European Journal of Computer Science and Information Technology
Vol.9, No.4, pp.54-72, 2021
Print ISSN: 2054-0957 (Print),
Online ISSN: 2054-0965 (Online)

UTILIZATION OF SECURITY TECHNIQUES FOR CYBER WARFARE: KSA

Ohoud S. Al-Harthi1*, Osama S. Faragallah2, and Jehad F. Al-Amri3

1Master's degree in cyber security, Saudi Arabia

2Department of Information Technology, College of Computers and information Technology, Taif University, Taif, Saudi Arabia

3Department of Information Technology, College of Computers and information Technology, Taif University, Taif, Saudi Arabia

ABSTRACT: *Cyber warfare is considered mysterious targets of unknown sources that move through information and communication networks worldwide and use electronic weapons targeting information technology. They are directed against vital installations or invaded by agents of the intelligence services. Cybersecurity is one of the most significant digital technological breakthroughs that the world is now witnessing. It is considered the first weapon specialized in defending computers, electronic systems, and data from malicious attacks, servers, mobile devices, and networks. As a result, the goal of this research is to determine how Saudi Arabia uses security approaches for cyber warfare. The study adopted the descriptive method which addressed several aspects related to the strategies and security techniques for cyber warfare. The results indicate that the focus on cyber that pays importance to the possible countermeasures and preventive techniques that could be used to counter the risks of attackers, and discusses the encryption and watermark measures organizations can protect data against the illegal leak and hacking.*

KEYWORDS: cyber warfare, cybersecurity, encryption, watermark.

INTRODUCTION

With the expansion of electronic hostilities into the information infrastructure of countries to achieve interrelated purposes (political, economic, criminal, and others), the concept of electronic warfare carried new dimensions, and some preferred the term “cyberwar”, as an expression of that new trend. The cyber risks increase as the dominance of information and communication technology on the general pattern of life increases, and we are facing real and full-fledged crimes that are carried out through the Internet in various forms, such as theft of money, fraud, planning terrorist operations, spreading misleading news, as well as piracy.

Importance of the topic

The topic of the research discusses the security and strategic studies, which have emerged as a central field in international relations, especially after the end of the Cold War, and the new discussions that have been adopted to expand the concept of security in terms of political, economic, social, cultural, environmental and cyber aspects (Franklin, 2018).

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

The problem of the study

In our digital age, the numbers and risks of cyber threats increase, and their effects and implications vary in the world in general, and Saudi Arabia in particular, as these threats extended to affect various sectors, whether military, political, economic, social, and cultural, thus threatening the national security of countries.

Question of the study

-How security techniques can be used for warfare in Saudi Arabia?

The main question of research has sub-questions include the following:

-How has cyberspace affected the concepts of security, power, conflict, and war?

-What are security techniques for cyber warfare can be used in Saudi Arabia?

-How did Saudi Arabia deal with cyber threats?

LITERATURE REVIEW

This chapter deals with the literature that dealt with national security and cyber warfare and how cyber warfare can affect national security.

Throughout the ages, the great powers sought to dominate and dominate the countries of the world by various means and ways. The information and communication technology are open fields that no one can control their economic, political, media, social, and even military aspects. (Hay & LaFountain, 2016).

Definition of cyber-warfare

Many sources defined cyber warfare, "it is the use of computer technologies to sabotage the activities of a state or organization, particularly prepared attacks on private information systems, for strategic or military purposes."

Cyberwarfare includes sabotage and espionage operations

Sabotage: Computers of the military and financial systems may be at risk of sabotage to disrupt their normal operations and equipment.

Espionage: Illegal methods are used to disrupt the work of spider networks, their computers, and their systems to steal confidential information from the opponent's institutions or individuals and transfer it to the political, military, or financial friend.

In brief, cyber warfare means the operations that take place in cyberspace-software vulnerabilities and malicious programs - using modern technological means to penetrate and direct electronic strikes to a target party or country, which do not focus on killing directly but strikes that cripple the state’s technological movement.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Types of Cyberwarfare

Cyber Cold War: Cold or low-intensity cyber warfare is used in the case of conflicts of a protracted nature, long-term and deep-rooted between countries, and has different cultural, social, or economic aspects.

Cyberwarfare of Medium Intensity: It expresses the transformation of the conflict in cyberspace into an arena similar to conventional wars on the ground, and it may pave the way for real military action, in which websites are hacked, sabotaged, and a psychological war is waged against opponents, and others.

High-intensity Cyber Wars: This pattern specifically expresses wars in cyberspace separately and is not related to aspects or traditional military operations, and it is an advanced type of war that has never been witnessed in the world, despite the possibility of their occurrence in the future, especially with the development of technological capabilities, and the expansion of dependence among countries And entities and individuals on cyberspace. (Hay & LaFountain, 2016).

Cyberwarfare between security and international law

Due to the nature of cyberspace, as a global arena that transcends the borders of states, the issue of cybersecurity extends from within the state to the group of the international system, and with the presence of risks threatening all actors in the global information society, the issue becomes linked to global security.. (Franklin, 2018)

The biggest danger lies in the cyber wars that countries may be exposed to, including armies and cyber teams of unknown origin. The dimension of these attacks is not known. Cybersecurity is not just a national issue, but an individual issue as well.

Electronic combat units

In recent years, some countries of the world have developed the use of the Internet and computer skills as tools of attack, defense, and intelligence warfare. The United States, Britain, France, and South Korea have established special units in their armed forces responsible for electronic or information warfare. These special units combine a military mind with technical skills that enable them to defend and repel attacks or cause losses. On the other hand, the Internet in general, and social media in particular, are increasingly being used as an effective tool in the war waged by armed organizations, especially in the Middle East. According to the report of the Symantec company working in the field of cybersecurity, a copy of the computer virus "Stuxnet" was used to attack and destroy Iran's nuclear program in 2010, in cooperation between the United States and the Israeli entity.

Digital violence between confrontation and privacy

Some analysts believe that “the biggest challenge facing electronic warfare is the opposition of civil society organizations to some of the measures followed by some countries, which lead to a reduction in the freedom of individuals through Internet monitoring, means of communication

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

and messaging, which represents an infringement on the freedom of individuals and the confidentiality of their personal information and privacy. The unconventional nature of these wars requires unconventional solutions or standards for dealing with them. This means that the traditional solutions of strict censorship and blocking the websites and social media accounts of armed organizations and factions, will not achieve great success in this context. Many security Cyber experts have acknowledged the difficulty of this procedure because, for every page, site, or account that closes, dozens of websites will be launched. "(Syed, et al., (2019).

Information or cybersecurity and its implications

An understanding of the logic of the Internet's operation, and its general philosophy, cannot be established without invoking the functions of search engines within the network, as well as their roles and methods of designing them as portals. (Abdyraeva, 2020). Therefore, the problem of information security in this aspect is no longer confined to the companies or institutions involved, to protect their data banks from any targeting but has also become a major challenge facing states and governments. Consequently, the confrontation between security interests and extremist organizations is no longer confined to the real and tangible space, but rather has moved part of it to take from the network as a refuge, and a field for the upcoming hypothetical wars, which we hear echoed for some time, and the interest in electronic security is no longer limited to the technical dimension but bypassed it. In addition to other dimensions of a cultural, social, economic, military, and other nature, the "non-peaceful" use of cyberspace affects the economic prosperity and social stability of all countries whose infrastructure has become dependent on cyberspace.

Previous Studies

Mukherjee, S. (2019) aimed to define cyber warfare and the measures taken by any international organization to attack and attempt to harm the infrastructure, computers, or information systems of another country through computer viruses or denial of service (DOS) attacks. Electronic warfare is also known as the use or effect on the battlefield or war in the background of computers, Internet Control Systems (IoTs), and networks.

Erol & Benzer (2018) discussed how computers and computer systems are important for both military and government issues. The topic of electronic and cyber warfare has become a huge subject of learning to research and debate.

Khan, M. (2019), in his study, aimed to clarify the type of threat that Pakistan faces in the field of electronic warfare and what effective measures should be taken by Pakistan against such threats. This study relies on deductive thinking from the experiences of other countries to chart a way forward in the national e-policy of Pakistan, as Pakistan is already developing at an effective speed in the field of information and communication technology, but it does not attach importance to security aspects, which exposes a major unorganized area of cyberspace. Cyberattacks, which could undermine the national security of Pakistan.

The study of Ibrahim, et al. (2019) aimed to assess the degree of the impact of electronic warfare on national security, with an emphasis on Malaysia's experiences and study of issues

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

linked to electronic warfare that harmed the security of the Malaysian system, and to determine the causes of electronic warfare. Issues related to cyber warfare have become a serious concern as they pose a threat to Malaysia's national security.

Caplan, N. (2013) aimed to analyze the role of China and Iran as two countries that pose cyber threats and to explore the dangers of cyber terrorism. Despite the efforts of the United States Department of Homeland Security, the US Cyber Command Unit, and the FBI, a coordinated policy must be put in place to protect critical infrastructure from cyber-attacks.

White (2016) in his research outlined the importance of understanding the growth of cyber threats and cybersecurity measures imposed by the United States. This research paper will also address the cybersecurity measures that the United States must adopt to reduce and prevent cyberattacks in the future.

Alqurashi et al. (2020) in their study on the impact of the use of the Internet and cybercrime on adolescents has discussed the types of computer crimes which include spam, worms, sniffer, phishing, denial of service attack, and virus dissemination. Spam is a problem. E-mail messages are a critical component. Attempts to defraud are frequently made through hacking, design attacks, and malicious attacks on e-mail systems. To obtain user data, attackers send emails with original content and phishing URLs. The worms, which are computer worms, are designed to spread without warning or user engagement, resulting in an increase in traffic service demands and, ultimately, a cyber-attack. Furthermore, Phishing is the act of attempting to obtain data such as usernames, PINs, and credit card information (and, on rare occasions, money) by posing as a trustworthy object in an electronic broadcast. Phishing via e-mail deception or instant messaging leads victims to a fake website that looks and feels almost identical to the real thing. No additional received TCP impacts can be acknowledged once the board congregation's resources have been depleted. The following figure show relatives and environments of viruses.

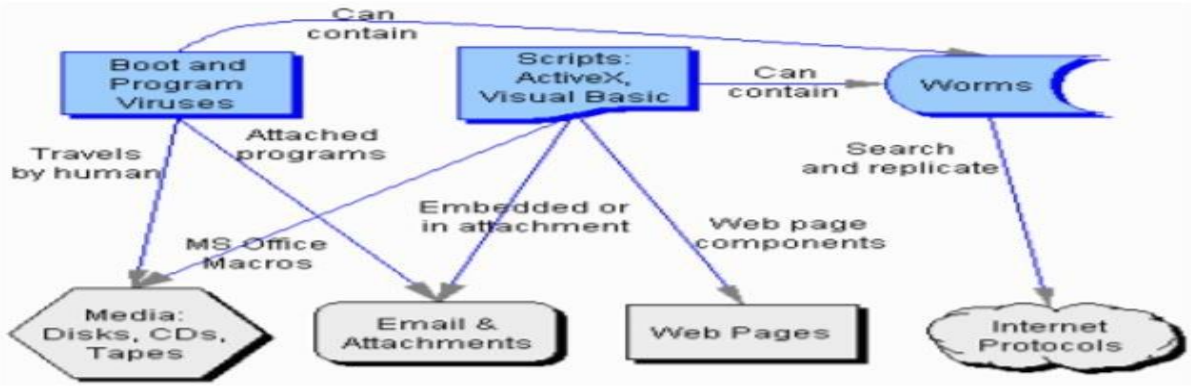

Figure 1 Viruses – Families and Habitats

There's also cyberstalking, which is utilizing the Internet to track down a different person on a regular basis. This irritation could be seen in the landscape, or it could be accompanied by additional interests such as annoyance. People online disseminate a lot of information about

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

themselves. Such information can make one vulnerable to cyber stalking, a term that refers to the use of the Internet to extort money from people (to illegitimately shadow and wristwatch somebody). Furthermore, the purpose of a password attack is to deduce or create a password using trust avoidance techniques, which is known as social engineering. And simple experiences are consumed by password attacks. The majority of password hacks are designed to be deceptive. Admission containers, on the other hand, are prone to theft and destruction. The outbreak must be carefully planned and carried out.

Cyber Attack in Saudi Arabia

In Saudi Arabia, there have been several cyber-attacks, the most notable of which was a cyber-attack on the state oil company Aramco. In August 2012, a virus infected more than 30,000 computers at Saudi oil major Aramco, resulting in the destruction of data and hard drives. (World Exchange Report, 2013), (Al-Arabiya, 2013).

The Anti -Crime Act in Saudi Arabia

Every civilization's backbone is lawmaking. Laws, when combined with an ethical conscience, can lead to a world that is less violent. It is a secure method of establishing civilization and making a country a suitable location to live and interact with others.

Future of Cybercrime

Cybercrime has unpredictable future judging from the trends where the culprits always end up a step ahead of the authorities. (Alqurashi et al.,2020).

Alharbe (2020) in his study the cyber Security, Forensics and Its Impact on Future Challenges in Saudi Arabia Smart Cities: Case Study on the Modern, Urban Planning and Design disclosed the major challenges of maintaining smart cities in Saudi Arabia.

Challenges for Smart Cities SA

Governors of smart cities face a number of issues, including a lack of IT infrastructure, artificial intelligence, cybercrime, fund generation, strategic planning, and limited energy resources, all of which can have negative or positive consequences on the quality of life.

Table 1: Compare the Better Alternative Between Artificial Intelligence and Smart Operations for the Future Challenges for Smart Cities in Saudi Arabia.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Challenges for Smart operations	Frequency of Occurrence %
Cybercrime	28
Limited of Energy Resources	12
Lack of IT Infrastructure	18
Fund Generation	10
Artificial Intelligence	20
Lack of Strategic Plan	10

Intelligence, Cybercrime, Fund Generation, Lack of Strategic Plan, and Limited of Energy Resources. The results indicate the probable threats of smart cities in Saudi Arabia and most frequencies of occurrence in percentage are recorded in table no. 1. Smart cities are the witness of cybercrime that has negative impacts on the survival of normal life with open access data resources, which is one of the major challenges of smart cities, especially in Saudi Arabia. The migration of population from different corner of the world becomes the extra burden for the administrators of a few smart cities in Saudi Arabia that demands a large number of energy resources.

Strategies for Challenges of Smart Cities

The smart city concept not only offers benefits to citizens, but it also comes with a number of obstacles. There is a disconnect between the findings of currently accessible literature and actual corporate and societal needs in terms of future difficulties and effective solutions for overcoming those challenges.

Almulhim et al. (2020) in their study of the cyber-attacks on Saudi Arabia Environment discussed the role of cyberwarfare is increasing and Saudi Arabia has become a major target of Cyber-attacks. This case study of the cyber-attacks on the Saudi environment focused on two specific malware Shamoon and Mamba Ransomware. A data wiping malware attacked the Aramco company, and it succeeded in wiping around 30,000 computers. The working of this virus was, once a computer is infected, the virus compiles a list of all the files on the system and erases them. Finally, the virus makes the system unusable by overwriting the master boot record of the computer. The malware was unique and powerful. It was used to target the Saudi government by extinguishing the national oil company Saudi Aramco. The attackers cited oppression and the AlSaud regime as a reason behind the attack. As per a security advisor to Saudi Aramco, it started by sending phishing mail to the employees. Therefore, the following practices recommended for overcoming future attacks:

They should store a duplicate of their important and valuable data.

Besides, they should always keep their patch levels updated, particularly computers that are accessible through the firewall and host public services as DNS services, mails, and HTTP.

They should impose a strict password policy since complex characters make it harder to crack and is the front-line defense.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Moreover, the Aramco IT department should initiate an alarm system that will alert the IT department once any employee will connect a hard drive to their PCs.

Further, they should provide the users with the lowest level of privilege needed to complete a task and train their employees not to open any email attachment form outsource unless it was expected since they are commonly used to place malware.

Moreover, they should conduct regular scanning of vulnerability on a weekly and daily basis and develop a team to maintain and respond to any incident that may occur with proper tools and procedures.

Nowadays, technology has become a vital part of all sectors since the considerable development of the Saudi Arabia organization, and the most significant project which is NEOM that will be relay on technology.

The study of Dolzhenkova et al (2020) titled the national and International Issues of Cyber Security. The International Telecommunication Union's 2018 Information Society Report shows that the nuclear-armed countries that spend most of them on telecommunications development are the USA and China. There is no data available for Israel and North Korea. Among the nuclear-armed states that have territorial disputes, India and Pakistan pay the most attention; The latter has around 150 nuclear warheads, With such a tiny opening in the number of nuclear weapons, India spends annually on telecommunications production is $30 mln since 2014, Pakistan's annual spending is a little over $4 mln (Figure 2).

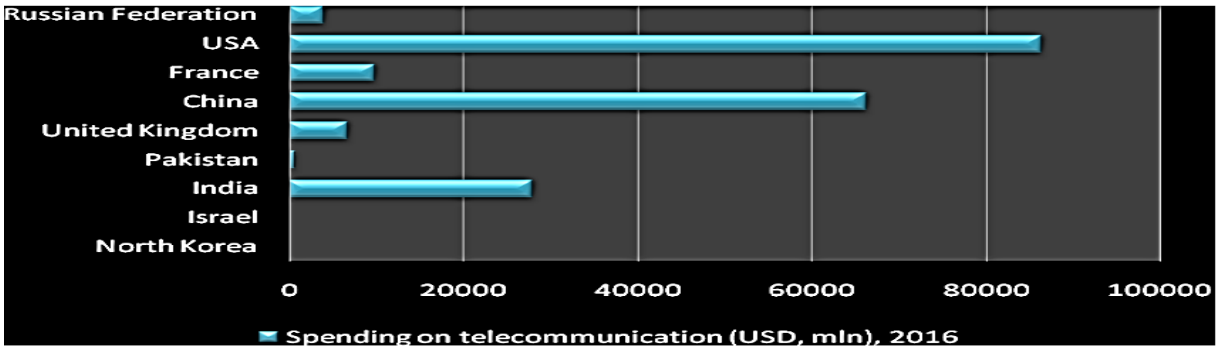

Figure 2 Spending on telecommunications by country (USD, mln), 2016

The study concluded that the country's national security services aim to establish the most efficient means of defending the state's cyberspace against intervention by foreign external organizations, militant entities, infiltrators, and others. Military activity has transcended armed strife. In today's world, the effectiveness of action relies on the ability to wage technological warfare both in the cyberspace of an individual and in the cyberspace of an individual's adversary. In cyberspace, the importance of military personnel's personal knowledge of national security has increased.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Digital improvements are productive with a single boost inefficiency, though they create uncertainty and complexity in the long run.

In the industrial and social industries, leakage of personal data raises the risk of extortion and illegal enrichment through the use of personal data. Hacker attacks, which can inflict damages of millions of dollars to businesses and people, are a cybersecurity threat and have a cross-border criminal nature.

When contemplating the danger to the welfare of all human beings, it is important to remember the nuclear threat that can emerge from a military war between nations but may also arise from terrorism. There is also a possibility of an unintended military confrontation that might lead to a nuclear war. Russia and the United States have been working for five years to avert such a situation.

While the study of Koch & Golling (2019) silent Battles: Towards Unmasking Secret Cyber Threat, cybersecurity firms have been warned on a daily basis that inadequate monitoring protocols may be anticipated in places that record few to no cyber-attacks. In this respect, a glance at the cyber events of recent years shows that the attacks on Distributed Denial-of-Service (DDoS) appear to be used to cover the real intrusion to distract the IT security department. For example, a systematic analysis of DDoS attacks reported by Kaspersky in 2015 reported that "74% of attacks leading to a noticeable denial of service coincided with a different sort of security incident, like malware attacks, network intrusions or other types of attacks." On the other hand, other organizations argue and provide contradictory conclusions from the study of the evidence available to them. Verizon made a satirical analogy with the government to cover up evidence of alien visitation for DDoS assaults involving other violations: it is always heard, but not so straightforward to confirm. Based on their review, "this year's data set had only one infringement involving the DoS, and in that case, the infringement was a corrupted asset used to help launch the DDoS, not the other way around." These essentially different outcomes for the same basic attack vector, namely DoS, demonstrate the difficulty of evaluating the cybersecurity system. Silent Fights in the cyber domain can be followed by a noise like DDoS, but of course, they don't have to be.

The cyber vulnerability must be measured for the execution of the respective decisions. Therefore, a quantitative approach is required. Besides, the programmers have placed in place a matrix that represents the personalized Cyber Kill Chains of each sheet. Characteristics are specified for each layer and stage, which causes a further assessment of another Cyber Kill Chain step and layer, normally moving back in time to the new layer. Sensitivity and threshold values may be adapted for the next assessment stage. Some features trigger further assessments of another step in the current Cyber Kill Chain, or even in the current steps. As the complete range of concepts in the transformation matrix is the cornerstone of the prototype currently being applied, due to restricted space. However, for a deeper understanding of the role and usefulness of the transformation matrix, two examples of associated transformations and behavior are given:

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Adaptation of criteria for the re-evaluation of the IDS logs to detect very sluggish network scans, which usually stay below the identification level. For example, you can think of acts such as "paranoid timing" scanning by the nmap4 network scanner: Nmap-T0, switch the search window from the Distribution Stage back to the Recognition Step. Notice that the results of the assessment are based on a difference in the related conditional probabilities and are not attributable to a simple change in the sensitivity of the analysis, thus they are also not directly apparent in this case. Switch the search window from the Layer 1 Manipulation Stage to the Layer 2 Weaponization Step based on unpredictable device actions or application crashes. Such a transition is visualized by an arrow running from i1/3 to i2/1 in Figure 3, denoting the range of t1,4/2,1, shifting the search window from the Exploitation Stage in Layer 1 to the Weaponization Phase in Layer 2 due to known, irregular, and suspect device actions.

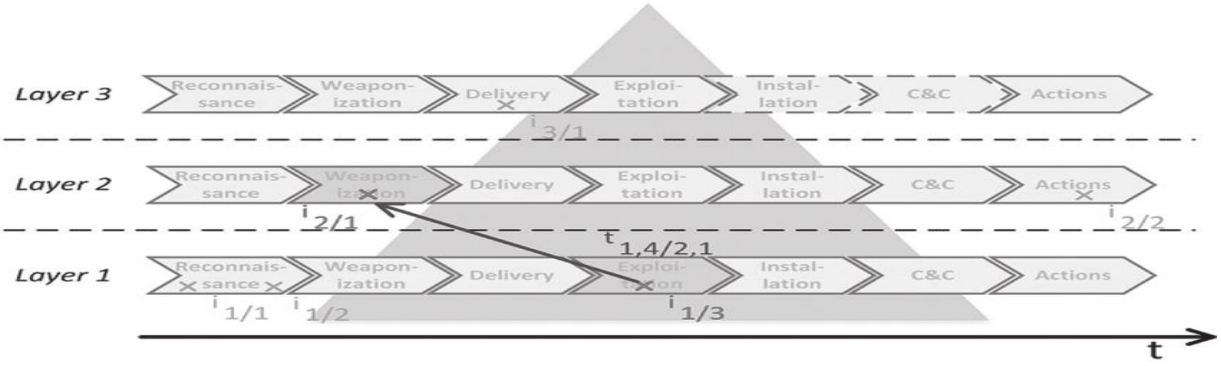

Figure 3 Typical visualization of secret cyber threats. I represent the markers of the respective layer and is combined with the incident number, and (T) represents transformations that pass from one layer to another and are combined with the moves of the respect

The Murino et al. (2019) titled “Resilience of Cyber-Physical Systems: An Empirical Assessment of Quantitative Procedures,” cyber-physical systems connect the physical world with computers and digital networks to automate production and distribution processes. At the present time, most electronic physical systems do not operate in isolation, yet the digital part of them is connected to the Internet to facilitate remote monitoring, control and configuration. In this analysis, the thesis seeks a model-free, quantitative, and general-purpose assessment approach to derive durability indexes from, for example, machine logs and process data.

Finally, Sander (2019) in his study the Sound of Silence: International Law and the Governance of Peacetime Cyber Operations has argued for greater specificity in evaluating the silence of Countries in a cyber context by distinguishing between three different types of security threats in peacetime: cyberattacks, cyber espionage, and cyber information operations. Cyber-attacks and espionage are technical security threats that involve penetrating, communication technologies, and targeting information.

First of all, this paper has highlighted the various aims of state silences. States can remain silent on the allocation of a cyber operation to another State or on the steps taken in response to the operation. State silences often lead to existential issues as to whether or not specific laws fall

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

within the framework of international law or whether or not specific rules of international law extend to specific cyber operations, such as the assessment of the applicability of international human rights commitments of extraterritorial espionage activities.

Second, this paper has shown how the extent of state silences can differ based on the security threat under investigation. In certain peacetime cyber activities, States have become quiet on the applicability of a certain subset of universal legal standards and more outspoken about others.

Finally, this paper has exposed some of the potential rationales that could underpin the silences of States surrounding the applicability and sense of international law in the cyber realm.

Aims and Objectives

The objective of the study is to

Highlight and clarify new concepts in cyberwarfare.

Identify the security techniques for cyber warfare that can be used in Saudi Arabia

Explore the contributions and efforts of Saudi Arabia in confronting cyber threats.

METHODOLOGY

The research methodology is the process that is used in a research process to work out the objectives of the research. In other words, a research methodology explains how the procedure has been undertaken to reach the ultimate conclusion of the study. (Kothari, 2008).

Business organizations are at greater risk of increasing cybercrimes. Hackers are particularly more interested in small business organizations that generally keep their funds in the banks than a single individual and their care for security also lacks in most cases. Easily available toolkits are made use of by the hackers for attacking the computers of such organizations. It has also been obtained that such attack kits are becoming more and more developed in recent years and also have plans to incorporate the Java computer language that can run on almost every operating system and in every browser on the Web. (Haley, 2012).

Need to Protect Sensitive Data

Considering the huge amount of information and details associated either with any personal individual or with business organizations, it can be realized that there is a huge need to protect those data without which this information may be taken advantages of by the hackers or wrongdoers and create damages to the organizations as a whole. Certain measures have been studied that might enable the secured protection of such data, as have been tried to be determined over the years (Top-10 Guide for Protecting Sensitive Data from Malicious Insiders, n.d., p.1). These include:

To secure the information, the process must be known to the individuals taking the responsibility as well as the organizations as a whole.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Native Database tools should not be trusted unless otherwise fully understood about their authenticity.

Effective monitoring processes are necessary to monitor users who are the good, the bad as well as the privileged.

It is also necessary for the responsible individuals to be able to understand what normal activities mean, such that any anomaly can be detected if they exist.

User accountability is essential, and it has been obtained that there are no easy ways to determine the end-user requesting any particular activity.

The augmentation of machines is necessary. Reporting of augments is achievable by two means.

Finally, the most important thing that has been realized is that sensitivity resides within databases. Hence, securing the databases is extremely essential (Top-10 Guide for Protecting Sensitive Data from Malicious Insiders, n.d., pp.2-5).

The advancement of cyber methods has resulted in a situation in which numerous countries attempt to hack into the computer systems of other countries only for the goal of obtaining trade secrets. This has recently been a source of substantial conflict between the United States and China, with the former accusing the latter of stealing trade secrets from numerous American corporations and using them for commercial gain. The United States declared and displayed the photos of those individuals in the Chinese army's cyber warfare unit who were responsible for the hacking, further inflaming tensions between the two countries. It is for this reason that these two countries have in recent weeks traded accusations and counteraccusations to such an extent that despite being each other’s biggest trading partners, the possibility of their continuing their business, as usual, has been somewhat compromised. This has created a situation where each of these countries has chosen to work towards upgrading their cybersecurity to protect themselves against potential attacks; leading to some analysts believing that these countries are preparing for a new form of warfare. Cybersecurity activities involve measures to prevent threats ranging from malicious codes, also known as malware and spyware, to computer viruses. Some of these viruses are so dangerous that they can wipe away whole operating systems of the computers that they attack, essentially erasing all evidence that could lead to the tracking of their creators.

A range of industry-wide efforts has been undertaken that have a build-up to the adoption of DRM.

Software Designed for Securing Information

With the ever-increasing concerns on the security of information and the cyber-attacks, different organizations are coming up with the development of different advanced software intended to protect the information from the attacks of cybercriminals. (Disk Encryption and Data Protection Software, 2011).

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Another such software is the Disk Password Protection 4 that puts forward multifaceted password security tools to guarantee all-inclusive and well-built admission to the defense of one's hard drive and disk partitions. (Disk Encryption and Data Protection Software, 2011).

Reliability and Effectiveness of Data Security

With the increasing amounts of essential and secret information being involved in organizations, the software and the mechanisms used for the protection of information from cyber-attacks must be reliable and effective in their performances. Storage and backup of data is a significant measure that organizations might use for their protection of information. (Leatherman & Dietz, 2007). The backup software proves to be effective in the way they simplify the server backup strategies for an organization's storage of data. Costs are saved in the process that also proves to be beneficial when the process accompanies the protection of data from destruction by cyber-attacks. (Leatherman & Dietz, 2007).

Encryption

Encryption is a certain measure that may prove to be beneficial for preventing cyber-related crimes and help organizations from severe damages of information and data. Encryption systems are generally used to correspond to numeric, alphabetic, and special characters in a computer's internal storage and on the magnetic media. Fixed-size clusters of binary points are used in the process to create the codes. Practicing secure encryption techniques aids in keeping away from most of the defects in the software that might be accountable for causing susceptibility of the software. However, to build up a secure function, encryption techniques only is not adequate. Security needs to be built-in into each stage of the software improvement lifecycle (Shiralkar & Grove, 2009, p.2). Encryption is the knowledge of protecting information. (Network & Information Security, 2012).

Watermark

Watermarks and fingerprints are commonly used to track web content. Watermarks are created by the content creator, while fingerprints are created by the copyrighted work's purchaser

Image Encryption Techniques

Encryption of the image can be described as a method of manipulating a plain image pixel to convert it to an incomprehensible type (Anwar & Meghana, 2019). Image decryption is the reverse method of encryption that extracts the plain image from the encrypted image using a secret key. The following section discusses a number of recently proposed image encryption schemes.

Hamza & Titouna (2016) suggested a cryptographic scheme focused on Zaslavsky chaotic map in the study of Pesin (1977) to encrypt the digital images. The Zaslavsky chaotic map is used as a pseudo-random generator to generate the key encryption of the images; hence their proposed algorithm has a high sensitivity in the plain image and the secret key. The proposed cryptosystem in the study of Hamza & Titouna (2016) consists of two stages. The cryptosystem first uses 2-D chaotic Zaslavsky map to construct the encrypting keys. The 2-D Zaslavsky map

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

is widely used in the development of arbitrary real numbers and its chaotic behavior. As mentioned above, the proposed cryptosystem in the study of Hamza & Titouna (2016) employed the map to produce keys, which they are generated in an iterative procedure. According to the article, the 2-D map is defined as following:

{(x_(n+1)=x_n+v(1+μy_n)+ϵvμ[cos⁡〖2πx_n 〗]mod1@y_(n+1)=e^(-1) [y_n+ε cos⁡〖2πx_n 〗]@μ=(1-e^(-τ))/τ)

, where x_n, y_n are the chaotic samples of this map. x_0, and y_0 are the initial values. ε, τ, and ν are the controlling parameters for regulating the proposed chaotic behavior, and e is the exponentiation. The cryptosystem introduced in the study of Hamza & Titouna (2016) is discussed in depth in the following paragraph. Given the matrix of plain image I with size (h × w), the system encrypts that image as follows. After reading the size of the gray image (h × w), the R, V, V′, alongside α, K, L are generated according to an algorithm that employs the aforementioned 2-D map. Next, the rows and columns of the plain image matrix are shifted according to the elements of V and V′, which then the matrix I2 is computed as: I2 : I ⊕ α. The I2 matrix is separated into [32 × 32] blocks denoted by B, where each rows and columns of each block B are shuffled using the column of matrix R as indexes. The matrix obtained is denoted by I3. The next step is the diffusion processes of the matrix I3 using the matrixes K and L as follows: I4: L • B • K. The matrix I5 is the obtained by shifting the rows and columns of the matrix I4 using the sorts elements V and V′. Finally, the ciphered image (c) is obtained by repeating the aforementioned steps for four rounds.

The size of the key space of the cryptosystem is 〖10〗^255≈2^711, which allows the proposed scheme to overcome exhaustive search attacks. According to their result also, the correlation coefficient of the neighboring pixels in the ciphered images is near to zero.

Li, Y et al. (2017) proposed a hyper chaos-based image encryption algorithm that uses pixel-level transformation and bit-level permutation. The proposed scheme in the study of Li, Y et al. (2017) includes four main processes: the hyper-chaotic system, pixel-level transformation process, bit-level transformation process, and the diffusion process. The adopted chaotic system is a 5-D multi-wing hyper-chaotic system as per Zarei (2015) which is used to produce the chaotic sequence. The generated sequence is relevant to the characteristics of a plain-image as the initial keys of the chaotic system are calculated according to the sum of all pixels in that image. The pixel-level permutation is the next phase of the proposed algorithm. The plain-image 〖(A)〗_(m×n)) in this phase is first converted to one-dimensional vector

P={p_1, p_2, p_2...,p_(m×n)}. Then, the hyper-chaotic system is used to generate a chaotic sequence that has MN elements, L={L_1, L_2, L_3•••,Lm×n}. The last step in the pixel-level permutation includes sorting the chaotic sequence upwards. The sequence L'={ 〖L'〗_1 , 〖L'〗_2•••, 〖L'〗_(m×n) } is then obtained according to the pixel location in the initial sequence. Then the sequence L′ is used to permute the P-positions of the image pixel in which to obtain a shuffled sequence Q={Q_1,Q_2,••,Q_(m×n)}.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

The bit-level permutation is applied after the pixel-level permutation process as follows. First, the aforementioned Q sequence is divided into MN/16 matrices which are 4×4. Then, a new 4×4 matrix is obtained by multiply a constant matrix and a 4×4 matrix. This step is then repeated until MN/16 matrices have performed a round of bit-level permutation procedure. Lastly, the D_(m×n) matrix is obtained by combining MN/16 matrices. The last step in this algorithm is the diffusion process, which normally increases the resistance against statistical attack and differential attack considerably. To accomplish this process, a key stream K is computed according to the value of the L sequence as follow: K_i = mod((abs (L_i) - floor (abs (L_i))) × ⟦10⟧ ^14 ,256). Then, the pixel values of the image matrix D_(m×n) is computed according to the following formulas: C_1 = mod(D_1 + ⟦ C⟧ _0,256) ⊕ mod(Q_1 + K_1,256), and C_i = mod(D_i + C_(i-1),256) ⊕ mod(Q_i + K_i,256).

According to their experimental results, the size of the key space of the hyper-chaotic system is approximately 2273, which makes their system an efficient cryptosystem. Wang et al. (2018) presented a new chaotic image encryption approach that uses Josephus to cross and combine chaotic maps. The proposed approach incorporates three primary processes: the central stream generation process, the three-round scrambling process, and the one-round diffusion process. Wang et al. (2018), a novel approach for calculating initial value X_0 for chaotic maps was also proposed, which in turn improve the security of the cryptosystem. To compute that value, the average of the plain image P denoted δ is calculated according to the following equation: P_(mean)= floor(δ|M × N). Next, the X_01 is calculated as X_01=∑_(i=1)^16▒ ⟦[2^(17-i)/i!×|P_mean-a|+a]/2^25 ⟧ , where a is a control parameter. Then, 16-pixel values P are randomly selected in order to compute the X_02 as follows: X_02=∑_(i=1)^16▒ ⟦P/2^16 ⟧ . Lastly, the X_0 value is computed as X_0=(X_01+X_02)mod1 The second phase of the proposed approach in Wang et al. (2018) is the scrambling, in which the correlations between the value of adjacent pixels are reduced using Josephus traversing; then the rows and columns of pixels are exchanged.

Watermarking Techniques

Image watermarking is the process of embedding an image into another image or simply covering information in some sort of data. The hidden image is commonly known as the watermark and the image in the carrier is usually known as the host (or cover). The following section addresses a variety of newly proposed watermarking schemes for image. Sending and receiving holograms using untrustworthy network systems may result an incorrect 3D restorations and false annotations. Consequently, Chan et al. (2015) proposed novel watermarking algorithm for holograms supporting high vigilance protection. For both embedding and extraction of watermarks, the algorithm is based on Horadam, K. J. (2012) transformation and requires only a few additional operations. The proposed algorithm in Chan et al. (2015) can be divided into three components: the embedding of the watermark, the extraction of the watermark, and the restoration of the host image. The purpose of the watermark embedding phase is to obtain $\bar{H}$ by hiding the watermark W in the host hologram H, where the $\bar{H}$ is used then for the transmission. The watermark embedding includes the following steps. The host hologram (H) is first divided into blocks U_(i,j), after that the

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Hadamard transform is used to obtain the V_(i,j). The C_(i,j) is then computed based on a quantizing procedure using the V_(i,j). The B_(i,j) is then computed by rounding off each pixel of the C_(i,j). Lastly, the H^{-} is obtained as $H^{-} = \{B^{-}\_(i,j) \ ,0,\leq i,j \leq 2\text{^}n \ - 1\}$.

Watermark extraction is the process of obtaining the watermark W^{-}form the hologram H^{-}. The watermark extraction is the inverse procedure of the embedding phase as follows. The $H^{-}$is divided into blocks $B^{-}\_(i,j)$, where the Hadamard transform is applied to the blocks in order to extract the $C^{-}\_(i,j)$. Finally, the $W^{-}$is obtained $W^{-} = \{C^{-}\_(i,j) \ ,0,\leq i,j \leq 2\text{^}n \ - 1\}$. The original hologram H is then extract by basically turning off each pixel of $H^{-}$to 8 bits. According to the experimental findings, the reversibility of the proposed algorithm in Chan et al. (2015) is assured for the resolution stage $m \geq 10$. In a different angle, there is normally quite a lot of pixels in a hologram, and therefore several works have suggested embedding a watermark image into a host hologram. Gray level hologram is commonly used for this application as it only uses one bit for each pixel. Also, Gerchberg–Saxton (GS) algorithm is one of the most common binary hologram generation algorithms. However, it has been shown that the quality of binary Hologram retrieved image embedding is still not sufficient particularly when the GCD Binary Hologram contains noise. Zhuang et al. (2017) therefore proposed an improved approach for inserting a gray-level image into a binary hologram with a high noise tolerance capability.

The Zhuang approach includes the following phases. The Gray-level image is compressed using the well-known JPEG lossy image compression algorithm. Secondly, in order to resist noise contamination, the JPEG data is encoded using Bose–Chaudhuri–Hocquenghem (BCH) as per Lin & Costello (2004) to generate JPEG–BCH code that is able of identifying and fixing bit errors. The next phase is embedding the JPEG–BCH compressed image into a GCD binary hologram. In the embedding phase, a sequence of random locations L that has the same length to the JPEG–BCH coded is generated using a random number generator. Then, each pixel location corresponding to number in L is replaced by the corresponding bit in the JPEG–BCH code. Random sequence L is also used as a watermark retrieval key to retrieve the JPEG–BCH coded bit-stream. Deep learning methods have dominated a lot of fields in recent years by delivering excellent results in different applications and tasks. Ming et al. (2020) suggested a general watermarking method based on deep neural network (DNN) to embed information into a target image. Through theoretical analysis, Ming et al. (2020) have shown that the DNN model is capable of embedding a watermark in an image and it is also an invertible process by which the watermark can be successfully extracted from the image. The DNN model function is assessed by matching the original image with the watermark image, and simultaneously the original watermark with the watermark extracted.

Expected Benefits

This study focuses on cyber and pays importance to the possible countermeasures and preventive techniques that could be used to counter the risks of attackers. As the world is linked by the internet, the possible damage would likely result in a domino effect; damaging and affecting one country after another. This study deals with the technical countermeasures deal with the protection of information security systems and the network system of government

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

organizations. To increase the security of information, government organizations use a firewall system.

The encryption and watermark measures organizations can protect data against illegal leaks. It is a scientific procedure where data and information are encoded in storage media and spread over the internal network. If any unofficial person enters into the network, the encryption makes the stolen information worthless and thus inhibits the misappropriation of information.

References

Abdyraeva, C. (2020). The Use of Cyberspace in the Context of Hybrid Warfare.: Means, Challenges, and Trends (pp. 15-20, Rep.). OIIP - Austrian Institute for International Affairs. DOI:10.2307/resrep25102.7.

Alharbe, M. A. (2020). Cyber Security, Forensics, and Its Impact on Future Challenges in Saudi Arabia Smart Cities. International Journal, 9(2).

Al-Mulhim, R. A., Al-Zamil, L. A., & Al-Dossary, F. M. (2020). Cyber-attacks on Saudi Arabia Environment. International Journal of Computer Networks and Communications Security, 8(3), 26-31.

Alqurashi, R. K., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2020). Cyber Attacks and Impacts: A Case Study in Saudi Arabia. International Journal, 9(1).

Caplan, N. (2013) Cyber War: The Challenge to National Security. Global Security Studies, Winter 2013, Volume 4, Issue 1 93.

Chaikin, D. (2006). "Network Investigations of Cyber Attacks: The Limits of Digital Evidence." Crime, Law, and Social Change 46, no. 4-5: 239.

Clayton, M. (2013) "NSA Cyber Spying on China Not a Surprise, but it's Not Ho-Hum, either." The Christian Science Monitor.

Dolzhenkova, E., Mokhorov, D., & Baranova, T. (2020, September). National and International Issues of Cyber Security. In IOP Conference Series: Materials Science and Engineering (Vol. 940, No. 1, p. 012015). IOP Publishing.

Erol, S. E., Benzer, R. (2018) Electronic Warfare and Cyber Warfare During the Time of Computers. Paper presented at the Fifth International Management Information Systems Conference.

Franklin, A. (2018). An International Cyber Warfare Treaty: Historical Analogies and Future Prospects. Journal of Law & Cyber Warfare, 7(1), 149-164. Retrieved October 9, 2020, from https://www.jstor.org/stable/26777966

Hay, B. & LaFountain, S. (2016). Introduction to the Cyberwarfare: Offensive and Defensive Software Technologies Minitrack. 5560-5560. 10.1109/HICSS.2016.687.

Ibrahim, A., Mahmud, N., Isnin, N., Hazelbella Delilah, D., & Nurfauziah Fauz Delilah, D. (2019). Cyber Warfare Impact on National Security - Malaysia Experiences. KnE Social Sciences, 3(22), 206–224.

Khan, M. (2019) Cyber-Warfare: Implications for the National Security of Pakistan. NDU Journal. P. 100-115.

Kothari, C.R. (2008), Research methodology: methods and techniques, India: New Age International.

Mukherjee, S. (2019). Cyberwarfare and Implications. University of the Cumberland's Chicago, United States.

Syed, R., Khaver, A., & Yasin, M. (2019). Cyber Security: Where Does Pakistan Stand? (pp. 4-5, Rep.). Sustainable Development Policy Institute. doi:10.2307/resrep24376.7

White, J. (2016) Cyber Threats and Cyber Security: National Security Issues, Policy, and Strategies. Global Security Studies, Volume 7, Issue 4.

Koch, R., & Golling, M. (2019, May). Silent Battles: Towards Unmasking Hidden Cyber Attack. In 2019 11th International Conference on Cyber Conflict (CyCon) (Vol. 900, pp. 1-20). IEEE.

Murino, G., Armando, A., & Tacchella, A. (2019, May). Resilience of Cyber-Physical Systems: an Experimental Appraisal of Quantitative Measures. In 2019 11th International Conference on Cyber Conflict (CyCon) (Vol. 900, pp. 1-19). IEEE.

Sander, B. (2019, May). The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations. In 2019 11th International Conference on Cyber Conflict (CyCon) (Vol. 900, pp. 1-21). IEEE.

S. Anwar and S. Meghana (2019). A pixel permutation based image encryption technique using chaotic map. Multimedia tools and applications, vol. 78, no. 19, pp. 27569-27590.

R. Hamza and F. Titouna (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Information Security Journal: A Global Perspective, vol. 25, no. 6, pp. 162-179.

Y. B. Pesin (1977). Characteristic Lyapunov exponents and smooth ergoic theory. Russ. Math. Surveys, vol. 32, pp. 55-114.

Y. Li, C. Wang, and H. Chen (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Optics and Lasers in Engineering, vol. 90, pp. 238-246.

A. Zarei (2015). Complex dynamics in a 5-D hyper-chaotic attractor with four-wing, one equilibrium and multiple chaotic attractors. Nonlinear dynamics, vol. 81, no. 1, pp. 585-605.

X. Wang, X. Zhu, and Y. Zhang (2018). An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access, vol. 6, pp. 23733-23746.

H.-T. Chan, W.-J. Hwang, and C.J. Cheng (2015). Digital hologram authentication using a hadamard-based reversible fragile watermarking algorithm. Journal of display technology, vol. 11, no. 2, pp. 193-203.

K. J. Horadam (2012). Hadamard matrices and their applications. Princeton university press.

Z. Zhuang, S. Jiao, W. Zou, and X. Li (2017). Embedding intensity image into a binary hologram with strong noise resistant capability. Optics Communications, vol. 403, pp. 245-251.

S. Lin and D. J. Costello (2001). Error control coding (no. 4). Prentice Hall.

Y. Ming, W. Ding, Z. Cao, and C.T. Lin (2020). A General Approach for Using Deep Neural Network for Digital Watermarking. arXiv preprint arXiv:2003.12428.

Anwar, S., & Meghana, S. (2019). A pixel permutation based image encryption technique using chaotic map. Multimedia Tools and Applications, 78(4), 27569-27590. doi:10.1007/s11042-019-07852-2

Chan, H., Hwang, W., & Cheng, C. (2015). Digital hologram authentication using a hadamard-based reversible fragile watermarking algorithm. Journal of Display Technology, 11(2), 193-203.

Hamza, R., & Titouna, F. (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Information Security Journal: A Global Perspective, 25(4-6), 162-179. doi:10.1080/19393555.2016.1212954

Horadam, K. J. (2012). Hadamard matrices and their applications (2nd ed.). Princeton, NJ: Princeton University Press.

Li, Y., Ye, R., & Chen, Y. (2017). A Novel Hyper-Chaos-Based Image Encryption Algorithm Using Bit-Level Permutation and Pixel-Level Diffusion. International Journal of Computer Trends and Technology, 62(1), 40-49. doi:10.14445/22312803/ijctt-v62p106

Lin, S., & Costello, D. J. (2004). Error control coding (4th ed.). NJ: Prentice-hall Englewood Cliffs. doi:10.1007/978-1-4615-3998-8_3

Ming, Y., Ding, W., Cao, Z., & Lin, C. (2020). A General Approach for Using Deep Neural Network for Digital Watermarking. Computer Science - ArXiv:2003.12428.

Pesin, Y. B. (1977). Characteristic Lyapunov Exponents And Smooth Ergodic Theory. Russian Mathematical Surveys, 32(4), 55-114. doi:10.1070/rm1977v032n04abeh001639

Zarei, A. (2015). Complex dynamics in a 5-D hyper-chaotic attractor with four-wing, one equilibrium and multiple chaotic attractors. Nonlinear Dynamics, 81(1-2), 586-605.

Wang, X., Zhu, X., & Zhang, Y. (2018). N image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access, 6, 23733-23746. doi:10.1109/ACCESS.2018.2805847

Zhuang, Z., Jiao, S., Zou, W., & Li, X. (2017). Embedding intensity image into a binary hologram with strong noise resistant capability. Optics Communications, 403, 245-251. doi:10.1016/j.optcom.2017.07.028