iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35455

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

A Research on Cyber Security And Cyber Coercion

Ganraj Rajendra Dol[1], Prof. Anil V. Nikam[2]
[1]*Student, MCA-SEM VI, Faculty* [2]*Research Guide, Department of Computer Application, YM Institute of Management, Karad*

Abstract: ***Cyber Security accepts an active role within the space of data technology. Safeguarding the knowledge has become a vast downside within the current day. The cyber security the most issue that originates in mind is 'cyber crimes' that are combination colossally daily. completely different governments and organizations are taking various measures to stay these cyber wrongdoings. aside from completely different measures cyber security is until now a major worry to several. This paper principally emphases on cyber security and cyber coercion. the numerous trends of cyber security and also the consequence of cyber security discuss in it. The act of terrorism might build associations lose billions of bucks within the region of organizations. The paper conjointly explains the parts of cyber coercion and motivation of it. 2 case studies associated with cyber security conjointly offer during this paper. Some answer concerning cyber security and cyber coercion conjointly justify in it.***
Keywords: Cyber security; cyberspace; cyber terrorism; Information security

I. INTRODUCTION

Today a private will receive and send any data could also be video, or Associate in Nursing email or solely through the clicking of a however ton but did s/he ever chew over however safe this data transmitted to a different individual powerfully with no spillage of data? the right response lies in cyber security. nowadays over sixty one of full business exchanges are done on the web, therefore this space requirement top quality of security for direct and best exchanges. Thus, cyber security has become a most up-to-date issue. The extent of cyber security doesn't just limit to confirmative the info in IT business nevertheless additionally to totally different fields like computer network so forth. rising cyber security and guaranteeing that necessary information systems are important to every country's security and monetary prosperity. Creating the net safer (and safeguarding web clients) has become to be essential to the development of latest management even as a legislative strategy. The encounter against crime desires an intensive and safer observe. the actual estimates alone cannot keep any crime; it's essential that law authorization offices square measure allowable to investigation and charge crime expeditiously. these days various countries and administrations square measure compelling strict rules on cyber safeties to stay the loss of some very important knowledge. every ought to be equipped on this cyber security and save themselves from these increasing cybercrimes. Cyber-security is each regarding the insecurity created by and thru this new house and regarding the practices or procedures to form it (progressively) secure It alludes to heaps of exercises and measures, each specialized and non-specialized, expected to make sure the bioelectrical condition and also the info it contains and transports from all attainable threats. This analysis aims to collect all knowledge} and summary associated with cyber-crime and supply the historical facts and perform reports on the analyzed data of various attacks according everyplace within the last 5 years. supported the analyzed info, we might wish to offer all the countermeasures that organizations could undertake so as to make sure improved security that may support in defensive the organizations from being attacked by the hackers and supply a cyber-security to avoid all risks.

II. TRENDS OF CYBER SECURITY

Cyber Security assumes a important role within the space of information technology. Safeguarding the info became the best issue within the current day. The cyber security the most issue that raids a chord is cybercrimes that area unit increasing hugely step by step . completely different administrations and organizations area unit taking several measures to stay these cybercrimes. further the various measures cyber security is until now a massive worry to varied. Some main trends that area unit dynamical cyber security provide as follows:

A. Web Server

The risk of assaults on net applications to separate data or to flow into malicious code perseveres. Cyber criminals convey their code victimization smart net servers they need listed off. In any case, data taking attacks, a substantial ton of that get the deliberation of media, are a big risk. Currently, people would like a strange accentuation on securing net servers moreover as net applications . net servers square measure primarily the pre-eminent stage for these cyber criminals to require the knowledge. Thus, one ought to faithfully utilize a further secure program, primarily amid very important exchanges all at once to not fall as a quarry for these dirtiness.

B. Mobile Networks

The risk of assaults on internet applications to separate data or to flow into malicious code perseveres. Cybercriminals convey their code exploitation sensible internet servers they need listed off. In any case, data taking attacks, a substantial ton of that get the deliberation of media, are a big risk. Currently, people want a more odd accentuation on securing internet servers moreover as internet applications. internet servers area unit in the main the pre-eminent stage for these cybercriminals to require the knowledge. Thus, one ought to dependably utilize a further secure program, in the main amid very important exchanges all at once to not fall as a quarry for these defilements.

C. Encryption

It is the tactic toward cryptography messages thus programmers cannot scrutinize it. In encoding, the message is encoded by encoding, dynamical it into a stirred-up figure content. It usually completes with the utilization of associate "encryption key," that demonstrates however the message is to inscribe. encoding at the earliest indicator level secures data protection and its honorableness . further use of encoding obtains additional issues in cyber security. encoding is employed to make sure the knowledge in travel, as an example, the knowledge being changed exploitation systems (for example the net, on-line business), mobile phones, wireless radios and then on.

D. ADP's and Targeted Attacks

Advanced Persistent Threat (APT) may be a whole of the dimension of cyber crime ware. For quite an while network security capacities. for instance, IPS or internet filtering have had a key influence in characteristic such focused-on assaults . As attackers become bolder and utilize progressively dubious ways, network security should incorporate with different security advantages to spot assaults. Thus, one should recover our security procedures to counteract a lot of dangers returning in a while. later the higher than may be a portion of the patterns dynamic the essence of cyber security on the world. the highest network threats area unit showing in figure one

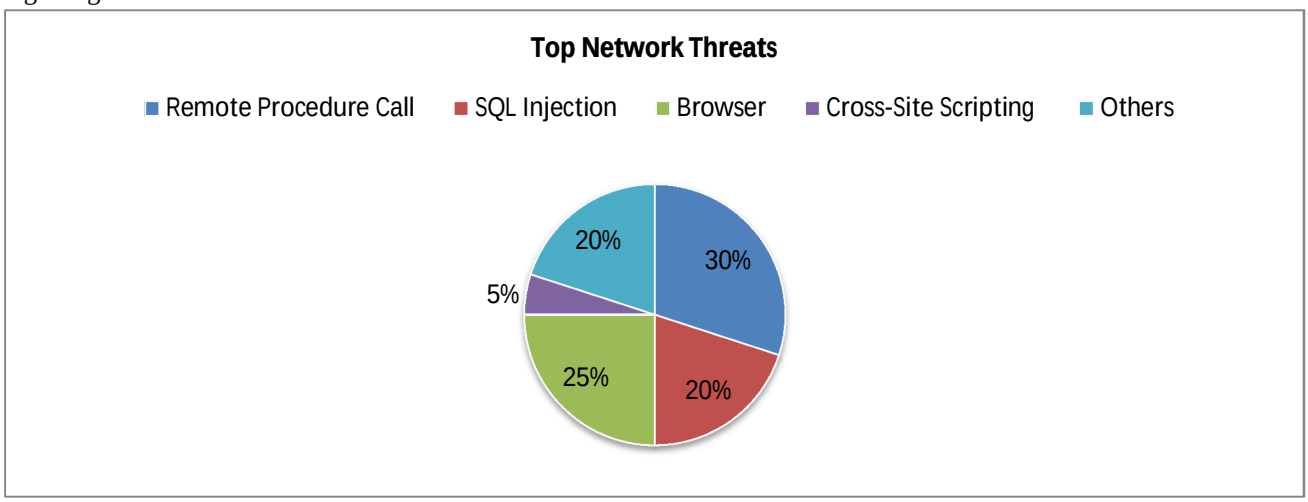


Fig -1

III. SOCIAL MEDIA IN CYBER SECURITY

Social media has become a way of life for a few people. we tend to use it to remain in grips, set up occasions, share our images and discuss recent developments. it's replaced email and phone needs a large amount folks. However, equally like no matter else on the online, it's imperative to grasp regarding the risks. PCs, cell phones, and completely different gadgets area unit valuable assets that furnish individuals of any age with the extraordinary capability to attach and collaborate with no matter remains of the planet. people will try this in numerous ways that, together with the employment of social media or networking sites.

Courtesy of social media, individuals will share musings, pictures, exercises, or any a part of their lives. they'll bring AN unknown explore the lives of others, in spite of whether or not they live near or over the world. sadly, these networks to boot represent security toward one's laptop, protection, and even their security. Social media assortment among school is soaring as is that the risk of assault (Sharma, 2012). Since social media sites area unit nearly used by the bulk of them faithfully, it's become a wonderful stage for cybercriminals for hacking personal knowledge and taking important knowledge.

IV. CYBER TERRORISM

The term cyberterrorism refers to the use of the Internet in order to perform violent actions that either threaten or result in serious bodily harm or even loss of life. Cyberterrorism acts often aim to achieve political or ideological advantages by means of intimidation, fear and threat. Sometimes**,** the definition of cyberterrorism expands to cover the terrorist activities like intentional disruption of computer networks through using various tools like worms, viruses, phishing activities and various other malicious software and programming scripts

Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

It is important to distinguish between cyberterrorism and "hacktivism," a term coined by scholars to describe the marriage of hacking with political activism. ("Hacking" is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. Unlike hacktivists, hackers tend not to have political agendas.) Hacktivists have four main weapons at their disposal: virtual blockades; e-mail attacks; hacking and computer break-ins; and computer viruses and worms.

V. CONCLUSION

Cyber-security is each concerning the insecurity created by and thru this new house and concerning the practices or procedures to form it (progressively) secure. labor to verify the Internet ought to provides a definitive want else the "information technology" won't be viably utilized by shoppers. The terrorist of things to return can win the wars while not discharging an attempt simply by crushing the country's necessary substructure if steps don't seem to be taken to handle the generality of the enlargement in such a cyber-attack. they'll bring associate degree unknown examine the lives of others, in spite of whether or not they live close or over the world. The "cyber-terrorism" will in one methodology or alternate prompts the cost even as inflicting severe harms. although social media will utilize for cybercrimes, these organizations cannot stand to quit utilizing social media because it assumes an important role within the attention of a company. Cyber terrorist act has warranted varied innocent lives and within the meanwhile render varied homes to a condition of the matter that's often materializing to mental injury to the influenced families. Cyber terrorist act stays important problems with the current society. Not simply that the battle against Cyber terrorist act is falling behind, current law-breaking assaults are ending up more and more forceful and resistance. Cyber security has associate degree intriguing parallel to terrorist act. Guaranteeing the protection of knowledge, data, and correspondence is imposingly tougher than hacking into a system.

REFERENCES

[1] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077-

[2] Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. EURASIP Journal on Information Security. doi:10.1186/s13635-018-0080-0

[3] Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.

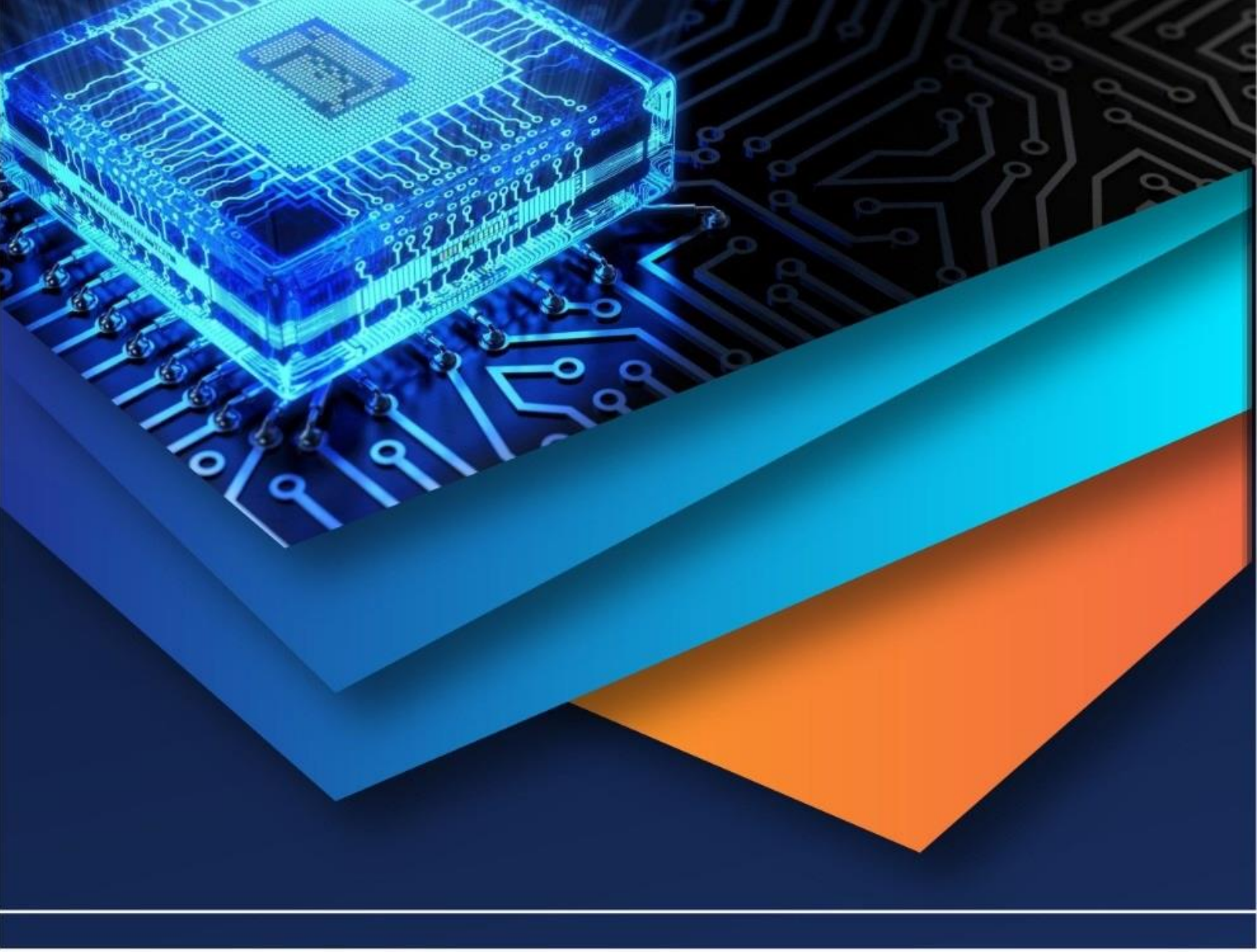
[4] Gade, N. R., & Reddy, U. G. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Retrieved from https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

[5] Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

[6] Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp. 175-186.

[7] Kumar, S., & 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.

[8] Gabriel Weimann, 'Cyberterrorism – How real is the threat', United States Institute of Peace, Special Report 119, December 2004; Zahri Yunos and Sharifuddin Sulaman, 'Understanding Cyber Terrorism from Motivational Perspectives', *Journal of Information Warfare*, Vol. 16, No. 4 (Fall 2017), pp. 1-13; Maura Conway, ''Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet', *First Monday*, Vol. 7, No. 11-4, November 2002.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY