Sub-Sahara African Academic Research Publications
March, 2023, Editions

JASOR
Journal of Advanced Science and Optimization Research
Vol. 27, No.9, ISSN 2418-9325

CRITICAL REVIEW ON THE EMERGING THREATS, PROSPECTS AND SOLUTIONS TO CYBER SECURITY

AMANNAH, CONSTANCE IZUCHUKWU; AND OFUALAGBA, MAMUYOVWI HELEN
Department of Computer Science, Ignatius Ajuru University of Education, Port Harcourt, Nigeria

ABSTRACT
Cyber security is concerned with preventing illegal usage, invasions, sabotage, and natural catastrophes from affecting information, hardware, and software on the Internet. The aim of the study was to review the emerging threats and prospects in cyber security. The objectives of the study were to; identify the emerging threats in the cyber landscape, identify the prospects in cyber security and recommend measures to mitigate the cases of cybercrime. The method used in the study is the exploratory review. The study exposed seven emerging threats; inn cyber security; Third-Party Exposure, Configuration Mistakes, spyware, ransomware extortion plots, social engineering schemes, phishing scams, and malware attacks. The study also identified six emerging prospects for cyber security; global response to cyber threats, national security implications, corporate cyber security strategies, strategic assessments, operational assessments and tactical assessments. The emerging solution to cyberspace determined in the study were; Multifactor Authentication (MFA), Security Service (SS), Firewall System, Regulatory Requirements, Cloud Computing, and End-user education. The study recommends Firewall and Cloud computing as effective solution measures to emerging threats to Cyber security

Keywords: Critical Review, Emerging, Threats, Prospects, Solutions, Cyber Security

Introduction

It is, in fact, changing socioeconomic activity, security postures, and opening up prospects for innovation and wealth increasing the resources available for better global governance and people's well-being thereby unleashing their individual and national creativity and productivity seamlessly on a global scale (Mbanaso & Dandaura, 2015).

As globalization has changed the way businesses are conducted especially across the Internet, new opportunities are open up for wireless network devices which can be hacked. From the plethora of challenges in the cyberspace there is the need for the review of the emerging threats and prospect in cyber security to insight into the recent trends.

The aim of the study is to review the emerging threats and prospects in cyber security. The objectives of the study are to;

i. identify the emerging threats in the cyber security landscape,
ii. identify the prospects in cyber security and
iii. recommend measures to mitigate the cases of cybercrime

This study is limited to emerging threats in the cyber space. The technique or method used is the explorative review approach.

In this paper we used the exploratory research method which is described as research conducted to address an issue that is not yet well understood. This research method facilitates the process for carrying a deeper comprehensive review on the current trend in personality prediction models using machine learning techniques. Exploratory research is used when a problem needs to be investigated for the first time, it is worthy to note that it does not give a definitive finding but rather an overview of the main ideals to a given research question.

Cybercriminal and attackers are everywhere, from attacks on personal computers of individuals to government institutions and multinationals. This study will be beneficial to the following;

i. Internet users,
ii. Businesses
iii. Multinational corporations,
iv. Research institutes,

v. Government agencies and Parastatals.

Related Literature

Cyberspace is a phrase that has yet to be fully defined and has no geographical boundaries. It is a word linked with the use of the Internet on a global scale. It is sometimes referred to as a virtual space since the physical existence of cyberspace cannot be detected. Cyberspace is defined as "the absolute interconnectivity of human beings through computers and telecommunications regardless of physical geography." William Gibson, a science fiction novelist, created the word "cyberspace" to characterize the entire spectrum of information resources accessible via computer networks. For our purposes, cyberspace is a place in which digital data sent through computer networks facilitates communication and interaction between two people or between a person and a machine. This engagement or conversation can be employed for a variety of reasons. Madahar (2013) posit that the cyberspace is pervasive and unconstrained by boundaries or geography; it pervades most, if not all, civil and military sectors and is difficult, if not impossible, to govern and impose national authority on. It is ethereal and complicated, with many potential to do good as well as bad.

According to the UK Cabinet Office (2011), the flood of innovations brought about by the convergence of information and communication technology (ICT), as well as the changing mobility and social media landscapes, is surely building a new world. Similarly, the fast advancement and sophistication of mobile technology has resulted in a rapid shift in how cyberspace resources are presented and interacted with. Equally, developments in fundamental technologies, which have resulted in lower technological prices, are making global access to the cyberspace more affordable and stress-free. As a result, the population of cyberspace will continue to grow, making it more appealing to all actors and stakeholders. Consequence, there is a transition from the physical world to the virtual world, which is supported by the growth of computers, telecommunications, people's responsiveness, and the quick advancement of auxiliary technologies, such as core electronics.

Furthermore, the 2022 UK Cyber Security Strategy report, also states that exponential breakthroughs in technology combined with lowering prices have made the globe more closely linked than ever before, enabling exceptional potential, innovation, and development. The coronavirus (COVID-19) pandemic has hastened this tendency, but this is most likely still in the early stages of a long-term structural transformation. The worldwide spread of cyberspace is altering how people live, work, and communicate, as well as revolutionizing vital systems on which people rely upon, such as banking, energy, food delivery, healthcare, and transportation. To summarize, cyberspace is now critical to the world's future security and economy (UK Cabinet Office, 2022).

With this rise in the activities of individuals and organisation on the cyberspace for high impact service delivery and the ever increasing traffic and business activities online, there is also a rising need to secure data transmission processes from malevolent user to ensure data integrity as the threat inherent on the cyberspace is also on the increase. Despite the immense advantages in the growth of the cyberspace, there has been consistent attacks on information management systems with the intent to either steal or corrupt information critical to organization. Website and databases (both personal and corporate) attacks occurs frequently at an alarming rate and these attacks and their mode of operation have evolved and are still evolving as the day goes by.

Attacks on information management systems are becoming more sophisticated daily with features involving very high skilled attackers with knowledge about their targets, there is therefore the need for some system to be put in place that could detect those attacks on the databases as they impact heavily on individual, small organization and Multinational Corporation (Shukla & Verma, 2015). With the global nature of web application servers in the sense that they are remotely accessible, it becomes much more vulnerable and easier for malevolent users to launch attacks on the network at different protocol level which include the transport and network layer of the TCP/IP, with additional vulnerability induced by custom web applications designed with little or no consideration to security and privacy concerns which can be utilized by the

attackers to invade and infiltrate network systems security leading to loss of data and disruption of web servers which adversely affects impacts the organizations and their customers (Sher, 2016).

Creating a safer and more secure cyberspace have become one of the critical needs of the industries and individuals in the twenty-first century as cyber criminals have devised novel approach to infiltrating network infrastructures to steal and plunder vital business and personal information (Seemma et al., 2018).

Kalakuntla et al., (2019) refers to cyber security as both the insecurity created by and through the use of the internet and the cyber space, as well as the techniques or processes used to make it progressively safe and secured. It is essentially the security of systems, networks, and data in cyberspace, and it is becoming increasingly important as more people across the world connect to the internet. It addresses not just confidentiality and privacy, but also data availability and integrity, both of which are critical for the quality of service delivery.

With the recent trend of attacks on the internet and the speed at which these attacks are transmitted it is clear that the defence mechanism deployed by organization to protect host computers connected to the internet can easily be compromised and defied. In order to realize an efficient intrusion prevention from these malevolent attacker, there is need for a relative knowledge to be acquired on the pattern of potential attack or threat to the system (Diebold et al., 2005). As networks assets becomes increasingly vulnerable to the speedy growth of the internet, impacts of automated attacks on computer networks have gone beyond the scope of individual host and enterprise, not only infecting these hosts with malicious codes but also denying legitimate users access to network services and resources. Internet worm is one threat that can operate on a network undetected as it blurs the conventional threat detection and makes quarantining very difficult (Bailey et al, 2006).

Researchers and network security professionals have expressed rising worry about how to control, simplify, and possibly eradicate the activities of harmful assaults and attackers on individual and organizational network

infrastructures. To thwart these hostile assaults, network assets must be monitored and protected (Joseph, 2015).

Cyber-attacks and threats may take the following for Farhat (2021);

i. Unauthorized access to a computer system or its data;
ii. Unwanted disruption or denial of service attacks, including the complete shutdown of websites;
iii. Virus or harmful code (malware) installation on a computer system;
iv. Unauthorized access to a computer system for the purpose of processing or storing data;
v. Changes to the hardware, firmware, or software of a computer system without the owner's knowledge, instruction, or agreement;
vi. Workers of former employees making inappropriate use of computer systems.

There are two distinct categories of cyber-attack a computer network, they include

i. Active and
ii. Passive attack,

The following are various countermeasures to this sort of attack, Hassan (2020; Saxena et al., 2012), Wireshark (Hassan, 2020).

i. A random session key that is only valid for one transaction at a time can be produced; this should successfully prevent a malicious user from re-transmitting the original message after the original session has ended.
ii. The use of one-time passwords assists in the authentication of transactions and sessions between communication parties. This ensures that even if an attacker is successful in capturing and retransmitting the intercepted message, the associated password will have expired by that time.
iii. Using the Kerberos authentication system (often found in Microsoft Windows Active Directory), which provides several safeguards against various forms of replay attacks.

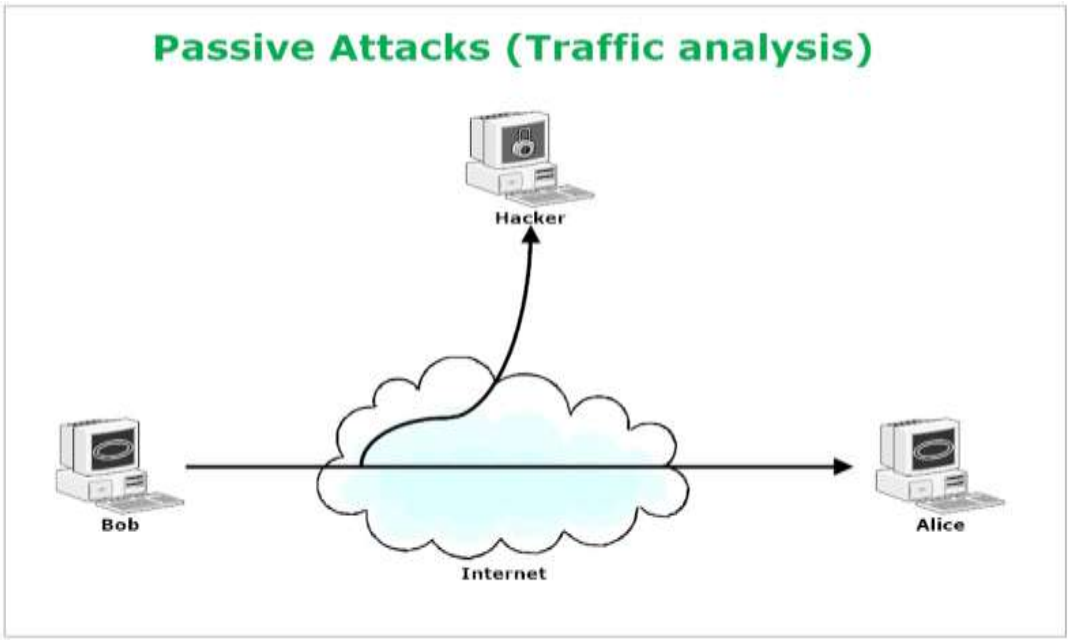

Figure 1: **Passive attack-Traffic analysis (Source: Hassan, 2020)**

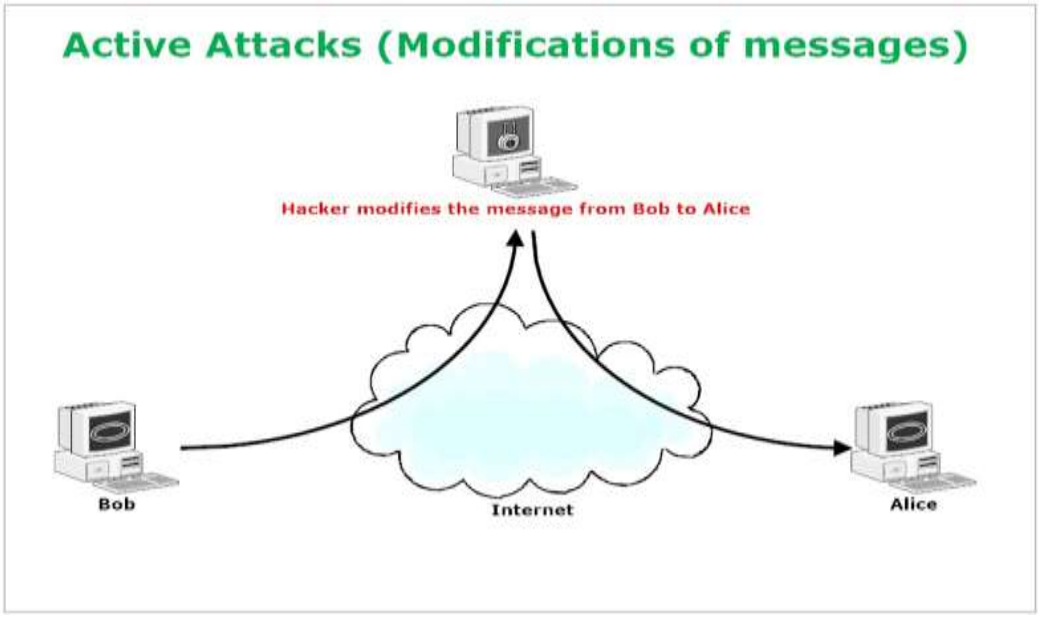

Figure 2**: Illustration of an Active Attack (Source: Hassan, 2020)**

Emerging Cyber Security Threats

The massive number of connected devices objected and individual on the cyber space and the large volume of data and other activities conducted per

second calls for the need to review the cyber security architecture at regular interval. The world of the internet has evolved drastically as people from across the globe carryout huge business transactions virtually with little or no previous knowledge of the person of the other side of the bargain, the risk factor is unimaginable. Irrespective of the level of security deployed in these online transactions, malevolent users and cybercriminal still find their way to swindle unsuspecting members of the society via the cyber space on daily basis. The threat is growing at an alarming rate with more innovation deployed by these cybercriminals to beat the best of cyber security technologies deployed.

Humans and nature are the two principal sources of threats. Human threats are those that are created by humans, such as malevolent threats that include both internal and external threats that seek to harm and disrupt a system. While natural disasters such as earthquakes, hurricanes, floods, and fires can inflict serious damage to computer systems, no one can stop those (Obotivere & Nwaezeigwe, 2020). Moreover, Abi (2020) defined cyber security threat as a malevolent act that aims to harm, steal, or disrupt digital life in general.

Cyber security threats are designed by those who seek to gain unauthorized access to a control system device and network through a data communications channel. This access can be directed from within an organization by trusted people or from remote areas over the Internet by unknown individuals. Control system threats can arise from a variety of sources, including hostile governments, terrorist organizations, disgruntled personnel, and criminal intruders. Cyber security threats can be categorized based on their character, impact, origin, and actor as follows;

1. Accidental or Intentional Threats
2. Active or Passive Threats
3. Origin of Threat
4. Threat Actor
5. Vulnerability

Accidental or Intentional Threats

Accidental threats arise when there is no intentional aim. For example, system or software failures, as well as physical failures. Intentional threats, on the other hand, are the outcome of purposeful activities against an

asset's security. Intentional threats vary from casual network investigation using readily available monitoring tools to complex assaults requiring particular system expertise. Intentional threats that manifest as attack (Bendovsch, 2015).

Active or Passive Threat

Active threats are those that cause a change in the status or functioning of a system, such as data alteration or physical equipment destruction. Passive threats, on the other hand, do not involve a change in the status of the equipment. Passive threats seek information from a system while causing no harm to the system's resources. Eavesdropping, wiretapping, and deep packet analysis or inspections are examples of common passive threat approaches. Passive threats that are successful become passive attacks.

Origin of Cyber Security Threat

The origin of threat might be defined as an entity that seeks to break the security controls of information or physical assets. (Sher, 2016)The main goal of the origin or originator of the cyber security threat is to make financial gain from the cyber security breach that is initiated.

Threat Actors

A cyber security threat actor is a person or entity that carries out the attack or, in the case of an accident, exploits the mishap. For example, if an organized criminal gang corrupts an employee, the organization is the Threat Source, and the employee is the threat actor, (Sher, 2016).

Vulnerability

The origin of threat and the actors' intents frequently manifest as attacks, owing to gaps in security mechanisms. A vulnerability might be a lack of software patching or a faulty setup. Even good technological protections may fail if social engineering assaults trick employees with limited expertise into violating security.

Emerging threats in the cyberspace

Cyberspace is a vast and ever-evolving digital landscape that facilitates communication, exchange of information, and access to services. Unfortunately, with such extensive capabilities, comes the potential for malicious activity and cyber threats. As technology continues to progress and more sensitive data becomes accessible online, it is essential to understand the emerging threats in cyberspace. (Bailey,e tal 2006). This article aims to explore the current and future trends of cyber security risks and discuss strategies for protecting against these threats.

Cyber Threats are one of the most serious security challenges facing businesses today. Cybercriminals are constantly evolving, creating new and more sophisticated ways to exploit weaknesses in digital networks, leading to costly consequences for organizations worldwide. In a world where technology is advancing faster than ever before, it's essential for businesses to stay ahead of emerging threats in cyberspace.

Businesses must be proactive about the threat landscape in order to protect their sensitive data and systems from malicious actors looking to breach them. This includes developing secure networks that can detect potential cyber threats before they become a reality and having access control policies in place, so only allowed personnel can access important information. Training employees on how to avoid falling victim to phishing attacks and other forms of social engineering can help keep businesses safe from cybercriminals.

Types of Malware

Malware is one of the most common forms of cyber threat, and it is a major concern for those who use computers and other devices on the internet. Malware is any software or code that has been created intending to damage, disrupt, or gain unauthorized access to a computer system or network (Obotivere & Nwaezeigwe, 2020). There are many types of malware, each with its own unique purpose and methods for attacking systems. Some of the most commonly seen types include;

Viruses

Viruses are one of the most dangerous and malicious programs that can be found in cyberspace.

These viruses replicate themselves by attaching to existing files or programs in order to spread further and cause potential damage. A virus can destroy important data and can even steal sensitive information from an individual or business.

It is important for users of computers, laptops, and other digital devices to take proactive measures in order to protect their systems from viruses. Installing antivirus software that scans for malicious code regularly is a good way to start. Keeping software up-to-date ensures that they install any new security patches which could help mitigate attacks from known viruses.

Worms

Worms are a type of malicious software that can cause serious damage to networks and devices in cyberspace. They are unique in their ability to spread rapidly, autonomously, and with no user interaction. This makes them a difficult cyber security threat to protect against as they can quickly move through computer systems and networks, allowing them to access confidential data and other sensitive information.

In recent years, the emergence of new technologies has led to the development of more sophisticated worms that can bypass traditional security measures. These threats can be delivered through emails or malicious websites, often with a file attachment containing malicious code which will then launch when opened. Worms also can spread from one device or network to another by exploiting vulnerabilities in an organization's IT infrastructure.

Trojans

Trojans have become an increasingly common threat in the cyber landscape. These malicious programs, also known as malware, are designed to gain unauthorized access to systems and networks without the user knowledge or consent. Once installed on a computer, Trojans can

cause serious damage by stealing data or compromising system performance. It is essential for users to remain vigilant and take steps to protect their systems from Trojan infection.

Trojans are of particular concern as they often masquerade as legitimate software applications that users download from the Internet. Some may appear to be benign files like audio or video clips but in reality contain malicious code that will install itself onto a computer when opened.

Hackers use sophisticated techniques like social engineering and spear phishing attacks to infect computers with Trojans via email attachments or links embedded in emails.

Ransomware

Ransomware is a type of malicious software that has become increasingly common in the Cyber world. It works by encrypting files or data on computers and then demanding payment from victims for the decryption key. Sometimes, even after payment, there's no guarantee that the victim will regain access to their data. They often spread this type of malware through malicious links or downloads, as well as email spam campaigns and vulnerable networks. Ransom-ware is an emerging threat in cyberspace because it can target not only individuals but also organizations and businesses, which can cause major losses for victims because of disruption of service operations or loss of confidential information. (fruhlinger & Hassan 2020). Ransomware attack techniques involve stealing sensitive information before the target system is encrypted.

Spyware.

Spyware is an emerging threat in cyberspace that has been growing in prevalence over recent years. It is software that can be installed on a computer or mobile device without the user knowledge, allowing third parties to collect data from the user without their consent. Cybercriminals can use spyware for malicious purposes such as stealing personal information, monitoring online activity, and even key-logging. Spyware can interfere with system performance by taking up processing power and

memory resources. The danger of spyware lies in its ability to remain undetected and cause serious damage to both businesses and individuals alike. Companies may have confidential data stolen or may suffer financial losses because of unexpected costs associated with spyware removal and data recovery services. Similarly, consumers must also know this threat as it can lead to identity theft, fraud, and other types of cybercrime if left unchecked.

Phishing: Scams and Fraud

Phishing is an ever-growing threat in cyberspace, with scammers and fraudsters targeting unsuspecting victims. With the continuous advancement of technology, it is becoming increasingly difficult to stay ahead of these malicious cyber-criminals. (Seemma et al., 2018) Phishing attacks involve a scammer or fraudster posing as a legitimate business, person, or organization in order to trick people into giving up personal information such as passwords and credit card numbers. This type of attack can cause major financial losses for individuals and businesses alike. Recent reports have shown that phishing activity is on the rise, with many organizations reporting significant increases in phishing emails over the past year. Cyber security experts recommend taking proactive steps to protect yourself from this growing threat by keeping your antivirus software up to date, using strong passwords, and being aware of any suspicious emails or messages that you receive online.

Data Breaches

Data breaches have become an increasingly common occurrence in the digital age, and they pose an important risk to businesses and individuals alike. In recent years, cyber-attacks have grown more sophisticated, with attackers targeting large companies and organizations in order to gain access to sensitive information. As cyberspace continues to expand, so do the emerging threats that come with it. Data breaches can have devastating financial impacts on individuals and businesses alike. Not only can data breaches lead to financial loss due to stolen funds or services, but they can also cause long-term damage by compromising personal data or trade

secrets. (Obotivere & Nwaezeigwe, 2020). Fortunately, there are several steps that both businesses and individuals can take in order to protect themselves against data breaches. Organizations should implement strong security protocols such as two-factor authentication or encryption technologies in order to safeguard their systems from attack.

Social Engineering

Social engineering is a cyber-attack that relies heavily on deception tactics to manipulate users into revealing confidential information or gaining access to the target computer system. This type of attack has become increasingly common as more people use technology, and it is one of the most difficult threats to detect and mitigate in cyberspace. With social engineering, attackers can use techniques such as phishing, baiting, impersonation, tailgating, and pre-texting to target unsuspecting victims. These methods are effective when they appear legitimate so that users feel comfortable providing personal information or clicking on links without being suspicious. By using these deceptive tactics, attackers can gain access to sensitive data or disrupt operations without having to penetrate technical security systems, (UK Cabinet 2022).

Botnets

Botnets are an emerging threat in cyberspace, designed to live undetected and remain hidden from security systems. With social engineering, attackers can use techniques such as phishing, baiting, impersonation, tailgating, and pre-texting to target unsuspecting victims (UK Cabinet 2022) Therefore, it is important for individuals and organizations alike to take steps toward defending their networks against botnets and other threats that exist in cyberspace today.

Crypto-jacking

Crypto-jacking is a new cybercrime trend where hackers use popular mining software to hijack computers and use them to mine cryptocurrency. Miners are rewarded with cryptocurrency for verifying and solving blocks on the block-chain, which is the underlying technology of bitcoin and other

cryptocurrencies. Cryptojacking can slow down a computer, drain its battery, or even consume all of its available processing power. Cryptocurrencies are attractive to criminals because they are relatively easy to mine without being detected. . (UK Cabinet 2022) Mining software is freely available online and doesn't require any special skills or knowledge. Once a miner has installed the mining software on a computer, it will start searching for blocks and trying to solve cryptographic puzzles. If the miner finds a solved block, they will receive rewards in cryptocurrency.

Emerging prospects to Cyber space

The modern internet age has brought about extraordinary advances in technology and communication. However, this new digital world comes with its own set of unique security challenges, known as cyberspace threats. These threats can come from malicious actors such as hackers or even nation-states. They can range from the theft of sensitive data to the disruption of critical networks and services. Fortunately, there are emerging prospects to counter these threats that provide organizations with greater protection and peace of mind. To start, we need a proactive approach to detect and mitigate cyber threats before they cause serious damage. This includes strategies such as Security awareness training for employees will empower them to recognize the signs of a Cyber Attack and respond appropriately.

Global Response to Cyber Threats

The cyber threat landscape has grown exponentially in recent years, with sophisticated attacks now posing a serious threat to businesses, governments, and individuals alike. As the sophistication of such threats rises, so too does the need for effective global responses. This article will examine emerging prospects for responding to cyberspace threats at an international level. There is no single answer to addressing this complex challenge. A comprehensive response needs to come from governments and intergovernmental organizations around the world working together. To ensure effective cooperation between nations, it is essential for all

countries to have a shared understanding of how to approach the issue and what measures are necessary for successful response strategies. International collaborative efforts are being undertaken across multiple disciplines including law enforcement, intelligence sharing, and technology development in order to combat cyber-crime more effectively, (UK Cabinet 2022).

National Security Implications

As our world continues to become increasingly reliant on technology, it is becoming more and more important for organizations to understand the national security implications of emerging cyberspace threats. Over the past decade, cyberspace threats have grown in complexity and magnitude, making them a major security challenge that must be addressed. From nation-state-sponsored Cyber Attacks targeting critical infrastructure to sophisticated ransomware campaigns targeting private sector organizations and individuals, the array of malicious actors operating in cyberspace has never been larger or more diverse. Organizations must take proactive steps to ensure they are aware of current cyber threats and have systems in place to protect against them. . (UK Cabinet 2022).

Corporate Cyber Security Strategies

As the world becomes increasingly more connected, the need for Cyber Security measures to safeguard data and networks has become paramount. The rise of cyberspace threats such as hacking, phishing, Ransomware, and malware has made it necessary for corporations to establish effective strategies to protect their information systems. For corporate entities looking to ensure their operations are secure against these emerging cyber threats, there are some key security solutions that can be implemented.

The first step in establishing a corporate cybersecurity strategy is identifying all assets at risk of attack and understanding the current threat landscape. Companies should then conduct vulnerability assessments to identify any weak spots in their network infrastructure that malicious actors could exploit and develop policies for preventing unauthorized access or data leakage, (UK Cabinet 2022). Companies should consider

implementing multifactor authentication protocols along with strong encryption technologies to prevent unauthorized users from accessing sensitive information stored on their networks.

Emerging Solutions, to cyber-crime in the cyber space

The internet is becoming increasingly vulnerable to cyber threats, with malicious actors working tirelessly to infiltrate users' networks and steal valuable data. . (UK Cabinet 2022) To combat such attacks and keep personal information secure, businesses, and individuals must consider the emerging solutions available.

Multifactor authentication (MFA)

This security measure requires an additional layer of authentication beyond a username and password, such as a text message code or fingerprint scan. MFA makes it far more difficult for hackers to gain access to online accounts, even if they have a user's login information. Firewalls can be set up both at the server level and on individual devices to protect against malicious software from entering internal networks. (UK Cabinet 2022).

Security Service

As technology advances and more of our lives take place online, our need for cyber security also increases. The emergence of new cyberspace threats has put us in a vulnerable position that can only be protected with the help of an efficient and secure security service.

A good security service should provide comprehensive protection from many threats such as malware, phishing, identity theft, malicious coding, and so forth It must also detect any potential problems before they become serious issues. It should be able to monitor user activities and alert when suspicious behaviour is detected so that appropriate steps can be taken to prevent further damage. The best way to ensure a secure environment is by implementing a multi-layered defense system that comprises firewalls, antivirus software, encryption protocols, and other strategies that work

together to protect against various types of cyber threats. (UK Cabinet 2022).

Regulatory Requirements

Regulatory Requirements play a key role in the emerging solutions to cyberspace threats. As security and privacy issues become more complex, governments are introducing stricter regulatory laws that public and private organizations must follow. Such regulations help ensure personal information is kept safe and secure while also protecting against cyber-attackers who seek to gain access to sensitive data. One of the most prominent examples of regulatory requirements is the introduction of the General Data Protection Regulation (GDPR). The European Union introduced this law in 2018 to protect their citizens' data privacy rights and requires organizations on an international level to adhere to stringent standards in protecting user information. (UK Cabinet 2022)

End User Education

End-user education is an essential part of emerging solutions to cyberspace threats. As the world becomes increasingly connected, it is important for all users to be aware of their role in protecting themselves and their networks from malicious actors. End-user education should include awareness about the dangers of phishing attacks and other social engineering tactics, as well as guidance on how to identify malicious websites, emails, links, and downloads. Besides increasing end-user awareness, organizations must also equip their users with the tools they need to detect and prevent cyber security threats. . (UK Cabinet 2022) This can include training on best practices such as using strong passwords and two-factor authentication. Organizations should also provide employees with access to resources such as security software programs and threat intelligence services that can help them stay ahead of potential threats in cyberspace.

Cloud Computing

Cloud computing is an emerging technology that has revolutionized the way businesses handle their IT systems. As organizations are increasingly turning to cloud solutions to increase efficiency and cost savings, they must

also consider the associated cyberspace threats. . (UK Cabinet 2022) Organizations have been leveraging cloud-based services for years, but with the rise of massively distributed systems on the internet, traditional security measures may no longer be sufficient. Newer approaches include identity management that can help protect access control and secure authentication protocols like Open-ID Connect. Enhanced encryption algorithms can provide protection against data breaches or theft. It is important for organizations to monitor usage patterns in order to detect any strange behaviours or malicious activities from inside or outside their network.

Comparative Results of the reviewed cyber security variables
The emerging threats, prospects, and solutions reviewed in this study are summarized in table 1.

Table 1 Comparison of reviewed on the emerging threats, prospect and solution in Cyber Space

S/N	Emerging threats in the Cyber Space	Emerging prospects in the Cyber Space	Emerging solutions to crime in the Cyber Space
1	Ransomware attack techniques involve stealing sensitive information before the target system is encrypted	Global Response to Cyber Threats	Multifactor authentication (MFA) This security measure requires an additional layer of authentication beyond a username and password, such as a text message code or fingerprint scan.
2	Phishing uses technique like email to tacks sensitive information like login credentials, credit card numbers, bank account details by masquerading as a trusted source	National Security Implications to cyber threats	Security Service (SS) should provide comprehensive protection from many threats such as malware, phishing, identity theft, malicious coding, and so forth. It must also detect any potential problems before they become serious issues.

3	Spyware is another threat which is used for malicious purposes such as stealing personal information, monitoring online activity, and even keylogging. Spyware can interfere with system performance by taking up processing power and memory resources.	Corporate Cyber Security Strategies for Cyber threats identifying all assets at risk of attack and understanding the current threat landscape.	Firewall system will block any brute force attacks made on your network and/or systems before it can do any damage, something we can help you with
4	Data breach is a threat that can also cause long-term damage by compromising personal data or trade secrets.	Strategic assessments Inform decision-makers on broad and long-term issues, as well as providing timely warnings of threats.	Regulatory Requirements play a key role in the emerging solutions to cyberspace threats As security and privacy issues become more complex, governments are introducing stricter regulatory laws that public and private organizations must follow.
5	With social engineering, attackers can use techniques such as phishing, baiting, impersonation, tailgating, and pre-texting to target unsuspecting victims	Operational assessments target potential incidents related to events, investigations or activities and provide guidance about how to respond to them	Cloud computing is another solution to increase efficiency and cost savings,
6	Crypto-jacking is a new cybercrime trend where hackers use popular mining software to hijack computers and use them to mine Cryptocurrency.	Tactical assessments are real-time assessments of events, investigations, and activities that provide day-to-day support.	End-user education is an essential part of emerging solutions to cyberspace threats

Summary and Conclusion

With the ever-increasing prevalence of cyberspace threats, it is critical for organizations to take appropriate steps to protect their systems and data. In this paper, we explored some of the emerging threats; this includes spyware, phishing scams, malware attacks, ransomware extortion plots, social engineering schemes, and more. Fortunately, there are emerging prospects to counter these threats that provide organizations with greater protection and peace of mind. Such as; global response to cyber threats, national security implications, corporate cyber security strategies, strategic assessments, operational assessments and tactical assessments We also discussed solutions that can be employed by organizations namely; implementing robust firewalls and antivirus solutions as well as using strong passwords and two-factor authentication systems where possible. While there is no one-size-fits-all solution for protecting against cyber-attacks, a combination of measures can help reduce risk and bolster an organization's security posture. After careful review, the recommends firewall and cloud computing because they take into account the specific needs of an organization while adapting to changing technology trends so that systems remain secure even as new threats emerge.

REFERENCES

Abi, T. (2020). *What is a Cyber Threat?* Retrieved from Up Gaurd: Http://www.upguard.com/blog/cyber threat

Bailey, M, Cooke, E, Watson, D, Jahanian, F & Provos, N. (2006). A Hybrid Honeypot Architecture for Scalable Network Monitoring. *20th Annual Network and Distributed System Security*, (pp. 1-16).

Bendovsch, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *7th International Conference on Financial Criminology* (pp. 24-31). Oxford, UK: Elsevier.

Diebold, P; Hess, A & Schaefer, G. (2005). A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks. *14th Kommunikationin Verteinlten Systemen.* , (pp. 1-26). Kaiserslautern.

Farhat, K. (2021). *Explaining US Cybersecurity Policy Integration Through a National Regime Lens.* Georgia Institute of Technology, School of Public Policy. Georgia: Georgia Institute of Technology.

Fruhlinger, J. (2020). *Ransomware explained: How it works and how to remove it.* Retrieved from CSO online: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Hassan, N. (2020). *What Is an Active Attack vs Passive Attack Using Encryption?* Retrieved from Venafi: https://www.venafi.com/blog/what-active-attack-vs-passive-attack-using-encryption

Joseph, S. (2015). Advanced Honeypot Architecture for Network Threats. *International Journal of Scientific Engineering and Applied Science (IJSEAS), 1(5)., 5*(1), 20-32.

Kalakuntla, R., Vanamala, A.B & Kolipyaka, R.R. (2019). Cyber Security. *HOLISTICA, 10*(2), 115-128.

Madahar, B. (2013). Cyber Defence: Defence and Surveillance Section. *Pan European Networks: Science & Technology, 1*(4), 23-29.

Mbanaso, U.M., & Dandaura, E.S. (2015). The Cyberspace: Redefining A New World. *IOSR Journal of Computer Engineering (IOSR-JCE), 17*(3), 17-24.

Obotivere, B.A & Nwaezeigwe, A.O. (2020). Cyber Security Threats on the Internet and Possible Solutions. *International Journal of Advanced Research in Computer and Communication Engineering, 9*(9), 92-97.

Saxena, P., Kotiyal, B & Goudar, RH. (2012). Cyber Era Approach for Building Awareness in Cyber security for Educational System in India . *International Journal of Information and Education Technology, 2*(2), 45-56.

Seemma, P.S., Nandhini, S & Sowmiya, M. (2018). An Overview of Cyber Security. *International Journal of Advanced Research in Computing and Communication Engineering, 7*(11), 125-128.

Sher, M. (2016). *Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS).* Retrieved from Semantic Scholar: https://www.semanticscholar.org/paper/Security-Threats-and-Solutions-for-Application-of-(-Sher/1db751da37420f25a2029204a5a34d683e7f421f

Shukla, M & Verma, P. (2015). Honeypot: Concepts, Types and Working. *International Journal of Engineering Development and Research, 3*(4), 596-598.

UK Cabinet Office. (2022). *Policy paper on National Cyber Security Strategy 2022*. Retrieved from UK: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

UK Cabinet Office. (2011). *The UK Cyber Security Strategy 2011*. Retrieved from UK Cabinet Office: httpswww.cabinetoffice.gov.uk