International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Comprehensive Analysis on Cyber Security Awareness and Measures for Cyber Espionage

Manasi P. Shirurkar[1], Dr. Minakshi S. Tumsare[2]

Submitted: 07/05/2024 **Revised**: 19/06/2024 **Accepted**: 26/06/2024

Abstract: In today's Modern era, we cannot visualize the world without gadgets. Every sector has moved to digitization and almost everything gets executed through online medium and platforms. As a result, network security becomes vital globally. Routine tasks are executed via network or through online mediums so one cannot ignore cybersecurity. One single security breach can lead to exposing vital information. These breaches leave strong impact and extensive loss occurs in terms of personal, societal, national etc evidence seepage. Hence, cyber security is very essential to protect one's cyber space. This paper will define the need of cyber space protection. It will also focus on the difference between cyber-attacks and cyber threats. Additionally, paper will enlighten on various cyber-attacks with examples that should be known to individuals to understand that such attacks hamper their cyber space. Lastly, paper will broadly discuss the impacts of cyber-attacks in various domains and numerous measures to control them.

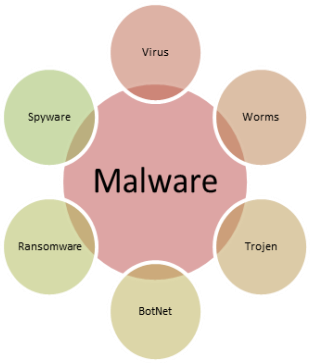
Keywords: *Cyber Attacks, Cyber Espionage, Cyber Security, Cyber Terrorism, Cyber Threats, Cyber War.*

INTRODUCTION:

Network security has become pivotal in this arena of digitization. Securing the network is nothing but securing the cyber space from external factors. Network security, Cyber security are two sides of same coin. Cyber security is the protection of systems, networks and data in cyberspace. The Internet allows users to gather, store, process, and transfer massive amounts of data, including proprietary and sensitive business, transactional, and personal data. As our inevitability on technology and connectivity grows, so does our prospects of vulnerability to cyberattacks increases. At the same time businesses and consumers rely more and more on several mediums, Cybersecurity threats endure to plague the Internet economy. [1][4][6][16] Cyber Threats, Cyber-attacks, Cybersecurity extortions evolve as rapidly as the Internet expands, and the associated risks are becoming increasingly global. These countless methods make us major to have rigorous techniques for guarding cyber space all over. Cyber Security complements major arenas from social networking, Ecommerce, Artificial Intelligence, Data warehouses etc. As a result, cyber security is becoming multifaceted issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses for safeguarding the cyber space.[2][10][23][43]

[1]*Research Scholar MES' Institute of Management and Career Courses (IMCC), Pune*
msu.imcc@mespune.in
[2]*Assistant Professor MES' Institute of Management and Career Courses (IMCC), Pune*
mst.imcc@mespune.in

1. UNDERSTANDING CYBER ATTACKS AND CYBER THREATS:



Cyber-security is the response to the growing threat of cyber-related crimes, and the concept has developed to provide a safe and secure computing environment for all users. While using Internet or while using any form of digital/online platform we are prone to countless cyber-attacks on our cyber space. Cyberspace refers to the virtual computer world, mainly an electronic standard that is used to enable online communication. [11][14][16][17] Cyberspace classically comprises a huge computer network made up of numerous universal computer and subnetworks that aid in communication and data exchange activities. Ensuring that the cyber space of the individual is safe is at most important. Any individual at time of using cyber space are accustomed to cyber-attacks knowingly or unknowingly. [21][25][28].

1.1. CYBER ATTACKS:

Disruption of integrity or authenticity of data or information is termed as computer network attack or cyber-attack. Cyber-attacks are made intentionally with

the motto of destruction/theft of data. [10] Cyber Attacks are mostly targeted intentional attacks. Cyber-attack intents to snip or hack the information of any organization, government offices, sectors, etc . To steal the data or information the attacker or hacker follows certain patterns and achieve their goal. [10][11] Cyber-attacks always aims to disable, disrupt, destroy and many times the intent is to take control of computer systems and alter, block, delete, manipulate or steal the data held within these systems. Negligence to our own systems, data will lead to pruning to attacks.[21]

1.2. CYBER THREATS:

A cyber threat in cybersecurity is a malicious act that pursues to damage data, steal data, or disrupt digital life of the person. Cyber threats can originate from within a group by trusted parties or from remote locations by unknown parties. [15][30][34] The source of the threat may be accidental, environmental (natural disaster or any calamity), human negligence, or human failure too. Cyber threats can be intentional or unintentional. Until the act is analysed and the intent becomes clear, we can't predict the motto behind the attack is intentional or unintentional. The circumstance that has the ability to damage and the attack may or may not be malicious for cyber threats.[18][25]

2. VARIOUS CYBER ATTACKS/THREATS:

Following table describes different types of cyber-attacks with example to understand the variants of types of attacks. [19][20][23][41]

SR. NO.	TYPE OF ATTACK	ENLIGHTENMENT	EXAMPLES
1	Malware	It is malicious software or any program or code that is created with the intent to harm computer, network or server.	a) Trojan b) Worms c) Spyware d) Ransomware
2	Denial of Service	Intrusion into a system by disabling the network with the intent to deny service to authorized users	a) Smurf b) SYN Flood c) DNS attacks d)DDos(Distributed Denial of Services)
3	Phishing	It is a type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information — such as passwords or account numbers — or to download a malicious file that will install viruses on their computer or phone.	a) SMiShing b) Whaling c) Vishing d) Spear Phishing
4	Spoofing	This is a technique through which a cybercriminal masks themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access their systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.	a) Domain Spoofing b) Email Spoofing c) ARP Spoofing
5	Identity-Based Attacks	When a valid user's credentials have been compromised and an opponent is camouflaged as that user, it is often very difficult to differentiate between the user's typical behaviour and that of the hacker using traditional security measures and tools for identity theft management.	a) Brute Force Attack b)Credential Harvesting/Stuffing c) MITM (Man in The Middle Attack) d)Password Spraying
6	Code Injection Attacks	Code injection attacks consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action.	a)SQL Injection b)Cross Site Scripting (XSSS) c) Malvertising
7	Cyber terrorism, Cyberwar	The practice of using cyber space for creating large scale disruption and destruction of life and property of individual or nation.	a) Crashing the power grids by al-Qaeda via a network b) Poisoning of the water supply c) Russia's war on Estonia (2007) d) Russia's war on Georgia (2008)

8	Active Attacks/Passive Attacks	Active attack with data transmission to all parties thus acting as a liaison enabling severe negotiation. Passive Attack is majorly eaves dropping attack.	a) Masquerade b) Reply c) Modification of message d) Traffic Analysis
9	Attacks in MANET	Attacks which goal to slow or stop the drift of information amid the nodes	a) Byzantine Attacks b) Black Hole Attack c) Flood Rushing Attack
10	Network Attacks	A network attack intent to access a network without permission, either to steal or alter data. Network is disturbed and hampered in such cases.	a)Password Based Attacks b) Man in the Middle attack c) Close in Attack

Table1: List of various types of cyber-attacks**.**

3. IMPACTS OF CYBER ATTACKS:

As our conviction on technology and connectivity grows, so does our vulnerability to cyberattacks raises. Breaching cyber security leads to numerous consequences as loss of productivity, revenue, reputation etc are some of the most common risks of cyber-attacks. Following impacts showcase various aspects of cybersecurity attacks:

3.1. SOCIAL IMPACT:

Research in public perception of risk (Slovic, 1998, 2000; Sjöberg, 2000; Dickert, Västfjäll, Mauro & Slovic, 2015) proves that there are potential influences which can affect the public levels such as whether or not exposure to the risk is perceived to be intentional risk or unintentional risk.Some of the incidents happens due to lack of knowledge. This lack of knowledge is called as self-efficacy.[11] Time, cost, money and phycological issues are hampered with these attacks. Another important factor that harms the society is emotional breakdown and behavioural changes. Examples of these are cyberbullying, cyber-crime through online social media hangouts. These types of attacks when occurs on large scale a culture of fear in society urges and as a result convulse the individuals societal, emotional well-being. This in return hazards demographic risks of the nation as well. [12] [13[14][19]

3.2. ORGANIZATIONAL IMPACT:

Economic growth, social aspects are responsible for organizational growth. Different sectors such as private sector, ecommerce, banks, insurance, businesses are prone to vulnerabilities. An effective cyber-attack causes major damage to your business. Startup or a large enterprise business are prone to cyber security threats. People are using online mediums to share significant information; hence cybersecurity should be imparted strictly in businesses. It is a need in today's day and age since a major chunk of our activities are online. Online methods have made our lives easier to survive. Consequently, this has imposed a threat to our private information that might easily leaked. The seepage of such information can stance devastating consequences. In such a condition, the small firms can even go bankrupt by paying price to respond against a cyber-attack. There can be a huge loss of revenue resulting in business disruption. It affects your business' wellbeing, standing, reputation, financial loss and consumer trust, sustaining from which cannot be easier.[22][26][27][28]

3.3. ECONOMIC IMPACT:

The importance of electronic information systems is obvious to all contributors in the modern economy. When circulation of information fails, entire segments of the economy are susceptible. Finance, wholesale and retail trade, transportation, much of manufacturing, and many service industries would sluggish to a crawl without computers. Vivacious public services – utilities, national defence, and medicine – are equally dependent. Information security, safeguarding of computer systems data, the integrity, confidentiality, and availability of the data they contain – has extensively been recognized as a critical national policy issue. To safeguard the nation economy, fruitful steps should be taken to safeguard public and private sectors from the revenue they generate immensely. Cyber terrorism, online extortion is also growing on large scale to hinder nation economy. Major player of economic cyber -attack is the 'banking sector'. Bank servers, ATM machines, bank accounts are hacked mostly for online fraud. Control measures and policy formations should be set up to protect economy. Generators right from public-private sectors, stock markets, insurance, cyber terrorism etc which affects the nation economy globally must strive hard for survival.[15] [16][17][24]

3.4. IMPACT ON GOVERNMENT:

As technology increases amid governments that are involved in international business, criminals have understood that this is a lucrative method to make currency. The greatest fear of a cyberattack on a government entity is the absolute capacity of data that can be lost, ranging from information about individual citizens that can be traded on the dark web, to issues of national security and military data that can be used by terrorist organizations. Government agencies are accountable for mass amounts of complex data to classified information

pertaining to national security. In our data-centric world, information ruins a warm service in dark marketplaces and thus shades a target on its upholders. These attacks endeavours constantly to keep a terror and fear in the state of the art so that government will be busy in solving such issues and the agenda of attack gets successful. [16][22][24]

3.5. IMPACT ON HEALTHCARE:

There have been a number of significant cyber breach incidents in healthcare globally. As healthcare systems across the world is increasingly dependent on digital systems to deliver care of the user, cyber-attacks are also increasingly at a pace. Renowned healthcare attack is the attack made during Covid 19 war for vaccine. These vulnerabilities have been exploited globally during that phase. Some of the common examples were (1) a cyberattack that halted the network of a Czech hospital in March 2020 (2) a ransomware attack on a vaccine trial group in UK in March 2020 (3) an unspecified cyber-attack on the US Health Agency in March, (4) an unspecified cyber-attack on the construction company building the UK's emergency COVID-19 hospitals in May2020. Many online cyber wars were done for vaccine production as well to hinder economic, government and social aspects of the nation. This resulted in significant diagnostic delays that adversely impacted patient care.[11][31][32][33][34]

3.6. IMPACT ON EDUCATION:

Educational institutions are amongst the highest boards for hackers and cybercriminals. Educational establishments are besieged for a numeral of motives, mainly for the volume of individual student data that they hold, moreover with student loan details, confidential research data, and an absence of adequate cybersecurity information with students. The education sector is one of the sluggish adopters of contemporary cybersecurity solutions characteristically due to a lack of funding which can primarily impact the use of out-of-date technology, inadequate resources to invest in cyber solutions, and ever-growing establishment sizes. Research shows that, social engineering being the significant hazard to the education sector. This includes phishing attacks and ransomware attacks. Cybercriminals take advantage of these types of access authorizations to a school or university network. The most common way for them to get such credentials is via a unsecured networks. Cyber-attacks continue to be on the rise and sadly educational institutions are not immune to these threats. Schools, colleges, and universities are increasingly being targeted by cyber criminals, and the consequences can be devastating. [35][36][37]

3.7. IMPACT ON NATIONAL DEFENCE:

Several countries with an elongated history of national struggles exists. Cyber terrorism is the new technique to devastate the national stature. Assigning resources to national defence is vital and also willingness of the country's citizens is important for national security. With the proper understanding and guidance, cyber defence can examine the different threats possible to their environment. It aids in devising and driving the strategies necessary to pledge the malicious attacks or threats. A wide range of different activities are involved in cyber defence for protecting the threat landscape. Cybersecurity is now been practiced in defence services so that the nation cyberspace and territory can be safeguarded.[18][28][30][38][39]

4. MEASURES TO IMPLY TO DEFENSE THE CYBER ESPIONAGE:

In frontline of this digital war against cybercrime, governments, organizations and individuals must create resistance by implementing cyber security measures and best cyber security practices and policies to stay away from cyber-attacks and threats. Some of the measures are summarized from the literature review: [16][21][22][23][29][30][34][38][40][41][42]

1. Always keep the goal of Prevention (PREV), Deterrence (DETER), Surveillance (SURV), Detection (DETECT) of illegal access, alteration, destruction, or disclosure of information assets.
2. Access control, password security, Authentication of data these strategies should be to followed by everyone firmly.
3. Cyber Ethics must be followed while surfing on online platforms/portals/mediums. Cyber ethics are nothing but protocol to use the internet.
4. Keeping strong passwords and changing passwords alternatively so that the rate of hacking and attempt of attack becomes less.
5. All the software used by your system should be updated on regular basis.
6. Good Antivirus protection framework should be implemented in all the sectors.
7. Two level and Three level authentication and authorization process should be applied everywhere.
8. Have an emergency plan of actions reserved in case you are victim of a cyber-attack.
9. Engage in some resolutions of information-security incidents in cooperation with owners and operators of impacted parts, telecommunication operators, internet services providers and government administration components, everywhere there should be a point-to-point connection to help, advice and for protect mechanism.
10. Learn about different scams and vulnerabilities and be prepared for worst.

11. Monitor your activities and focus on good practice of cyber security.
12. Review your online accounts and credit reports regularly.
13. Back up your data frequently.
14. Raise Awareness amongst peers and socially, urge for training programs as well. This will affect in nation building towards robust cyber security approach.
15. Set up a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) for protecting critical infrastructure of the country.
16. Provide fiscal schemes and benefits to businesses for adoption of standard security practices.
17. Encourage wider use of Public Key Infrastructure (PKI) for government services.
18. Engage InfoSec professionals / organizations to assist e-Governance initiatives, establish Centres of Excellence, cyber security concept labs for awareness and skill development through PPP - a common theme across all initiatives mentioned in Cyber Security Policy global standard.
19. Strengthening Promotion of Research and Development in cyber security arena so that secured ecosystem with new strategies/polices can be worked upon and implemented.
20. To develop bilateral and multilateral relationship in the field of cyber security with other country so that the rate of breach/hacking/attacks on international level can be regulated as well as a sense of harmony can be initiated so that global cyber space can be protected.

Conclusion:

Literature review defines cyber security by International Telecommunication Union (ITU) by stating that cyber-security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management methods, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, as well as 'organizations and users' assets (ITU, 2014). This paper overviews the current emerging issues, threats, attacks that cause vulnerability all over. Paper also focuses on various impacts of attacks that disrupt the peace, electric and physical assets of a nation, and cause physical world destruction with economic damage. Paper aims to share measures to incorporate on regular basis for good cyber security practise. It also illustrates the awareness and significance in the field of cyber security. Study summarizes that in cyber security, Malware attacks are most dreadful attacks amongst all types of attacks. In this paper, impacts discussed on several domains' concise focuses on various breaches where we come to know that majorly attacks done on networks are malware attacks or combination of various attacks where malware attack takes a lead for data breach. Aspects discusses in the paper will make aware an individual the importance of cyber security and its significance to keep secured.

References:

[1] THEILER, O.New threats: the cyber-dimension. NATO Review Magazine. 2011. On-line. [accesat: 22.08.2021]. Disponibil: https://www.nato.int/docu/review/2011/11-september/cyber-threads/en/index.htm.

[2] UNDP National Human Development Report Republic of Moldova. 1998. On-line. [accesat: 22.08.2021]Disponibil:www.md.undp.org/content/dam/moldova/docs/Publications/NHDR/NHDR_1998_english_all.pdf.

[3] YAR, M. Cybercrime and Society. Sage Publications. London. United Kingdom. 2006. 558 p.â Eurojust (2011) Eurojust Annual Report 2011. On-line. [accesat: 22.08.2021]. Disponibil:http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202011/Annual-Report-2011-EN.pdf.

[4] WALL, D.Policing Cybercrimes: Situating the Public Police in Networks of Security within the

[5] Cyberspace' Police Practice and Research. An International Journal 2007 On-line. [accesat: 22.08.2021].Disponibil:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=853225.

[6] ALFAWAZ, S. E-government security in developing countries: a managerial conceptual framework', paper presented to International Research Society for Public Management Conference, Queensland University of Technology, Brisbane: 26-28 March 2018.

[7] MOON, M. J. (2000). Organizational Commitment Revisited in New Public Management: Motivation, Organizational Culture, Sector, and Managerial Level. Public Performance & Management Review, 24 (2).

[8] NORRIS, D. F. and Moon, M. J. (2005). Advancing E-Government at the Grassroots: Tortoise or Hare? Public Administration Review, 65-75 (1).

[9] PANKE, D. Small states in the European Union: Structural disadvantages in EU policy-making and counter-strategies. Journal of European Public Policy, 17(6), 2020. 817.

[10] International Journal of Network Security, Vol.15, No.5, PP.390-396, Sept. 2013 390 A Survey on Various Cyber Attacks and Their Classification M. Uma and G. Padmavathi.

[11] Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press The Social and Psychological Impact of Cyber-Attacks Maria Bada etl, Benson & McAlaney (2019/20) Emerging Cyber

Threats and Cognitive Vulnerabilities, Academic Press.

[12] BBC. (2017a). NHS 'robust' after cyber-attack Retrieved July 14 2018, from https://www.bbc.co.uk/news/uk-39909441

[13] Nurse, J. R. C. (2018). Cybercrime and You: How Criminals Attack and the Human Factors that They Seek to Exploit. In Attrill-Smith, A., Fullwood, C. Keep, M. & Kuss, D.J. (Eds.), Oxford Handbook of Cyberpsychology 2nd Edition. Oxford: OUP. https://doi.org/10.1093/oxfordhb/9780198812746.013.35

[14] Introduction to information security and cyber laws-Surya Prakash Tripathi, Ritendra Goel, Praveen Kumar Shukla. ISBN 10: 9351194736

[15] 15.Fundamentals of Cyber Security(Principles, Theory and Practices) ISBN-10. 9789386551559 ,ISBN-13.

[16] Shirurkar, M. P., & Barve, A. A. (2015). CYBER SECURITY: A STUDY BASED ON STANDARDS, AREAS AND STRATEGIES IN INDIA WITH RECOMMENDATIONS FOR MAKING IT MORE OPERATIVE. Advances in Computational Research, 7(1), 209.

[17] 13 March 2020 World Health Organisation (WHO) Creation of a malicious site mimicking the WHO internal email system which aimed to steal employee passwords (https://tech.newstatesman.com/security/who-cyberattack-covid19).

[18] Reardon, R., & Choucri, N. (2012). The role of cyberspace in international relations: A view of the literature. Proceedings of the 2012 ISA Annual Convention, San Diego, CA

[19] CYBER ATTACKS AND ITS DIFFERENT TYPES Jibi Mariam Biju1, Neethu Gopal2, Anju J Prakash3International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 06 Issue: 03 | Mar 2019.

[20] A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks Atul S Choudhary [1], Pankaj P Choudhary [2] etl. in Proceedings of the International Conference on Inventive Computation Technologies (ICICT-2018) DVD Part Number: CFP18F70-DVD; ISBN:978-1-5386-4984.

[21] A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate Ioannis Agrafiotis etl, Journal of Cybersecurity, 2018, 1–15 doi: 10.1093/cybsec/tyy006 Review article.

[22] A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks Atul S Choudhary [1] etl Proceedings of the International Conference on Inventive Computation Technologies (ICICT-2018) DVD Part Number:CFP18F70-DVD; ISBN:978-1-5386-4984-8

[23] Study of Cyber Attacks on Cyber-Physical System Ajeet Singha etl, 3rd International Conference on Advances in Internet of Things and Connected Technologies (ICIoTCT) 2018 ELSEVIER-SSRN INFORMATION SYSTEMS & EBUSINESS NETWORK ISSN: 1556-5068

[24] Decision framework for evaluating the macroeconomic risks and policy impacts of cyber-attacks Andjelka Kelic etl, Springer Science+Business Media New York (2013) DOI 10.1007/s10669-013-9479-9

[25] CRS Report for Congress Received through the CRS Web, Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel Government and Finance Division.

[26] The Impact of Cyber Attacks on E-Businesses 1 Odero Eunice; 2 Bundi Dorothy; 3 Omari Omosa IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 4, August 2019 ISSN (Online) : 2277-5420 www.IJCSN.org Impact Factor: 1.5 354.

[27] PayPal's anti-fraud team, Gengler, B. 2017, ScienceDirect, vol.2002, issue3, (Gengler, 2017).

[28] Saleem, J, Adebisi, B, Ande, R and Hammoudeh, M (2017) A state of the art survey - Impact of cyber attacks on SME's. In: International Conference on Future Networks and Distributed Systems (ICFNDS 2017), 19 July 2017 - 20 July 2017, Cambridge, United Kingdom.

[29] Cyberattacks, cyber threats, and attitudes toward cybersecurity policies Keren L.G. Snider etl, Journal of Cybersecurity, 2021, 1–11 https://doi.org/10.1093/cybsec/tyab019.

[30] KRAUS, J. - NEMEC, V., FAJČIK, P.: The Use of Wireless Sensor Network for Increasing Airport Safety; In: MAD – magazine of Aviation Development, Volume: 1, Issue: 5, September 2013, s.: 16-19; ISSN 1805-7578

[31] Financial consequences of cyber attacks leading to data breaches in healthcare sector Marta Meisner* Copernican Journal of Finance & Accounting e-ISSN 2300-3065 2017, volume 6, issue 3 p-ISSN 2300-1240.

[32] Cybercrime and Other Threats Faced by the Healthcare Industry, http://documents.trendmicro.com/assets/wp/wp-cybercrime-and-other-threatsfaced-by-the-healthcare-industry.pdf (accessed: 06.11.2017).

[33] Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic

Review. Sensors 2021, 21, 5119. https://doi.org/10.3390/s21155119

[34] Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health Authors Ms Menaka Muthuppalaniappan, LLB1 ; Oxford University Press on behalf of International Society for Quality in Health Care 2021

[35] Othman, Z. (2023). Sustainability of higher education institutions: Case study on cyber attacks. Global Business Management Review, 15(1), 24-38. https://doi.org/10.32890/gbmr2023.15.1.2

[36] Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that O'Brien Niki etl, Digital Health Volume 8: 1–3 © The Author(s) 2022 Article reuse guidelines: sagepub.com/journals-permissions DOI: 10.1177/20552076221104665

[37] Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning Alexei Arina, Alexei Anatolie, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VO`LUME 10, ISSUE 03, MARCH 2021 ISSN 2277-8616 128 IJSTR©2021 www.ijstr.org.

[38] 38. Azian Ibrahim, Noorfadhleen Mahmud, Nadrawina Isnin, Dina Hazelbella Dillah, and Dayang Nurfauziah Fauz Dillah, (2019), "Cyber Warfare Impact to National Security - Malaysia Experiences" in FGIC 2nd Conference on Governance and Integrity 2019, KnE Social Sciences, pages 206–224. DOI 10.18502/kss.v3i22.5052

[39] Darko Galinec, Darko Možnik & Boris Guberina (2017) Cybersecurity and cyber defence: national level strategic approach, Automatika, 58:3, 273-286, DOI: 10.1080/00051144.2017.1407022

[40] Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. American Journal of Science, Engineering and Technology. Vol. 3, No. 6, 2022, pp. 12-19

[41] K. M Rajasekharaiah *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* 981 022062, DOI:10.1088/1757-899X/981/2/022062

[42] Security strategies to overcome cyber measures, factors and barriers, L Jawad Hussain Awan etl, ENGINEERING SCIENCE AND TECHNOLOGY INTERNATIONAL RESEARCH JOURNAL, VOL.1, NO.1, APR, 2017.

[43] Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin & Hamdullah Nejat Basim (2020): Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1712269.