Cyber Security

Assistant Teacher. Hiba Salah Mahdi

MSc Computer Science / Baghdad University

Email : habawy.20@gmail.com

General Directorate of Curriculum

Ministry of Education

Abstract:

Cyber security is acknowledged to play a proactive key in the area of evidence systems. Evidence protection became a serious problem in modern day. The vast number of daily cybercrimes is first thing tends to come to mind when considering cyber security. Several governmental and nonprofit entities are taking a number of actions to prevent these cybercrimes. Also, these safety measures, cyber security continues to worry a lot of individuals. The main advancements in cyber security and the results. Cyber terrorism might cost associations billions of dollars in the business sector. Additionally, the essay discusses the components and root causes of cyber terrorism. This study also includes two case studies pertaining to cyber security. It also offers some answers for cyber terrorism and security.

Keywords: (cyber security, electronic terrorism).

الأمن السيبراني

م.م. هبة صلاح مهدي

ماجستير علوم حاسبات / جامعة بغداد

قسم التحضير الطباعي / المديرية العامة للمناهج / وزارة التربية

الملخص:

من المسلم به أن الأمن السيبراني يلعب دورًا استباقيًا في مجال أنظمة الأدلة. أصبحت حماية الأدلة مشكلة خطيرة في العصر الحديث. إن العدد الهائل من الجرائم الإلكترونية اليومية هو أول ما يتبادر إلى الذهن عند التفكير في الأمن السيبراني. تتخذ العديد من الكيانات الحكومية وغير الربحية عددًا من الإجراءات لمنع هذه الجرائم الإلكترونية. أيضًا ، لا تزال تدابير السلامة هذه ، الأمن السيبراني مصدر

قلق للكثير من الأفراد. التطورات الرئيسية في الأمن السيبراني والنتائج. قد يكلف الإرهاب الإلكتروني الجمعيات مليارات الدولارات في قطاع الأعمال. بالإضافة إلى ذلك ، يناقش المقال المكونات والأسباب الجذرية للإرهاب السيبراني. تتضمن هذه الدراسة أيضًا دراستي حالة تتعلقان بالأمن السيبراني. كما يقدم بعض الإجابات عن الإرهاب والأمن السيبراني.

الكلمات المفتاحية: (الأمن السيبراني، الإرهاب الإلكتروني).

Introduction:

The term "cyberspace" has a long and illustrative history. Seven decades ago, the word "cyber" first appeared (Ottis and Lorents 2010). In 1948, Wiener defined "cybernetics" as " interactions between humans (or animals) and a device capable of creating a different environment." In the early 1980s, initially defined cyber space as "a Data abstractions are taken from the banks of each machine in a single system shown graphically" (1984 Gibson). Since then, it has become widely used, especially in study of information systems (Ottis and Lorents 2010). Information security and cyber security are commonly used in the same sentence (Luiijf et al., 2013). Cyber security Copes with protection in both instructional and une- instructional resources through ICT infrastructure, whereas knowledge security works with protection of knowledge as a resource, whether in physical and non-physical shape (von-Solms and van-Niekerk 2013). This distinction appears to be misleading from an knowledge systems perspective when examining the activity of information systems specialists. Which is due to the fact that despite von-Solms and van-Niekerk's (2013) efforts to separate evidence assets from infrastructure, they remain ultimately an essential part of that infrastructure. Information systems are critical to ensuring the smooth operation of dams and power plants in a way similar to how they may be crucial to running a financial organization, as software worm Stuxnet, which was designed to destroy the Iranian nuclear program, plainly demonstrated (Shakarian *et al.* 2013). This distinction appears to be misleading from an information systems perspective when examining the activity of information systems specialists. This is because the information assets von-Solms and van-Niekerk (2013) goal to distinguish of that infrastructure are actually a crucial component of that infrastructure. Information systems are critical to ensuring the smooth operation of dams and power plants in a way similar to how they may be crucial to running a financial organization, as the software worm Stuxnet, which was designed to destroy the Iranian nuclear program, plainly demonstrated (Merriam-Webster, 2016). By using this standard, it becomes obvious which the NCSS aims to address national objectives that have an effect on a nation's industry, government, and civil society. Strong security is necessary of direct and efficient transactions nowadays because more than 61% of industry transactions take place online . Cyber security is becoming a recent concern as a result (Dervojeda, *et. al*., 2014). The scope of cyber security encompasses more than just authenticating data in the IT industry; it also includes other domains, such as cyberspace. Enhancing cyber security and making sure that the necessary data systems are in place are crucial for each country's economic and security success. Making the Internet safer now rests on the strengthening of new management and a legislative strategy (and protecting Internet users). To tackle cybercrime, a comprehensive and secure strategy is needed (Gross *et al.,* 2017). In order to successfully investigate and file charges for cybercrime, law enforcement agencies must be given the right to do so. Specific estimates alone cannot prevent any crime. Several countries and nations have already adopted stringent cyber safety measures to protect the loss of important data. To defend themselves from the increasing number of cyber security threats, each person needs to be equipped for cyber security. Cyber security addresses the security brought through new environment or the methods as well as steps in order to make secure progressively (Kumar and Somani, 2018). It pertains to diversity of specialist and non-specialist procedures and actions that supposed of safeguard the bioelectrical state and the information it stores and communicates from any dangers that can arise. This study aims to combine knowledge that is currently available, a historical overview of cybercrime, and data analysis from a variety to attack that have been extensively reported over previous many years. Based of material examined, we would like to suggest the security measures that companies may take to ensure greater security. These measures would help shield the companies from hacker assaults and offer a cyber security to prevent the risks. Because there are so many different types of cybercrimes that are on the rise, everyone needs to aware of scams as well as the myriad tools and techniques that may be utilized to prevent them. Every business wants to safeguard its important information against hacking. Being hacked can lead to both the loss of personal data and relationship with users in market (Bendovschi, 2015). Cloud services, mobile devices, internet banking, and many other contemporary technologies necessitate stricter security guidelines and improved security practices. The tools and technology all utilized for transactions keep the sensitive and user significant information. It is essential to provide them with the security they require. Every country's top security priority include enhancing cyber security and protecting vital data and infrastructure (Panchanatham, 2015).

1.1 Cyber Security Strategy

The properties of the internet, stakeholder participation, the boundaries of cyberspace, and dynamic advancements all had a role in the establishment of NCSS. Although NCSS should try to maintain transparency and free flow of information on the internet, it should not jeopardize national security (Klimburg, 2012). To develop the NCSS, it is unavoidable that difficulties of economics, culture, and international relations be balanced with values to accessibility and free information flow from the internet (Arsneault *et al.*, 2005). It doesn't take much searching to get a link around cyber security and difficulties of global relations. For instance, it was determined that the previously stated Stuxnet attack was state sponsored by the US and intended to destabilize both Iran's nuclear program and its leadership. Another instance is the tense relationship between Australia and Indonesia in 2013 over Indonesian officials' and their families' phone calls being monitored by Australia's National Security Agency

(Reddick *et al.,* 2015). Countries restrict free information flow do so in an effort to maintain political stability, but they may do so at the expense of the advantages that the information era offers (Arsneault *et al.* 2005). Getting representation from all spheres of society, including the commercial sector, the government, and civil society, is a challenge when establishing a cyber security plan (Luiijf *et al.,* 2013). According to a government's point of view, developing government services has advantages for service delivery and enhancing their capabilities as government (Stier, 2015). The phrase "think globally, act locally" was made popular by civil society's active use of the internet to coordinate action. The Internet is a potentially transformational medium due to its capacity to retain confidentiality and anonymity (Seebruck, 2015), like political activism (Al-Rawi, 2014). The useing of cyber space by the private sector to facilitate electronic transactions encourages commerce, advertisement and banking (Porter 2001). Thus, a cyber security policy must take into account a variety of legitimate uses while ensuring that illicit activity is kept under control (Souza, 2013). Determining the boundaries of cyberspace is a significant obstacle in developing a cyber security plan. Borders are crucial for defining the areas where the law applied (Johnson and Post, 1996). Different sets of boundaries are highlighted depending on the lens being used, and hence, various views of jurisdictions are produced (Motlagh, 2015). Some argue that because there are no actual contacts, cyberspace should be unbounded and unclaimed by anyone (Barlow,1996). Globalization and technology have encouraged a change in how we understand authority and border, moving beyond a simple geographic boundary to include national borders as well (Finklea,2012). To decide the internet jurisprudence, a range of conventional jurisdictions are proposed, includes universal jurisdiction, extraterritorial judicial interpretation, identity jurisdiction, and territorial jurisdiction (Tehrani and Manap, 2013). Due to these diverse interpretations, a crucial part of any cyber security plan is to offer an appropriate framework within which security can be adequately handled. The final obstacle to development a cyber security plan is adapting to changing circumstances. The internet is regarded as a disruptive technology because it is a major enabler of cyberspace (Lyytinen and Rose 2003) that throws to question a number of widely accepted standards in industry, civic society, public policy, and military affairs. It is difficult to come up with a plan to deal with innovation's uncertainty. Making a sound strategy is difficult given the unpredictability of disruptive technology change. Therefore, cyber security policy needs to take into consideration potential developments in the online world.

1.2 Cyber Security Trends

Cyber security is important in the realm of data technology, also the largest problem in the modern day is data security. The primary worry for cyber security is cybercrimes, which are constantly becoming more serious (Samuel and Osman, 2014). Various governments and organizations are making a lot of efforts to stop cybercrimes. In addition, many people continue in case have serious concerns regarding the different cyber security measures. The following are some main trends that affecting cyber security:

1. **Online hosts**

Online app attacks that aim of steal data or transmit malicious still use code of problem, cyber criminals send their code using trustworthy web servers they have purchased. But there is also a severe threat from information-stealing assaults, of which there are many that are covered by the media. Today, there is a greater need to focus on protecting online servers and online applications (Bendovschi, 2015). Web servers are the main entrance point for these thieves to steal information. To prevent being victim of these defilements, one should constantly use a second secure program, especially during important transactions.

2. **Cellular Networks**

There is still a chance that online applications will be attacked to steal data or spread dangerous malware. Cybercriminals use reliable web servers that they have purchased to transmit their code. In any event, attacks aimed at stealing information of which a sizable number receive public attention pose a serious threat. Currently, people should place a more exceptional emphasis on safeguarding both online servers and online apps (Bendovschi, 2015). The primary location where these thieves access information is through online servers. To avoid being a target to these defilements, one should always use an additional security application, especially during crucial encounters.

3. Encryption

It is a method for encoding messages that makes them impossible for programmers to decode. The message is changed become an animated creature that is satisfied with encryption in encryption. The employment of "encryption key," which specifies how the message should be encoded, is a common last step. Encryption earliest possible reference point slope ensures information protection and respectability (Sharma, 2012). Cybersecurity problems increase as encryption usage increases. Encryption is used to protect information shared while journey via systems such as: Internet, , mobile phones, wireless radios, and other devices.

1.3 Advanced persistent threat and focused assaults

The phrase (APT) designates a sizable group in cybercrime malware. Network security features have been available for some time. IPS or web filtering, for instance, have proved essential in differentiating such focused attacks (Bendovschi, 2015). As attackers get more daring and employ more methods, network security should work in concert with other security measures to detect attacks. In order to protect against potential dangers, one must reinstate our security measures. The aforementioned patterns show how cybersecurity is changing on a worldwide scale.

1.4 Social Media's Place in Cybersecurity

Social media has become a significant aspect of some people's life. We make use of it to stay in touch, plan activities, upload their images, the comment of recent occurrences. It has replaced email, the using of phone requires a lot of our time. But, like with anything even online, critical to be aware of the risks.

We make use of it to stay in touch, plan activities, upload our images, and comment on recent occurrences. It has replaced email, and using the phone requires a lot of our time. But, like with anything else online, it's critical to be aware of the risks. There are numerous ways for people to do this, including through the use of social networking sites. Social media allows people to share their thoughts, photographs, workouts, and other areas of their lives (Gross *et al.*, 2017). Whether they are close by or far away, people can provide unexpected insights into the lives of others. Unfortunately, these networks also represent one's personal security as well as PC protection. Academics are increasingly using social media and running the risk of being attacked (Sharma, 2012). Because most individuals routinely use social media sites, they have become a top target for hackers who can easily access utilize accounts to steal crucial information. The organizations must make sure they are as quick to recognize risks as possible, respond more frequently, and avoid any form of rupture. People must therefore take the necessary precautions to prevent the loss of personal data, especially when handling social media. The core in the exact criteria that social media offerings of companies put to the test is people's ability to disseminate information to a group of people numbering in the millions (Cabaj *et al.,* 2018). Social media has the same capacity to spread incorrect information because it allows everyone to share financially sensitive information. It may only be damaging in the same way. Among the escalating risks is the quick transmission of false information via social media. These groups are unable to stop utilizing social media since it is so important to grabbing their attention, despite the fact that it can be used for cybercrimes. They should instead create systems that will alert them to the possibility of fixing prior to any genuine harm being caused by (Dervojeda *et al.,* 2014). In order to reduce dangers, businesses must be aware in this and the importance in data deconstruction, especially of social debates. They should also implement appropriate security measures. To enter into agreements with social media, specific strategies and appropriate solutions must be used.

1.5 Cyber Terrorist attacks

Illegal use of force or cruelty against people with aim of endangering government, its people, or associations, possibly of political or spiteful reasons is referred to as "terrorism" (Samuel and Osman,2014). Cyberterrorism, a form of terrorism enabled by innovation, has replaced the conventional definition of terrorism. They remain crucial issues in the culture of today. Along with slow progress in the battle against terrorism, modern cybercrime attacks are getting more violent and aggressive (Sharma, 2012). This terrorism includes the using of internet in launch to attack the major institutions on which organizations and nations depend totally. Several observational researchers exploratory online have recognized in some aspects and some attacks as cyber terrorism. It was stated (Samuel and Osman, 2014) their hypothetical model, recognize in five groups that a "cyber–terrorism" classification to intention behind the violence, motivation, and commitment to the task at hand when such an occurrence occurs, impact, tools used to commit such assaults and attacks of natural environment, in addition activity plan. Understanding the type of activities that wrongdoers' behavior will allow to know with confidence (Kumar and Somani, 2018). The main element of "cyber terrorism" is motivation behind carrying out an online act of savagery or damage to individuals (Dervojeda *et al.,* 2014) that, related to a few of sections. The cyber world's advantages are used with terrorists around the world as a launchpad for more rare epidemics with powerful motive. As referring from Yunos and Ahmad (2014), a terrorist could cause many considerable harms with use in information and communication technology and subject republic in difficult conditions due of that disruption in essential services. They asserted of "cyberspace terrorism" produces more obliteration and harm through cyberspace than through classical terrorism tactics.

2.1 The "Cyber Terrorism" Effects

Cyberterrorism consider a novel type of cyber threat and attack that can have a variety when used against any countries or organizations, impacts. Following are some effects in cyber terrorism:

1. **Data infringement :**

Thier purpose of cyber terrorism is of destroy information credibility such that can never again to believe, decimating its classification as encroaching of accessibility. Cyber terrorism's increasing rate in penetration into organizations' and countries' information has led to the loss of substantial and crucial information, which is frequently impossible to recover(Sutton, 2017).

2. **The assault on companies:**

Associations may lose billions of dollars as a result of organizational cyber terrorism. The lender's data setup is vulnerable to attack or hacking by terrorists, who would give them access to their accounts, causing them to lose astronomical amounts of money, and ultimately force that bank into collapse (Gade and Reddy, 2014).

3. **Cyber security fatality:**

While saving numerous innocent lives, cyber terrorism also could put many homes in a dangerous scenario that might occasionally result of mental injury to the affected family. "Cyber-terrorism" may, of one manner or another, result in fatalities like significant harms. It has been proven of attacks on networks and computer use, as well as attacks that came forth as a result in numerous explosions in a few airline accidents that occurred around the world and claimed many lives (Cabaj *et al.,* 2018).

2.2 Combating Cyber terrorism

For the purpose of combating cyber terrorism, it is important to be able to safely verify cyberspace. There is an important comparison between cyber security and terrorism both lack equilibrium. Ensuring security in information, data, and correspondence of substantially more challenging than hacking a system. The attacker unavoidably prefers both traditional terrorism and cyberattacks. Because of attacks that the government encourages, the problems are much worse (Cabaj *et al.*,2018). The nations of the world must take steps to make sure that their technological and punitive laws are adequate to address the problems posed by cybercrimes. Governments must make sure that their laws are respected, adequately executed, and cover cybercrimes (Kumar and Somani, 2018). Every firm relies on a sizable cyber resource to function, so it is imperative that every effort is taken to make sure that it is absolutely secure. his includes making certain that data is accessible, private, and accurate. The "cyber terrorist" feedback information of goes beyond records, including communications, web apps and certain essential operating systems (Kumar and Somani, 2018).

Conclusion

Cyber security related with security brought by through this new domain and methods or steps to make it gradually secure. The attempt to legitimize internet must show a clear need for it in order for "information technology" to be properly used by customers. The terrorist in future will win the wars without firing a shot of simply destroying the nation's fundamental substructure if action is not taken to combat the pervasiveness of expansion like a cyber-attack. "Cyber-terrorism" maybe result of fatalities as well as major harms, regardless of who is involved. Even if social media might be used for cybercrimes, these groups are unable to stop using it because that plays a key part in capturing their attention. Numerous innocent resided have been saved as a result of cyber terrorism, which has also caused many homes to deteriorate to the point where it is occasionally causing emotional harm to the impacted families. Cyber terrorism continues to be a major problem in today's society.There is an intriguing comparison between cyber security and terrorism. Securing information, data, and correspondence is substantially more challenging than breaking into a system.

References

- Al-Rawi, A. (2014). "Cyber warriors in the Middle East: The case of the Syrian Electronic Army," Public Relations Review (40:3), Elsevier Inc., pp. 420–428.
- Arsneault, S.; Northrop, A. and Kraemer, K. (2005). "Taking Advantage of the Information Age: Which Countries Benefit?," in Handbook of Public Information SystemsG. D. Garson (ed.) (Second Edi.), Singapore: Taylor and Francis Ltd.
- Barlow, J.(1996). "A Declaration of the Independence of Cyberspace," EFF (available at https://projects.eff.org/~barlow/Declaration-Final.html;retrieved December 5, 2015).
- Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31.
- Cabaj, K.; Kotulski, Z.; Księżopolski, B. and Mazurczyk, W. (2018). Cyber security: trends, issues, and challenges. EURASIP Journal on Information Security.
- Cottim, A.(20080. "Cybercrime , Cyber terrorism and Jurisdiction : An Analysis of Article 22 of the COE Convention on Cybercrime," European Journal of Legal Studies (17:3), pp. 81-103.
- Dervojeda, K.; Verzijl, D.; Nagtegaal, F.; Lengton, M. and Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.
- Finklea, K.(2012). "the Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement.," Journal of Current Issues in Crime and Law Enforcement (5:1/2), pp. 29- 67.
- Gade, N. and Reddy, U. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Retrieved from https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Ch allenges_And_Its_Emerging_Trends_On_Latest_Technologies.
- Gibson, W. (1984). Neuromancer (T. Carr, ed.), New York: Ace Books.

- Gross, M. ; Canetti, D. and Vashdi, D. (2017). Cyber terrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cyber security, 3(1), 49–58.
- Johnson, D. and Post, D. (1996). "Law And Borders: The Rise of Law in Cyberspace," Stanford Law Review (48:5), pp. 1367-1402.
- Klimburg, A. (2012). National Cyber Security Framework Manual The NATO Science for Peace and Security Programme, Tallin: NATO Cooperative Cyber Defence Centre of Excellence (doi: 9789949921119).
- Kumar, S. and Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.
- Luiijf, H.; Besseling, K.; Spoelstra, M. and De Graaf, P. (2013). "Ten national cyber security strategies: A comparison," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 6983 LNCS), pp. 1-17.
- Lyytinen, K. and Rose, G. (2003). "The disruptive nature of information technology innovations: The case of internet computing in systems development organizations," MIS Quarterly: Management Information Systems (27:4), pp. 557–595.
- Merriam-Webster.,(2016)."Definition of Strategy," (available at http://www.merriamwebster.com/dictionary/strategy; retrieved May 17).
- Motlagh, H. (2015). "Border Management of Cyberspace , First Step of Cyber Defense," (5:1), pp. 16–24.
- Ottis, R., and Lorents, P. (2010). "Cyberspace: Definition and Implication," in Proceeding of the 5th International Conference Information Warfare and Security, Ohio, USA: The Air Force Institute of Technology, pp. 267–269.
- Panchanatham, D. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.

- Porter, M.(2001). "Strategy and the Internet," Harvard Business Review (March 2001), pp. 63–78.
- Reddick, C.; Chatfield, A. and Jaramillo, P. (2015). "Public opinion on National Security Agency surveillance programs: A multi-method approach," Government Information Quarterly (32:2), pp. 129-141.
- Samuel, K. and Osman, W. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing, 3(5), pp. 1082-1090.
- Seebruck, R. (2015). "A Typology of Hackers: Classifying Cyber Malfeasance using a Weighted Arc Circumplex Model," Digital Investigation (14:14), Elsevier Ltd, pp. 36–45.
- Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific and Engineering Research, 3(6).
- Stier, S. (2015). "Political determinants of e-government performance revisited: Comparing democracies and autocracies," Government Information Quarterly (32:3), Elsevier Inc., pp. 270–278.
- Sutton, D. (2017). Cyber Security : A Practitioner's Guide. Swindon, UK: BCS, the Chartered Institute for IT.
- Tehrani, P. and Manap, N. (2013). "A rational jurisdiction for cyber terrorism," Computer Law and Security Review (29:6), pp. 689-701.
- Von-Solms, R., and van-Niekerk, J. (2013). "From information security to cyber security," Computers & Security (38), Elsevier Ltd, pp. 97-102.
- Wiener, N. (1948). Cybernetics: Control and Communication in the Animal and the Machin (second edi.), Cambridge, Massachusetss: The M.I.T Press.