Generation 4 - Approximately 2010, the rise of targeted, unknown, evasive, polymorphic attacks affected most businesses and drove the increase in anti-bot and sandboxing products.
- Generation 5 - Approximately 2017, large scale and multi-vector mega attacks using advanced attack technologies. Detection-only based solutions are not sufficient enough against these fast-moving attacks. Advanced threat prevention is required.

2.3 Digital threat

It is considered a digital threat when the contents or services published on the digital platform seek to be altered or violated in such a way as to modify the functionality of a digital system or infrastructure.

2.4 Detection System

There are platforms at the hardware and software level that allow preventing, blocking, or stopping different types of threats to a service published on the digital platform or to the operating system or hardware functionality. Detection systems alert to these threats and mitigate or eliminate the digital threat.

2.5 Digital Government

Any digital infrastructure or service that an organization has and that fulfills a function corresponds to the form and way of governing a system or process. Digital governance is said to exist because its decision processes are digital.

2.6 Web services

It is a set of standards and protocols that allows any digital platform to operate. Under this scheme, all the systems of different organizations can interoperate. Management

2.7 Digital platform

It is the architecture at the Hardware, software, directives, policies, and procedures level of a system or organization.

2.8 Digital Threats

Digital threats are malicious programs whose main purpose is to violate a digital service or infrastructure. It is related to digital attacks generating different ways and ways of violating the operability or continuity of a digital service of a particular organization. Its purposes are varied.

- Threat model
- System model
- Asset model
- Types of Digital Threats

There are several ways to classify the types of digital attacks or threats (ENISA, 2019), in the definition of common use we have:

- Malware
- Web-Based Attacks
- Attacks Web Applications
- BotNets
- spam
- Ransomware
- Internal Threat
- Physical manipulation / damage / theft / loss
- Exploit kits
- Data gap
    - Identity Theft
    - Information leakage
- Cyber espionage
- Advanced Persistent Threat (APT)
- Brute Force Attack
- Denial of Service Attack (DoS)
- Man in the Middle Attack
- Phishing attack
- Threat Agents

They are the means of carrying threats (ENISA, 2019) to the different technological infrastructures of the organization.

- Cybercriminals
- Employees (insiders)
- Nations (states)
- Corporations
- Hacktivists
- Cyber terrorists
- Script kiddie.
- The life cycle of an attack

The concept of an attack life cycle extends to threats beyond those that exploit the exposure of an organization's systems in cyberspace, internal threats, threats to industrial control systems and other systems, and the supply chain.

2.9 Global Cybersecurity Index

It is an indicator that measures the level of commitment of a country to cybersecurity. It has a wide field of applications covering industries and sectors and analyzing in 5 categories: Legal measures, technical measures, organizational measures, capacity building, and cooperation.

2.1O Digital Government

Oriented actions of an organization or country around good governance practices in the digital environment. In the particular case, good practices of RENIEC and state institutions, both publicly and internally, of their services placed in digital environments.

- Cybersecurity risk
- Classic strategies for risk management
- Avoiding risks
- Address the risks
- Accept risks
- Transfer risks
- Ignore risks
- Advanced Persistent Threat (APT)

It is a sophisticated and targeted attack. This threat poses a risk to all organizations, especially if they manage sensitive data or critical infrastructure. Recently, the analysis of these threats has caught the attention of the scientific community. Researchers have studied the behavior of this threat to create models and tools that allow the early detection of these attacks. The use of Artificial Intelligence can help automatically detect, alert, and predict these types of threats and reduce the time that the attacker can stay in a network organization. The objective of this work is a review of the proposed models to identify the tools and methods they have used.

Quintero-Bonilla, S., & del Rey, A. M. (2020). Proposed models for advanced persistent threat detection: A review doi: 10.1007 / 978-3-030-23946-6_16 Retrieved from www.scopus.com

- Advanced Persistent Threat Detection - APT
- Detection and Protection Techniques
- Cyber risks
- Mitigate cyber risks

• Assess the risks.

2.11 Cyberattack

A cyber attack is an assault launched by cybercriminals who use one or more computers against one or more computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cyber criminals use a variety of methods, including malware,

2.12 Digital threat

Digital Threats are malicious programs whose main purpose is to violate a digital service or infrastructure. It is related to digital attacks generating different ways and ways of violating the operability or continuity of a digital service of a particular organization. Its purposes are varied.

It is an indicator that measures the level of commitment of a country to cybersecurity. It has a wide field of applications covering industries and sectors and analyzing in 5 categories: Legal measures, technical measures, organizational measures, capacity building, and cooperation.

2.13 Detection System

There are platforms at the hardware and software level that allow preventing, blocking, or stopping different types of threats to a service published on the digital platform or to the operating system or hardware functionality. Detection systems alert to these threats and mitigate or eliminate the digital threat.

2.14 Digital Government

Any digital infrastructure or service that an organization has and that fulfills a function corresponds to the form and way of governing a system or process. Digital governance is said to exist because its decision processes are digital. Oriented actions of an organization or country around good governance practices in the digital environment. In the particular case, good practices of RENIEC and state institutions, both publicly and internally, of their services placed in digital environments.

2.15 Web services

It is a set of standards and protocols that allows any digital platform to operate. Under this scheme, all the systems of different organizations can interoperate. Management

2.16 Digital platform

It is the architecture at the Hardware, software, directives, policies, and procedures level of a system or organization.

2.17 Advanced Persistent Threat (APT)

It is a sophisticated and targeted attack. This threat poses a risk to all organizations, especially if they manage sensitive data or critical infrastructure. Recently, the analysis of these threats has caught the attention of the scientific community. Researchers have studied the behavior of this threat to create models and tools that allow the early detection of these attacks. The use of Artificial Intelligence can help automatically detect, alert, and predict these types of threats and reduce the time that the attacker can stay in a network organization. The objective of this work is a review of the proposed models to identify the tools and methods they have used.

Quintero-Bonilla, S., & del Rey, A. M. (2020). Proposed models for advanced persistent threat detection: A review doi: 10.1007 / 978-3-030-23946-6_16 Retrieved from www.scopus.com

- Advanced Persistent Threat Detection - APT
- Detection and Protection Techniques
- Cyber risks
- Mitigate cyber risks
- Assess the risks.

2.18 Cyberattack

A cyber attack is an assault launched by cybercriminals who use one or more computers against one or more computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cyber criminals use a variety of methods, including malware, phishing, ransomware, denial of service, among other methods.

3. Methodology

The type of research include the following:

- Research focus: Quantitative
- Research Type: Non-Experimental
- According to the planning of the measurements: Prospective
- According to No. of measurements Variable: Longitudinal
- According to the number of variables: Analytical
- Research Level: Relational / explanatory
- Non-Parametric Tests
- Related samples.

The investigation details the different existing theories about the problem under study. These theories constitute the theoretical-scientific support of the theoretical framework; Then are formulated our hypothesis and contrasted them with the problematic reality to arrive at theoretical conclusions about the Model of Detection of Digital Threats and Mitigation of Cybersecurity Risks in organizations. The research

level is situated at the descriptive-correlational level. It is descriptive because we are going to measure and describe the independent variable Digital Threat Detection Model and the dependent variable Cybersecurity Risks in organizations. It is correlational because the level of correlation between the variables will be established to carry out the respective interpretation then. Research Methods that will be used during the research process will be the descriptive-correlational method because the data obtained will be observed to explain the relationship between the two variables, that is, to know to what extent the variation of one of them affects the other, to know its magnitude, direction, and nature. Likewise, the use of the analytical-synthetic method is not ruled out. Through this method, all the variables will be decomposed to observe their relationships, similarities, differences, causes, nature, and effects towards other variables, and then reconstruct them from the elements distinguished by the analysis.

3.1 Population and sample

The universe considered are 300 organizations that have a unit related to digital government, being responsible for the digital platforms with the largest national presence. A sample of 30 information technology managers has been considered to be reviewed on their digital platforms.

3.2 Variables

Independent Variable: Digital Threat Detection Model.

- Indicators:
  - The number of cybersecurity equipment installed.
  - The number of certifications in cybersecurity.
  - The number of attention to digital security incidents.

Dependent Variable: Cybersecurity risks in organizations

- Indicators:
  - Electronic Government Index
  - Electronic government policies in cybersecurity.
  - Global cybersecurity index.

4. The digital threat detection model

Digital Threat model must contain:

- System Model
- Asset model
- Identify the Types of Digital Threats

There are several ways to classify the types of digital attacks or threats (ENISA, 2019), in the definition of common use:

ISSN: 2446-2918 DOI: 10.21058/gjecs.2020.51008

- Malware
- Web-Based Attacks
- Attacks Web Applications
- BotNets
- Spam
- Ransomware
- Internal Threat
- Physical manipulation / damage / theft / loss
- Exploit kits
- Data Gap
- Identity Theft
- Information leakage
- Cyber espionage
- Advanced Persistent Threat (APT)
- Brute Force Attack
- Denial of Service Attack (DoS)
- Attack Man in the Middle
- Phishing attack
- Threat Agents

They are the means of carrying threats (ENISA, 2019) to the different technological infrastructures of the organization.

- Cybercriminals
- Employees (insiders)
- Nations (states)
- Corporations
- Hacktivists
- Cyber terrorists
- Script kiddie.

Gyancity Journal of Electronics and Computer Science,
Vol.5, No.1, pp. 76-90, March 2020
ISSN: 2446-2918 DOI: 10.21058/gjecs.2020.51008

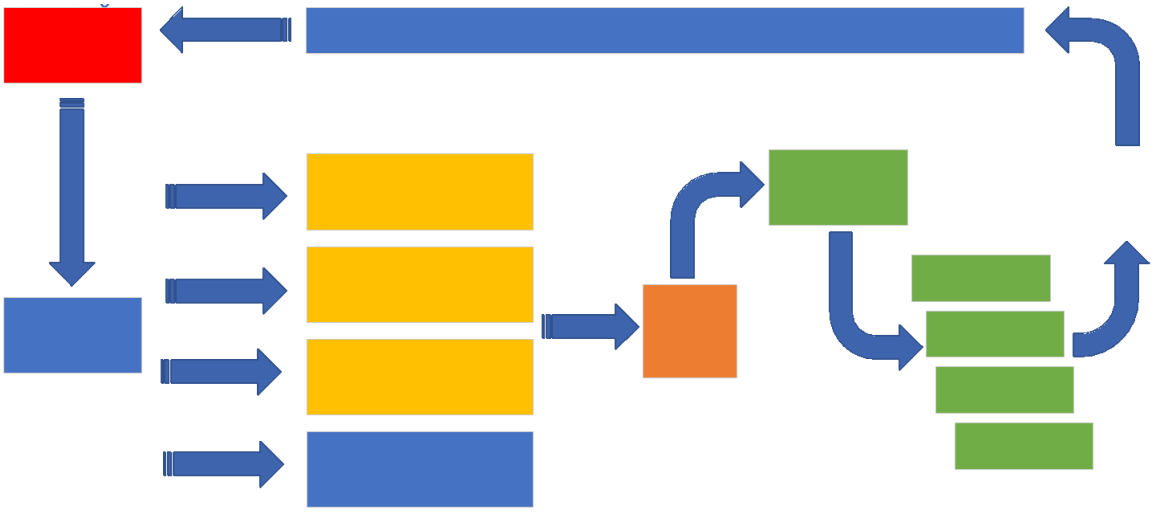

Figure 1: cybersecurity model

4.1 The life cycle of an attack

The concept of an attack life cycle extends to threats beyond those that exploit the exposure of an organization's systems in cyberspace, internal threats, threats to industrial control systems and other systems, and the supply chain.
Global Cybersecurity Index

5. Results

5.1 Variable 1: Digital Threat Detection Model

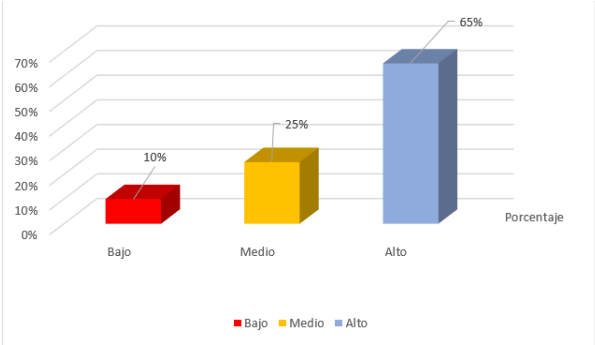

Figure 2: Digital Threat Detection Model

Figure 2 shows a high level for the variable and the Digital Threat Detection Model. Where 65% of respondents consider it important to establish a digital threat detection model that will guarantee a level of coverage to protect against cybersecurity risks

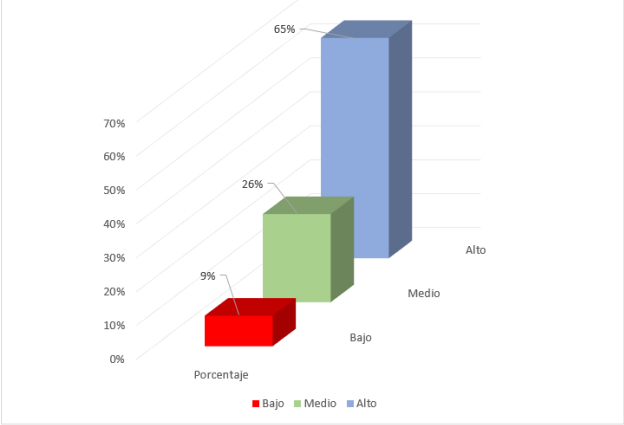

Figure 3 Cybersecurity Risks

Figure 3 shows a high level for the Cybersecurity Risks variable, where 65% of the respondents consider the existence of a digital threat detection model important.

Table1 Indicator: Number of cybersecurity equipment installed

LEVEL	%	VALID %	% ACCUMULATED
LOW	**18%**	**0%**	**0%**
MEDIUM	**14%**	**2%**	**2%**
HIGH	**68%**	**98%**	**100%**
TOTAL	**100%**	**100%**	

Table 1 shows the "Number of cybersecurity equipment installed" to control threats according to the proposed model

6. Discussion

After having carried out the fieldwork on our selected sample, acceptable and optimal results have been obtained, which allow us to coincide with the statements established by the different authors, which were cited in the present investigation. The results obtained allow us to establish that there is a relationship between the variables Model of Detection of Digital Threats and Cybersecurity Risks in Organizations; Similarly, the calculated correlation coefficient checks that the correlation is positive and high. Therefore, the hypothesis that "The implemented digital threat detection model influences the mitigation of cybersecurity risks in organizations" is accepted.

7. Conclusions

The different scenarios where organizations develop consider aspects to take into account in the construction of secure platforms. Each aspect must be considered when planning the prevention or defense strategy for digital services, considering that each technology demands different protection services and specialized management. The detection or prevention of digital assets in the face of threats requires an operations plan, trying to understand that each aspect must be considered when preparing a maintenance plan for the care or recovery of an affected asset. Employees must have sufficient capabilities in management tools and computer equipment to deal with alerts that different platforms report through monitoring consoles. It is necessary to bear in mind that adequate management in the monitoring of the services guarantees a forecast before the alerts that appear in the administration consoles. Every critical digital service in the organization requires specialization from the unit responsible for digital security. Both at the server platform level, whether it is an application or a database, as well as the security solutions responsible for protecting the organization's digital assets

References

[1] Avgerou, A., & Stamatiou, Y. (2015). Privacy awareness diffusion in social networks. IEEE Security and Privacy, 13(6), 44-50.
[2] Brotby, K., & Hinson, G. (2013). PRAGMATIC Security Metrics: Applying Metametrics to Information Security. Auerbach Publications.
[3] C. Bronk. (2016). Cyber threat: the rise of information geopolitics in U.S. national security. ABC-CLIO.
[4] Collaborative Cyber Threat Intelligence. (2017). Collaborative Cyber Threat Intelligence.
[5]Dawson, M., & Omar, M. (2015). New threats and countermeasures in digital crime and cyber terrorism. IGI Global.
[6]Dube, R. (2008). Hardware-Based Computer Security Techniques to Defeat Hackers: From Hackers:
[7] Khajuria, S., Sørensen, L., & Skouby, K. (2017). Cybersecurity and Privacy - Bridging the Gap.
[8] Kohnke, A. (2017). Implementing Cybersecurity. Auerbach Publications.
[9] Kulesza, J., & Balleste, R. (2015). Cybersecurity and Human Rights in the Age of Cyberveillance.
[10] Nelson, B., Philips, A., & Steuart, C. (2016). Guide To Computer Forensics and Investigation:
[11] Sha, K., Striegel, A., & Song, M. (2016). Security, Privacy and Reliability in Computer Communications and Networks.
[12] Tripathy, B., & Baktha, K. (2018). Security, Privacy, and Anonymization in Social Networks: Emerging Research and Opportunities. IGI Global.