ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 2, pp: (60-70), Month: April - June 2023, Available at: www.researchpublish.com

Cyber Security and its role in achieving the future visions of the State of Kuwait

Mohammed Jassem Al-Sarraf

The public Authority for Applied Education and Training

DOI: https://doi.org/10.5281/zenodo.7923877

Published Date: 11-May-2023

Abstract: **This field research deals with the role of cyber security in achieving the future visions of the State of Kuwait. Specifically, this research attempts to answer the main question of the research, which: What is the role of cyber security in achieving the future visions of the State of Kuwait**?

In this field study, both approaches are used: The qualitative approach and the quantitative approach, and the questionnaire tool was used, and one of the most important results was the existence of a correlation between the state's visions and the basic components of cyber security. Also, several elements of the cyber security requirements necessary to achieve the visions of the State of Kuwait are already available, as well as there are Some obstacles that limit the application of cyber security in an integrated manner.

The study also ended with some recommendations: The necessity of activating the basic components of cyber security. As well as reviewing and evaluating its mechanisms and functions and applying them in all government institutions, reviewing and monitoring the sub-components of cyber security, in addition to setting strategic plans and objectives for cyber security, applying security updates and reforms permanently and periodically to limit the spread of Distributed attacks across cyberspace.

Keywords: **Security, Cyber Security.**

1. INTRODUCTION

Now, Cyber Security has become one of the most important issues for individuals, businesses, and governments alike. Cyber Security refers to the protection of networks, computer systems, and sensitive information from unauthorized access, theft, or damage. Due to the increasing of dependence on technology, and the internet, the threat of cyber-attacks has become more prevalent than ever before. The consequences of a cyber-attack can range from minor inconvenience to severe damage, including financial losses, reputational damage, and even loss of life.

Search problem:

The problem of the study determined by the following main question: - What is the role of Cyber Security in promoting the vision of the State of Kuwait?

2. RESEARCH METHODOLOGY

In order to achieve the objectives of this research, I will rely on the following scientific methods:

a) The Deductive Approach: By studying and summarizing the researches that published before and related to the topic of the research. In addition, knowing the findings of these researches (the results) to start from where the others ended.

b) The inductive approach: The study used the qualitative approach and the quantitative approach, and the questionnaire tool is used.

Research aims:

Finding a link between Kuwait's vision programs and the basic components of Cyber Security. There are several elements of cyber security requirements, which are necessary to enhance the country's vision programs. Many obstacles limit the application of cyber security in the vision of the state.

Research limits:

The limitations of this field research are as follows:

- Objective limits: This research deals with the issue of Cyber Security, through a questionnaire to elicit opinions, and an effort to find solutions or treatment for this problem.
- Spatial boundaries: This field research applied to a sample of ordinary Kuwaiti individuals in the State of Kuwait.
- Time limits: This research implemented in the academic year 2022/2023.

Cyber security concept:

We can define Cyber security as employing the technologies, processes, and measures necessary to ensure the security of systems, networks, programs, devices, and data. Moreover, protect them from electronic attacks. Its main purpose is to reduce electronic risks to which systems and networks may be expose and protect them from unauthorized exploitation.

The birth of cyber security

The following is an explanation of the stages of the emergence of cyber security:

Seventies of the twentieth century:

The history of cyber security dates back to the 1970s. When terms such as spyware, viruses, and worms were not so popular due to the high rate of cybercrime. These terms have emerged in daily news headlines over the entire world. In addition, when we go back in time to the time of the emergence of cyber security, computers and the Internet were still under

Eighties of the twentieth century:

In the 1980s, Robert T. Morris can invented the first electronic virus program, which gained massive media coverage due to its spread between devices and causing system failures. Morris sentenced to prison and fined, and that ruling played a role in the development of laws related to cyber security.

Nineties of the twentieth century:

The development of cyber security events continues with the passage of time, with the development of viruses that infect devices. So the world became aware of electronic and fetal risks. In addition, among the most prominent measures taken in the nineties of the twentieth century was the development of website protection protocols such as (http) and other, which is one of the types of protocols that allow the user to access Internet safe.

Types of cyber security

Cyber security has different types; we can summarize it in the following important types:

Network security

In it, computers is protected from attacks that may be exposed to them inside and outside the network, and one of the most techniques used to implement network security is called the firewall. Firewall acts as a protector between the user device and all other devices in the network, Moreover e-mail security.

Application security

In Application security, information related to an application on the computer are protected, such as procedures for setting passwords, authentication processes, and security questions that guarantee the identity of the application user.

Cloud security

Cloud programs that known as data storage and preservation programs over the Internet, and many resort to saving their data through electronic programs instead of local storage programs, which led to the emergence of the need to protect that data. For this reason, cloud programs are concerned with providing the necessary protection for their users.

Operational Security

It is the risk management of internal cyber security operations, in which risk management experts are employed to find an alternative plan in the event of an electronic attack on user data. Moreover, it includes educating and training employees on best practices to avoid risks.

Cyber security goals:

The following are the most important goals that cyber security:

Data availability:

Data availability refers to the feature that allows authorized persons to access and modify data and information in a timely manner. In other words ensuring reliable and continuous access to information among the most prominent methods used for the availability of secure data: computer backup support and physical protection.

Integrity:

Integrity refers to the means used to ensure the validity and accuracy of data and to protect it from modification by any other users; it is the feature that aims to not change information in an unauthorized way. In addition, to ensure that the source of the information is real. Some of the most important techniques that cyber security employs to ensure integrity are test suites, backups, and data modification tokens.

Confidentiality:

Confidentiality is equivalent to the concept of privacy, in which unauthorized disclosure of information are avoided, data protection is ensured, trusted people have access to it, and others are not allowed to know the content of that data. An example of this is data encryption, which gives access only to those who can decrypt that data. Among the most important techniques, that cyber security employs to ensure confidentiality are encryption, data access control, authentication, authorization, and physical security.

Cyber security problems:

There are many difficulties and threats surrounding cyber security, these difficulties makes the information security sector alert, including the following:

Increasing the complexity of cyber attacks:

One of the most problems of cyber security is the increase in the complexity of electronic attacks in conjunction with the advancement of the electronic field, as the development of the fields of machine learning, encrypted currencies, artificial intelligence, and others has resulted in an increase in malware that exposes governments, companies, and individuals' data to constant danger.

Hide identities:

The emergence of some technologies, such as Bit coin crypto currency, has played a role in concealing the identity of users, allowing fraudsters to deploy techniques to steal information without fear of revealing their identity.

Lack of experts in the cyber security sector:

This means the acute shortage of experts from which the cyber security sector suffers, as this field suffers from a lack of specialists in it.

Unsecured internet connection:

Excessive reliance on an unsecured Internet connection may leads to the breakdown of information exchange systems and the increasing of the likelihood of malware spreading.

Spread of misinformation:

The intentional dissemination of misinformation using bots or automated sources, which endangers the safety of users of electronic information.

The evolution of fraud:

The increase in deception defrauds, as some people target people's data by tricking them into clicking on a link and the lack of awareness among people about that, and employing e learning in formulating more persuasive messages to deceive educated people about scams.

Physical cyber attacks

Physical cyber-attacks go beyond electronic data; as there are those who attack the data of water stations, trains and electricity.

Access to additional parties (three parties):

Three parties mean that the user allows other parties to access his own data, for example, logging into the sites using social networking applications or e-mail, which allows users of those sites to access the person's information.

Previous Studies:

1- Dan Craigen, Nadia Diakun-Thibault, Randy Purse, Defining Cyber security, October 2014.

Abstract:

Cyber security is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cyber security impedes technological and scientific advances by reinforcing the predominantly technical view of cyber security while separating disciplines that should be acting in concert to resolve complex cyber security challenges. In conjunction with an in-depth literature review, we led multiple discussions on cyber security with a diverse group of practitioners, academics, and graduate students to examine multiple perspectives of what should be included in a definition of cyber security. In this article, we propose a resulting new definition: "Cyber security is the organization and collection of processes, resources, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Articulating a concise, inclusive, meaningful, and unifying definition will enable an enhanced and enriched focus on interdisciplinary cyber security dialectics and thereby will influence the approaches of academia, industry, and government and non-governmental organizations to cyber security challenges.

2- Cyber security data science: an overview from machine learning perspective, Iqbal H. Sarker, A. S. M. Kayes, Shahriar Badsha, Hamed Alqahtani, Paul Watters & Alex Ng .

Abstract:

In a computing context, cyber security is undergoing massive shifts in technology and its operations in recent days, and data science is driving the change. Extracting security incident patterns or insights from cyber security data and building corresponding data-driven model, is the key to make a security system automated and intelligent. To understand and analyze the actual phenomena with data, various scientific methods, machine-learning techniques, processes, and systems that used, which commonly known as data science. In this paper, we focus and briefly discuss on cyber security data science. Where the data is being gathered from relevant cyber security sources, and the analytics complement the latest data-driven patterns for providing more effective security solutions. The concept of cyber security data science allows making the computing process more actionable and intelligent as compared to traditional ones in the domain of cyber security. We then discuss and summarize a number of associated research issues and future directions. Furthermore, we provide a machine learning based multi-layered framework for cyber security modeling. Overall, our goal is not only to discuss cyber security data science and relevant methods but also to focus the applicability towards data-driven intelligent decision making for protecting the systems from cyber-attacks.

3- A survey of emerging threats in cyber security, Author links open overlay panelJulian Jang-Jaccard, Surya Nepal

Abstract:

The exponential growth of the Internet interconnections has led to a significant growth of cyber-attack incidents often with disastrous and grievous consequences. Malware is the primary choice of weapon to carry out malicious intents in the cyberspace, either by exploitation into existing vulnerabilities or utilization of unique characteristics of emerging technologies. The development of more innovative and effective malware defense mechanisms that regarded as an urgent

requirement in the cyber security community. To assist in achieving this goal, we first present an overview of the most exploited vulnerabilities in existing hardware, software, and network layers. This followed by critiques of existing state-of-the-art mitigation techniques as why they do or do not work. We then discuss new attack patterns in emerging technologies such as social media, cloud computing, smartphone technology, and critical infrastructure. Finally, we describe our speculative observations on future research directions.

4- Cyber security: A Pre-history, Michael Warner - Published online: 05 Oct 2012.

Abstract:

The 'cyber' issue is not new, but rather has taken a half-century to develop. Indeed, it was already decades old before the public and many senior leaders recognized its salience in the mid-1990s. It developed, moreover, along a logical path, which can be depicted as the successive dawning (for American policymakers, officials, and intelligence officers) of four insights, each of which was glimpsed in theory at least shortly before empirical evidence verified that it was indeed a reality to consider in setting policies, standards, and doctrine. Thus, the official responses to the emergence of the cyber issue in the late-1990s were shaped by the outcomes of those earlier debates; the options available to policy-makers in the White House, Congress, the Pentagon, and the various agencies were already conditioned and even determined by previous arguments.

5- Machine learning in cyber security: A review, Anand Handa, Ashu Sharma, Sandeep K. Shukla, First published: 17 February 2019.

(https://doi.org/10.1002/widm.1306)

Abstract:

Machine learning technology has become mainstream in a large number of domains, and cyber security applications of machine learning techniques are plenty. Examples include malware analysis, especially for zero-day malware detection, threat analysis, anomaly based intrusion detection of prevalent attacks on critical infrastructures, and many others. Due to the ineffectiveness of signature-based methods in detecting zero day attacks or even slight variants of known attacks, researchers in many cyber security products are using machine learning-based detection. In this review, we discuss several areas of cyber security where machine learning used as a tool. We also provide a few glimpses of adversarial attacks on machine learning algorithms to manipulate training and test data of classifiers, to render such tools ineffective.

6- Cyber security Dynamics: A Foundation for the Science of Cyber security, Shouhuai Xum, Chapter, First Online: 23 May 2019.

Abstract:

Cyber security Dynamics is new concept that aims to achieve the modeling, analysis, quantification, and management of cyber security from a holistic perspective, rather than from a building-blocks perspective. It centered at modeling and analyzing the attack-defense interactions in cyberspace, which cause a "natural" phenomenon—the evolution of the global cyber security state. In this chapter, we systematically introduce and review the Cyber security Dynamics foundation for the Science of Cyber security. We review the core concepts, technical approaches, research axes, and results that obtained in this endeavor. We can outline a research roadmap towards the ultimate research goal. Moreover, identified technical barriers that poses challenges to reach the goal.

7- Cyber security of a power grid: State-of-the-art, Author links open overlay panelChih-Che Sun a, Adam Hahn a, Chen-Ching Liu, 2017.

Abstract

The integration of computing and communication capabilities with the power grid has led to numerous vulnerabilities in the cyber-physical system (CPS). This cyber security threat can significantly impact the physical infrastructure, economy, and society. In traditional IT environments, there are already abundant attack cases demonstrating that unauthorized users have the capability to access and manipulate sensitive data from a protected network domain. Electric power grids have also heavily adopted information technology (IT) to perform real-time control, monitoring, and maintenance tasks. In 2015, a sophisticated cyber-attack targeted Ukrainian's power grid causing wide area power outages. It highlights the importance of investment on cyber security against intruders. This paper provides a state-of-the-art survey of the most relevant cyber security studies in power systems. It reviews research that demonstrates cyber security risks and constructs solutions to

enhance the security of a power grid. To achieve this goal, this paper covers: (1) a survey of the state-of-the-art smart grid technologies, (2) power industry practices and standards, (3) solutions that address cyber security issues, (4) a review of existing CPS test beds for cyber security research, and (5) unsolved cyber security problems. Power grid cyber security research has been conducted at Washington State University (WSU) with a hardware-in-a-loop CPS tested. A demonstration provided to show how the proposed defense systems can be deployed to protect a power grid against cyber intruders.

8- Internet of Things (IoT) Cyber security Research: A Review of Current Research Topics, Yang Lu; Li Da Xu, Published in: IEEE Internet of Things Journal (Volume: 6, Issue: 2, April 2019).

Abstract:

As an emerging technology, the Internet of Things (IoT) revolutionized the global network comprising of people, smart devices, intelligent objects, data, and information. The development of IoT is still in its infancy and many related issues need to be solved. IoT is a unified concept of embedding everything. IoT has a great chance to make the world a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability. However, how to protect IoT is a challenging task. System security is the foundation for the development of IoT. This article systematically reviews IoT cyber security. The key considerations are the protection and integration of heterogeneous smart devices and information communication technologies (ICT). This review provides useful information and insights to researchers and practitioners who are interested in cyber security of IoT, including the current research of IoT cyber security, IoT cyber security architecture and taxonomy, key enabling countermeasures and strategies, major applications in industries, research trends and challenges.

Commenting on previous studies:

From the previously presented studies, and from some other studies, we can conclude the following:

1- Cyber security is of great importance in stabilizing state systems and maintaining the security and security of information at the individual and institutional levels, as well as at the state level.

2- Community members must made aware of the importance of cyber security and the importance of taking the necessary measures to protect their privacy and important information.

3- There are important cyber security factors that need support from the state to reach an acceptable degree of cyber security levels.

4- Continuous evaluation of the level of cyber security to find out its latest levels, and to improve this level permanently.

5- Informing of the seriousness of electronic attacks. Moreover, how to reduce or prevent them altogether.

6- Follow the necessary security instructions to avoid cyber-attacks.

7- Securing data and information by making a secure backup.

8- Use original anti-virus and cyber-attacks software.

9- Removing all obstacles that impede the advancement of the level of cyber security.

10- Preparing specialized cadres in cyber security to support the state in achieving it.

11- Develop a national strategy for cyber security.

12- Increase investment in research and development programs for cyber security.

13- Create internal industries for cyber security.

14- Increasing penalties related to cyber security.

Deductive method:

A questionnaire on Cyber security designed, consisting of 56 questions, this questionnaire designed using the Microsoft Forms application, and the questionnaire link was https://forms.office.com/r/6Qs2LJW71J

As for the questionnaire questions, they were as follows:

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 2, pp: (60-70), Month: April - June 2023, Available at: www.researchpublish.com

3. SUMMARY OF SURVEY RESULTS

Table 1

Variable	Category	Number	Percentage
Nationality	Kuwaiti	108	87.1%
	Non Kuwaiti	6	12.9%
Type	Male	52	41.9%
	Female	72	58.1%
Education Level	Less than University	4	3.2%
	University	86	69.4%
	Less than University	34	27.4
	Other	0	0
Age	Less than 20 years	0	0
	From 20 to less than 30 years	4	3.2%
	From 31 to less than 40 years	20	16.1%
	From 41 to less than 50 years	58	46.8%
	From 50 and more	42	33.9%
Total	124		

From the previous data, we note:

1. All responses number is 124.
2. Most responses are Kuwaiti (87.1%).
3. Males represents (41.9%), where Females represents (58.1%).
4. Most responses is in the age range from 41 and less than 50 (46.8%), where from 50 years and more represents (33.9%).
5. Most responses from workers in public sectors.
6. According to education level, we find university represents 86.4%.

Analyze data using SPSS:

After obtaining the different responses, we found that the number of responses is 124, and by converting these responses and entering them into the SPSS program, to analyze these results to obtain the stability coefficient of the questionnaire, as well as obtaining the frequencies, averages and standard deviation of these responses, we found the immediate results:

4. RESEARCH ANALYSIS

Through the results we have reached through statistical analysis using the SPSS program, we can summarize these results in the following points:

- The total number of responses is 124, of different ages and university qualifications, as well as of different ages.
- The number of women's responses reached 72, while men's was 52.
- Most of the responses were from the age group: from 40 to less than 50 years.
- The number of undergraduates reached 86, which is the highest percentage of all other categories.
- There is a consensus on the importance of cyber security, as the number of those who believe this is 112 out of 124 (50%).
- There are statistical indications in favor of using strong passwords, as well as copying data from time to time to preserve it.
- With regard to the security of dealing with commercial websites, there are statistically significant indicators indicating the lack of security to a large extent, as well as the complete lack of confidence in the confidentiality of data when electronic transactions.

- There is a not insignificant percentage that has been exposed to fraud and fraud during electronic transactions, and their number reached 44 of the total responses, which amounted to 124 responses.
- There are statistically significant indicators in favor of not being exposed to the theft of private accounts, but we find that 26 out of 124 were subjected to these operations.
- As for the impact of the risks of electronic attacks on government agencies and their disruption, there are statistically significant indicators of up to 48% stating yes.
- As for the state's awareness of the importance of cyber security, the results were disappointing, as 60 people acknowledged that the state does this to some extent, and 30 saw that the state did not carry out the necessary awareness.
- There are also statistically significant indicators in the direction that the state has not developed strong legislation related to cyber security, this percentage reached 52%, and the same applies to the application of laws related to cyber security.
- There is a government agency responsible for cyber security, but many people do not know about it.
- There are statistically significant indicators against the existence of investments in the field of cyber security.
- There are no academic programs or curricula in the field of cyber security or support the development of these programs and curricula.
- There are statistically significant indicators that there is no interest in the internal cyber security industry, this percentage reached 62.9%.
- There are statistically significant indicators indicating that there is no interest from the state in educating children about the dangers of electronic attacks, as well as the absence of legislation against these attacks and against the perpetrators. This percentage reached 59.7%.
- The results indicated the danger of electronic attacks, specifically on banking transactions and social networking sites, and confirmed that the accounts of many people were hacked, not for the purposes of stealing personal data, but rather the focus was on electronic attacks aimed at theft.
- There are statistically significant indicators in favor of the existence of social challenges facing cyber security in the country.
- There are also statistically significant indicators in favor of the existence of economic challenges facing cyber security in the country.
- Likewise, there are statistically significant indicators in favor of security challenges facing cyber security in the country.
- There are statistically significant indicators (90.3%) that confirm the lack of awareness of cyber security.

5. RECOMMENDATIONS

Through the results of the questionnaire, as well as by analyzing these results, we can present the most important recommendations through which cyber security can reached to the desired level, which contributes and helps the State of Kuwait to reach various future visions, especially as we live in a digital world, which dealt with in advanced digital methods. However, it has some disadvantages and risks, so the state and its institutions must take into account the following recommendations:

- Training community members to deal with electronic risks.
- Helping individuals reduce the risks arising from hacking into computer devices and networks, which result from their lack of awareness of prevention and protection methods and methods.
- Providing tips that contribute to developing awareness of cyber security to achieve a high degree of safety and protection in this digital world.
- Ensuring the achievement of cyber security and preserving the rights resulting from the legitimate use of computers and information networks.

- Protection of public interest, morals and morals, as well as the national economy as well.
- Legislation must put in place to cover all legal loopholes in the field of a safe cyberspace, or in other words, the development of the national criminal legislative structure with legislative intelligence.
- Amending the rules of criminal procedures to suit those cybercrimes.
- Security, procedural and judicial coordination and international cooperation must be made in the field of combating it by stating the provisions that must be followed in the event of inspection of computers and when seizing the information they contain and seizing e-mails so that the evidence derives its legitimacy.
- Providing a police force that is scientifically, practically and technically capable to face the challenges of combating it, by means of two police officers who are fully trained to deal with these crimes.
- Give sufficient time for investigation and prosecution by specialized police equipped with technical and organizational mechanisms.
- Existing authorities must allowed controlling and investigating e-mail and any other technology that may be useful in proving the crime and obtaining the necessary evidence that reveals the truth.
- Enhancing the protection of operational technology systems, including hardware and software, and the services they provide and the data they contain.
- Strong response to information security attacks and incidents targeting government agencies and public and private sector institutions.
- Work to provide a safe and reliable environment for all transactions in the information society.
- Supporting critical infrastructures to counter cyber-attacks.
- Providing necessary measures and requirements to prevent and limit cybercrime targeting the public.
- Work to get rid of vulnerabilities in computer systems and mobile devices of all kinds.
- Filling all gaps and defects in information security systems.
- Work to resist malware as much as possible.
- Reducing espionage and electronic sabotage at the government and individual levels.
- Guiding and training individuals on modern mechanisms and procedures used to face the challenges of hacking their devices.

6. CONCLUSION

Cyberspace offers huge advantages and opportunities for users, but it also has great threats and risks. It is constantly being exploited by a variety of enemies and aggressors such as: hostile states, political extremists, terrorists, businesses engaged in commercial espionage and theft; also individuals and criminal organizations that engage in financial fraud and trafficking in human beings, weapons and drugs; In addition to the individuals called hackers. Effectively responding to these threats and risks is what cyber security is all about.

The idea that cyber security could have a larger, more overarching goal may seem fanciful to some. However, the threat/response dynamic, while compelling, is certainly not all there is to say about cyber security: cyber security must have a larger goal than pursuit. To achieve a defensive advantage over hackers. If cyberspace can be valued as much as it is feared, then the broader goal of cyber security may not only be to disrupt threats as they emerge, but to enable the positive opportunities offered by the information revolution.

Cyber security must also address the safety, security, and governance of no less than a rapidly evolving and beneficial global digital ecosystem, at every level and in every field of human activity. It is possible and necessary to combine both perspectives—protecting from and advancing toward—in one account, as this global cyber security guide has shown.

Cyber Security is essential in today's digital age to protect individuals, businesses, and critical infrastructure from cyber-attacks. With the increasing dependence on technology, the threat of cyber-attacks will continue to grow. Therefore, individuals, organizations, and governments should take proactive steps to protect against cyber threats and ensure Cyber Security.

Cyber Security is a critical issue that affects individuals, organizations, and governments. With the increasing sophistication of cyber-attacks and the growing dependence on technology, Cyber Security will continue to be a significant challenge. Therefore, it is crucial to implement effective Cyber Security measures, stay up to date with the latest technologies and best practices, and collaborate with others to combat cybercrime and enhance international Cyber Security standards.

ACKNOWLEDGMENT

Finally, I would like to thank everyone who responded to the questionnaire for this research, which contributed greatly to reaching to these results and recommendations.

REFERENCES

[1] Kott,.Towards.fundamental.science.of.cyber.security,.in.Network.Science.and.Cybersecurity,.ed..by.R.E..Pino..Advances.in.Information.Security,.vol..55.(Springer,.New.York,.2014).

[2] Mohaisen,.O..Alrawi,.AV-meter:.an.evaluation.of.antivirus.scans.and.labels,.in.Detection.of.Intrusions.and.Malware,.and.Vulnerability.Assessment.-.11th.International.Conference,.DIMVA.2014,.Proceedings.(2014).

[3] Ramos,.M..Lazar,.R.H..Filho,.J.J.P.C..Rodrigues,.Model-based.quantitative.network.security.metrics:.a.survey..IEEE.Commun..Surv..(2017).

[4] Roque,.K.B..Bush,.C..Degni,.Security.is.about.control:.insights.from.cybernetics,.in.Proceedings.of.the.Symposium.and.Bootcamp.on.the.Science.of.Security,.Pittsburgh,.April.19–21,.2016.

[5] Herley,.P.C.v..Oorschot,.SoK:.science,.security.and.the.elusive.goal.of.security.as.a.scientific.pursuit,.in.2017.IEEE.Symposium.on.Security.and.Privacy.(SP),.May.2017.

[6] Trippel,.D..Lustig,.M..Martonosi,.Meltdownprime.and.spectreprime:.automatically-synthesized.attacks.exploiting.invalidation-based.coherence.protocols..CoRR.(2018)..

[7] D..Mulamba,.I..Ray,.Resilient.reference.monitor.for.distributed.access.control.via.moving.target.defense,.in.Data.and.Applications.Security.and.Privacy.XXXI,.ed..by.G..Livraga,.S..Zhu.(2017).

[8] E.M..Hutchins,.M.J..Cloppert,.R.M..Amin,.Intelligence-driven.computer.network.defense.informed.by.analysis.of.adversary.campaigns.and.intrusion.kill.chains,.in.2011.International.Conference.on.Information.Warfare.and.Security.(2011)

[9] Schneider,.Blueprint.for.a.science.of.cybersecurity..Technical.report,.Cornell.University,.May.2011..

[10] Da,.M..Xu,.S..Xu,.A.new.approach.to.modeling.and.analyzing.security.of.networked.systems,.in.Proceedings.of.the.2014.Symposium.and.Bootcamp.on.the.Science.of.Security.(HotSoS'14).(2014).

[11] George.Mutune.(1/3/2021),."The.Quick.and.Dirty.History.of.Cyber.security",.cyber.expert,.Retrieved.2021.

[12] Homer,.S..Zhang,.X..Ou,.D..Schmidt,.Y..Du,.S..Raj.Rajagopalan,.A..Singhal,.Aggregating.vulnerability.metrics.in.enterprise.networks.using.attack.graphs..J..Comput..Secur..(2013).

[13] J..Leonard,.S..Xu,.R.S..Sandhu,.A.framework.for.understanding.botnets,.in.Proceedings.of.the.Fourth.International.Conference.on.Availability,.Reliability.and.Security,.ARES.(2009).

[14] M..Pendleton,.R..Garcia-Lebron,.J.-H..Cho,.S..Xu,.A.survey.on.systems.security.metrics..ACM.Comput..Surv..(2016)

[15] M.A..Rahman,.E..AlShaer,.R.B..Bobba,.Moving.target.defense.for.hardening.the.security.of.the.power.system.state.estimation,.in.Proceedings.of.the.First.ACM.Workshop.on.Moving.Target.Defense,.MTD.'14.(2014).

[16] Provos,.A.virtual.honeypot.framework,.in.USENIX.Security.Symposium.(2004).

[17] Zheng,.S..Xu,.Fair.and.dynamic.proofs.of.retrievability,.in.First.ACM.Conference.on.Data.and.Application.Security.and.Privacy,.(CODASPY'2011).(2011).

[18] R..Garcia-Lebron,.K..Schweitzer,.R..Bateman,.S..Xu,.A.framework.for.characterizing.the.evolution.of.cyber.attackervictim.relation.graphs,.in.Proceedings.of.IEEE.MILCOM.(2018).

[19] R..Zheng,.W..Lu,.S..Xu,.Active.cyber.defense.dynamics.exhibiting.rich.phenomena,.in.Proceedings.of.the.2015.Symposium.and.Bootcamp.on.the.Science.of.Security. (2015)

[20] S..Xu,.Cybersecurity.dynamics,.in.Proceedings.of.the.Symposium.and.Bootcamp.on.the.Science.of.Security.(2014).

[21] Connell,.D.A..Menascé,.M..Albanese,.Performance.modeling.of.moving.target.defenses,.in.Proceedings.of.the.2017.Workshop.on.Moving.Target.Defense,. MTD.'17.(2017).

[22] Lu,.S..Xu,.X..Yi,.Optimizing.active.cyber.defense.dynamics,.in.Proceedings.of.the.4th.International.Conference.on.Decision.and.Game.Theory.for.Security.(GameSec'13).(2013).

[23] Cheng,.J..Deng,.J..Li,.S..DeLoach,.A..Singhal,.X..Ou,.Metrics.of.security,.in.Cyber.Defense.and.Situational.Awareness,.vol..62.(Springer,.Cham,.2014)

[24] Y..Han,.W..Lu,.S..Xu,.Characterizing.the.power.of.moving.target.defense.via.cyber.epidemic.dynamics,.in.Proceedings.of.the.2014.Symposium.and.Bootcamp.on.the.Science.of.Security.(HotSoS'14).(2014).

[25] Y..Zhao,.Y..Xie,.F..Yu,.Q..Ke,.Y..Yu,.Y..Chen,.E..Gillum,.BotGraph:.large.scale.spamming.botnet.detection,.in.Proc..NSDI'09.(2009).

[26] Z..Zhan,.M..Xu,.S..Xu,.A.characterization.of.cybersecurity.posture.from.network.telescope.data,.in.Proceedings.of.the.6th.International.Conference.on.Trustworthy.Systems.(InTrust'14).(2014).