Security Challenges in Cyber World

Y S Rao, Sibasish Rath,
Gandhi Institute of Excellent Technocrats, Bhubaneswar
R K Institute of Engineering & Technology, Cuttack, Odisha, India

ABSTRACT

Cyber Security accepts a vigorous role in the area of information technology. Safeguarding theinformationhasbecomeanenormousprobleminthecurrentday.Thecyber securitythemainthingthatoriginatesinmindis'cybercrimes'whichareaggregatecolossallydaily.Differe ntgovernmentsand organizations are taking numerous measures to keep these cyber wrongdoings. Other thandifferentmeasurescybersecurityisasyetasignificantworrytomany.Thispapermostlyemphaseson cyber security and cyber terrorism. The significant trends of cybersecurity and the consequenceof cybersecurity discuss in it. The cyber-terrorism could make associations lose billions of dollars inthe region of organizations. The paper also explains the components of cyber terrorism andmotivationofit.Twocasestudiesrelatedtocyber securityalsoprovideinthispaper.Somesolutionaboutcybersecurityandcyberterrorismalsoexplain init.

Keywords: Cybersecurity;cyberspace;cyberterrorism;Informationsecurity.

I. INTRODUCTION

Today an individual can receive and send any information may be video, oran email or only through the click of a button but did s/he ever ponder how safethis information transmitted to another individual strongly with no spillage ofdata? The proper response lies in cybersecurity. Today more than 61% of fullindustryexchangesaredoneontheinternet,sothisareaprerequisitehighqualityof security for direct and best exchanges. Thus, cybersecurity has become a mostrecent issue (Dervojeda, et. all., 2014). The extent of cybersecurity does notmerely restrict to verifying the data in IT industry yet also to different fields likecyberspace and so forth. Improving cybersecurity and ensuring that necessarydatasystemsare vitaltoeachcountry'ssecurityandfinancialprosperity.

Creating the Internet safer (and safeguarding Internet clients) has becometo be essential to the improvement of new management just as a legislativestrategy. The encounter against cybercrime needs an extensive and more securepractice (Gross, Canetti &Vashdi, 2017). The particular estimates alone cannotkeep any crime; it is essential that law authorization offices are allowable toinvestigationandindictcybercrimeefficiently.Nowadaysnumerouscountriesandadministrations are compelling strict rules on cyber safeties to keep the loss ofsomevitaldata.Eachshouldbeequippedonthiscybersecurityandsavethemselvesfromtheseincreasing cybercrimes.

Cyber-security is both about the insecurity made by and through this newspace and about the practices or procedures to make it (progressively) secure(Kumar, &Somani, 2018). It alludes to a lot of exercises and measures, bothspecialized and non-specialized, expected to ensure the bioelectrical conditionand the information it contains and transports from all possible threats. Thisresearch aims to gather all the information and overview related to cyber-crimeand provide the historical facts and perform reports on the analyzed data ofdifferentattacksreportedeverywhereinthelastfiveyears.Basedontheanalyzedinformation, we would like to provide all the countermeasures that organizationsmayundertakeinordertoensureimprovedsecuritythatwouldsupportindefending the organizations from being attacked by the hackers and provide acyber-securitytoavoidall risks.

II.   PURPOSE

Thepaperprovidesinformationaboutcybersecurityandcyberterrorism. It covers various information about these topics in its subsections.Trendsofcybersecurityandtheroleofsocialmediaincybersecuritydefineinthispaper.Thepaperprovidesso menecessaryinformationaboutcyberterrorism.Thecomponents of "cyber terrorism" and the consequences of this terrorism alsoexplain in this paper. There are some examples of case studies those related tocybersecurity. The paper also provides some solutions regarding cyber securityand cyber terrorism. It provides some techniques for preventing cyber terrorism.Thefuturestudyandscopeofcybersecuritydefineinit.

Cybersecurity has become a major concern over the last 10 year in the ITworld. In the present world, everybody is facing a lot of problems with cyber-crime. As hackers are hacking major sensitive information from government andsome enterprise organizations the individuals are very much worried as cyber-securityassaultcanbringabouteverythingfromwholesalefraud,toblackmailbigcompanies.Theyaremanyvarietiesofc yber-crimesemergingwhereeveryone

needs to be aware of the scams and they are different measures and tools whichcan be used for avoiding the cyber-crimes. Every organization wants to securetheirconfidentialdatafromgettinghacked.Gettinghackedisnotjustaboutlosingthe confidential data but losing the relationship with customers in the market(Bendovschi, 2015).

The Internet is today's fastest growing infrastructure. In today's technicalenvironment many new technologies are changing mankind. But due to theseemerging technologies, we are unable to protect our private information in anefficientway,sothecyber-crimesaredrasticallyincreasingondailybasis.Majorityofthetransactionsbothcommercialandpersonalaredoneusingth emeansonlinetransaction, so it is important to have an expertise who require a high quality ofsecuritymaintainingabettertransparencytoeveryoneandhavingsafertransactions.Socybersecurityisthelatestissue. Advancedtechnologieslikecloudservices, mobiles, E-commerce, internet banking and many more they require ahighstandardsandsaferprocessofsecurity.Allthetoolsandtechnologiesinvolvedforthesetransactionsholdthemostse nsitiveandcruicialuserinformation.Soprovidingthenecessarysecuritytothemisveryimportant.Improvingthecyberse curityandsafeguardingthesensitivedataandinfrastructuresareimportanttoeverycountriestopprioritysecurity(Pancha natham, 2015).

III.   TRENDS OF CYBER SECURITY

Cyber Security assumes a critical role in the area of data technology.Safeguarding the data have become the greatest difficulty in the current day. Thecybersecuritythemainthingthatraidsachordiscybercrimeswhichareincreasingtremendously step by step (Samuel, & Osman, 2014). Different administrationsandorganizationsaretakingmanymeasurestokeepthesecybercrimes.Additional the different measures cybersecurity is as yet an enormous worry tonumerous.Some maintrendsthatarechangingcybersecuritygive asfollows:

Webservers

Theriskofassaultsonwebapplicationstoseparateinformationortocirculate malicious code perseveres. Cybercriminals convey their code using goodwebservers they have traded off. In any case, information taking attacks,aconsiderable lot of which get the deliberation of media, are also a significant risk.Currently, individualsneeda moreunusualaccentuation onsecuringwebserversas well as web applications (Bendovschi, 2015). Web servers are mainly the pre-eminent stage for these cybercriminals to take the information. Thus, one shouldreliably utilizeanadditionalsecure program, mainlyamidvital exchangesalltogethernottofallas aquarryforthesedefilements.

MobileNetworks

Theriskofassaultsonwebapplicationstoseparateinformationortocirculate malicious code perseveres. Cybercriminals convey their code using goodwebservers they have traded off. In any case, information taking attacks,aconsiderable lot of which get the deliberation of media, are also a significant risk.Currently, individuals need a more unusual accentuation on securing web serversas well as web applications (Bendovschi, 2015). Web servers are mainly the pre-eminent stage for these cybercriminals to take the information. Thus, one shouldreliably utilizeanadditionalsecure program, mainlyamidvital exchangesalltogethernottofallas aquarryforthesedefilements.

Encryption

Itisthemethodtowardencodingmessagessoprogrammerscannotscrutinizeit.Inencryption,themessageisencodedbyencryption,changingitintoastirred-upfigurecontent.Itcommonlycompleteswiththeuseofan"encryptionkey," that demonstrates how the message is to encode. Encryption at the earliestreferencepointlevelsecuresinformationprotectionanditsrespectability(Sharma,2012).Additionaluseofencryptionobtainsmoreproblemsincybersecurity.Encryptionisusedtoensuretheinformationintravel,forinstance,the information being exchanged using systems (for example the Internet, onlinebusiness), mobilephones, wireless radios andsoon.

ADP'sandtargetedattacks
AdvancedPersistentThreat(APT)isawholeofthedimensionofcybercrimeware. For quite a long time network security capacities. For example, IPS or webfilteringhavehadakeyinfluenceindistinguishingsuchfocused-onassaults(Bendovschi, 2015). As attackers become bolder and utilize increasingly dubiousmethods,networksecuritymustincorporatewithothersecuritybenefitstoidentify assaults. Thus, one must recover our security procedures to counteractmoredangerscominglateron.Subsequentlytheaboveisaportionofthepatterns
changing the essence of cybersecurity on the planet. The top network threats areshowinginfigure1.
Figure1.ThreatsforCyberSecurity

Top Network Threats

- Remote Procedure Call
- SQL Injection
- Browser
- Cross-Site Scripting
- Others
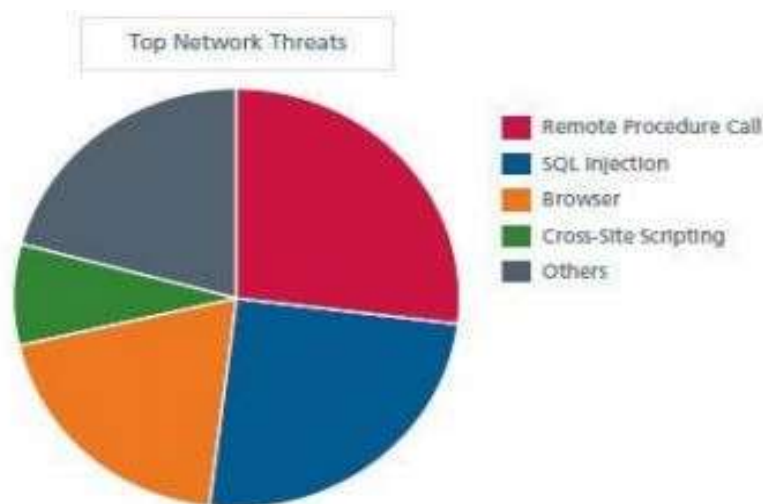
IV. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

Socialmediahasturnedintoalifestyleforsomeindividuals.Weuseittostayincontact,planoccasions,shareourphotographsandcommentonrecentdevelopments.Ithasreplacedemailandtelephonerequiresatonofus.However,similarly as with whatever else on the web, it is imperative to know about thedangers. PCs, cell phones, and different gadgets are priceless assets that furnishpeopleofanyagewiththeextraordinarycapacitytoconnectandcollaboratewithwhatever remains of the world. Individuals can do this in various ways, includingtheutilizationofsocialmedia ornetworking sites.
Courtesy of social media, people can share musings, pictures, exercises, oranypartoftheirlives(Gross,Canetti&Vashdi,2017).Theycanbringanunknownlook into the lives of others, regardless of whether they live nearby or over theglobe.Unfortunately,thesenetworksadditionallyrepresentsecuritytowardone'sPC, protection, and even their security. Social media collection among faculty issoaring as is the risk of assault (Sharma, 2012). Since social media sites are nearlyutilized by the majority of them reliably, it has become an excellent stage forcybercriminalsforhackingprivatedataandtakingsignificantdata.
The organizations need to assure they are likewise as fast in recognizingdangers, reacting increasingly, and keeping away from a rupture of any sort.Subsequently, individuals must take suitable measures particularly in managingsocial media to keep the loss of their data. The capacity of persons to impart datato a group of persons of millions is at the core of the exact test that social mediaofferingstoorganizations(Cabaj,Kotulski,Księżopolski,&Mazurczyk,2018).Nevertheless, enabling anyone to disperse financially delicate data, social mediaadditionally gives a comparable ability to range false data. It can be merely beingas harming. The rapid spread of incorrect information by social media is amongthegrowingdangers.Thoughsocialmediacanutilizeforcybercrimes,theseorganizationscannotstandtoquitutilizingsocialmediaasitassumesanessentialroleintheattentionofanorganization.Initsplace,theyshouldhavearrangement

s that will inform them of the risk to fix it before any actual harm isdoneDervojeda,Verzijl,Nagtegaal,Lengton,&Rouwmaat,2014).Anyway,organizations should understand this and observe the meaning of breaking downthe data chiefly in social deliberations and give good security plans to avoiddangers.Onemustcontractwithsocialmediabyusingspecificplansandtherighttechnologies.

V. CYBER TERRORISM

Theterm"terrorism"canalludetotheillegalutilizationofpowerorviciousness against people in order to threaten an administration or its residentsand associations which might be to accomplish a political or a malicious site [10].Terrorism has transformed from the conventional structure to the cyber type ofinnovation supported terrorism recognized as cyber terrorism. It stays vital issuesof the present society. Not just that the battle against terrorism is falling behind,currentcybercrimeassaultsareendingupprogressivelyforcefulandconfrontational (Sharma, 2012). This terrorism is the utilization of cyber word todispatch an assault to the essential foundations that the presence of associationsand countriesentirelydependedafterthatcanpromptitsshutdown.

ComponentsofCyberTerrorism
Afewattacksascyberterrorismhaveafewpartswhichhavebeendistinguished by numerous observational researchers in the exploration network.As indicated by Samuel and Osman (2014) in their hypothetical model recognizethe five sections that a "cyber-terrorism" classified they are; the objective of theviolence,inspirationanddedicationtowardsthemissiontobeaccomplishedwhensuchincidenttakesplace,impact,instrumentsareutilizedtodispatchsuchassault

andattacking's,areawhichisnaturejustasthestrategy foractivity.Itcanconfidently know by knowing the profile of activities that drive the actions of theculprits(Kumar,&Somani, 2018).
The critical issue in "cyber terrorism" is the motivation to complete such anaction on the Internet, that outcomes in savagery/damage to people and theirproperty Dervojeda, Verzijl, Nagtegaal,Lengton, &Rouwmaat, 2014). It is by aportion of the segments. The terrorists of the world proceed the upside of thecyber world with solid incentive as a stage with which they can use to dispatchmore unusual outbreak. Yunos and Ahmad (2014) said that with the utilization ofInformationandcorrespondenceinnovation,aterroristcouldpresentmorenoteworthy harms or exact the republic with troublesome conditions because oftheinterruptionofnecessaryadministrationsthatthe"cyberspaceterrorist"causesmoredamageanddevastationbythe cyberspacethandonetheconventionalstrategyforterrorism.

MotivatingFactorofCyberTerrorism
Themotivatingfactorsofcyberterrorismgiveasfollows:
Websites'SupportiveNature:
Theinternethasviewedasamediumthat
isexceptionallytremendous,andthatcaninthemeantimedrawinlightofalegitimateconcernforsomeindividualsto join some group of interest. The cyberterrorist prefers the utilization of thewebsite as a result of its robust nature in that it can refer a message to a greatmany individuals inside a twinkle of an eye; they consider it to be a stage that isanythingbutdifficulttoselectabsorbedindividuals.
AnonymityNatureof theinternet:
Anonymity is the pivotal element that each evil culprit leans towards withthe goal that their character could not be recognizable after playing out theirdevilish act.The Internet is a sheltered domain just as concealing stage for theterrorist astheycanstayunknown sothattheirpersonalitycannotbeknown.
Hacking:
Theoveralltermofallkindsofunapprovedaccesstoany"computersystem"networkorganizeishackingthatcanoccurinanystructureallthingsmeasuredas"cyber murder." A large number of these hackers make use of a "brute force"which is the combinations of every single imaginable letter just as numbers andimagestillthey getthepasswordSreenu,&Krishna, 2017).
ComputerViruses:
These viruses are here and there scattered on a system to in other to dohurtfulexercises.Thesemaybetofillinasanadministrativeagent,createinformationorevensplitdownthesystem.
    PasswordSniffing:
The "Cyber terrorist" may use one of the technique such as password sniffas procedures to complete their "cyber-attack" on different countries and manybig organizations to see their downfall and have control over their systems. Thepasswordsnifferisprogrammingwhichusestoscreenorganizeandinthemeantime catchallthepasswordthatpassesthesystem connector.

Consequencesof"CyberTerrorism"

Cyberterrorismisanoriginaltypeofcyberdangerandattackthathasmanyoutcomes connected to it when propelled against any countries and associations.Some consequencesofcyberterrorismdefineasfollows:

DataIntrusion:

The cyber terrorism can annihilate information honesty with the goal thatthe informationcouldneveragainbe trusted, pulverizingits classificationasintrudingonitsaccessibility.Theexpandingrateofthiscyberterrorisminencroachingassociationsandc ountry'sinformationhasproducedatonofdifficulties which has come about in loss of vitals and critical information that istypicallydifficulttorecover(Sutton,2017).

TheattackonBusinesses:

The cyber-terrorism could make associations lose billions of dollars in theregion of organizations. The data arrangement of a bank can be attacked or hackthroughtheterroristswhowillpromptunapprovedaccesstosuchfinancialbalance and make them lose gigantic millions of dollars which can create suchbanktokeep running intobankruptcy(Gade,&Reddy,2014).

LossofLife:

Cyber terrorism has guaranteed many acquitted lives and in the meantimerendernumeroushomestoaconditionoftheproblemthatisoccasionallycomingabouttomentalinjurytotheinfl uencedfamilies.The"cyber-terrorism"caninonemethod or alternate prompts the death toll just as causing severe harms. It hasshowninanattackonthePCsutilization,networks'aswellasattacksthathave comeabouttothedifferenttypesofblastsofafewplaneaccidentsissueseverywhere throughout the world which that has asserted numerous life (Cabaj,Kotulski,Księżopolski,&Mazurczyk,2018).

ConsumerTrustinDoubt:

The development of any organizations and its support relies upon the trustthatits purchaser has onsuchassociation as trustcansee tools that fortifyassociationandcertainty amongassociationsandclients.

VI.   CASE STUDY EXAMPLES

CyberSecurityinE-Governancecasestudy

E-Governanceistheextensionoftheeffortscompletedthroughthegovernmentstorecoverrelationswiththeirnationals.Wit hitsinstilledstraightforwardness and receptiveness, given the standards of the Internet, E-Governance conveys governments all the more near their residents. Existing andpotential dangers in the circle of cybersecurity are among the most genuinedifficultiesofthe21stcentury.ToensureE-Governanceextendsthereisarequirementfordatasecuritybestpractices(Hua,&Bapna,2013).Securitypolicies, practices, and techniques must be set up just as the use of securitytechnology. It helps to ensure e-Government systems against attack, recognizesgreat exercises administrations and to have a demonstrated alternate course ofaction set up. An open private organization is a vital part of cybersecurity in E-Governance.Theseassociationscanconvenientlygoupagainstcoordinationissues. Powerful cyber-crime prevention and arraignment activities in all the ICTappropriate conditions.

KasperskyKidnappingCase

The"highest-profile"cybersurveillance,stalking,andkidnappingcaseincludedIvanKaspersky,childoftheadministratorandCEOof Russia-basedKasperskyLab,astandoutamongstthemostunmistakablecybersecurityfirmsontheplanet.IvanKasperskywasab ductedforpayoffin2011whilestrollingtoworkfrom his Moscow loft. As indicated by Russian media sources, beginners – a moreseasoned obligated couple – organized the plot and enrolled their child and twoof hiscompanions as"muscle"for the plot(Cabaj,Kotulski,Księżopolski,&Mazurczyk,2018).TheabductorsstalkedKasperskyandhissweetheartforawhile precedingtheseizing,decidinghisconductstandardsandfindingthathedidnot haveaprotectivesecuritydetail.Thehijackerssupposedlyacquiredalltherequired data from Kaspersky's client profile on Vkontakte, a famous Russiansocial systems administration site. Kaspersky was compelled to call his dad totransfer the payoff requests (Gade, & Reddy, 2014). The abductors may haveutilizedsimilarwirelesstomakefooddeliveriesorhadgeolocationadministrationsempowered.

UberCasestudy

Data breaches happen every day, in too many places, but the risk of databreach doesn't necessarily depend on the number, it may also depend on the riskand damage it causes the company's revenue and impact on the users or accountholders, oneofthe biggestrecentdata breachesis Uber.

Impact:
Oneoftherecentmajorcyber-attackisdatabreachofpersonalinformationofaround57millionUber usersand600,000Uber driversgotrevealed.

Details:
The worst part of this attack is how the Uber handled the issue, this is alessontomostcompanieswhatnottodo.Inlate2016justtwohackerswereableto steel the Users personal data with includes names, phone numbers and emailaddresses.They were able to steal the 600,000 driver's license information.Hackers got access to the Uber'sGitHub account through a third-party cloud-based service. With the details found from the GitHub, Hackers found a way toaccessUberuserdatainAWS.Uberspaidthosetwohackers$100,000topermanently destroy the whole data they obtained and not letting the users ortheregulatorsaboutstoleninformation.

But also, Uber confirmed that data was destroyed with the assurance theyreceived from the hackers. According to US Law enforcement, any breach shouldbereportedtotheauthoritiesandnotpayhackers.AndthiskindofapproachfromUber led other hackers to blackmail Netflix, where Hackers frightened to releaseTVshowsunlessthecompanypaidthemoneyhackersrequested.Almost49stateshave this law enforcement where a security breach should be notified, after thecourthearingsUberagreedtopay20milliontosettleFTCcharges.NotonlytheUSbutalsoothermajorcountrieslikeUK ,Italy,andthePhilippinesreactedonthis

issue. Uber's breach is different from the regular breaches, the company tried tocover upthebreach andnotalerttheauthoritiesandtheusers.

Uber'splanafterthebreach:
Khrosrowshabi the new CEO of Uber received few disputed problems onlywithrespecttoitslegalissuealsocriticismforsexualharassment,underpayingthedriversandfewmore.

Solutions
Somesolutionsregardingcybersecurityandcyberterrorismdescribehere:

• CyberSecurityTechniques
Sometechniquescanusetoimprovecybersecurity.

• Access control and "password security": The idea of password and username has a primary method for ensuring data. It may be the principalmeasuresconcerning cybersecurity.

• Data'sAuthentication:Thedocumentsthatwegetshoulddependablybevalidated be before transferring. It should check if it has begun from acritical and dependable source and that they are not modified (Gade, &Reddy, 2014). Verifying of these records is typically done by the "anti-virus" software present in the gadgets. Subsequently, a decent "anti-virus"softwareislikewisenecessarytoshieldthegadgetsfromviruses.

• Anti-virussoftware:ItisaPCprogramthatclassifies,avoids,andmakesamove to harm or evacuate noxious software programs, for instance,viruses as well as worms. Most "antivirus programs" comprise an "auto-update"featurethatauthorizestheprogramtodownloadprofilesofnewviruses with the objective that it can chequer for the new viruses whentheyfind.

• Malwarescanners:Thisissoftwarethattypicallyfilterseachoftherecords and archives current in the framework for vindictive code ordestructive viruses [10]. Viruses, worms, as well as Trojan horses, areinstances of "malicious software" that regularly assemble and alluded toasmalware.

• Firewall:A"softwareprogram"oranequipmentthathelpsmonitorhackers, infections, and all types of worms which endeavour to achievePC over the Internet. All data which is transmitting to and fro over thewebgothroughthefirewallcontemporary,whichlooksateveryindividualmessageandhinderswhichdonotmeetthes ecurityrequirementsandclassifythemasthreatandtrytoblockfromthesystemand monitor the activities. Henceforth firewalls assume an essential jobinrecognizing themalware.

PreventionofCyberTerrorism
The capacity to prevent cyber terrorism lies with the capacity to securelyverify cyberspace. Cybersecurity has an intriguing parallel to terrorism. Both arelopsided. Guaranteeing the security of information, data, and correspondence isimpressivelyharderthanhackingintoaframework.Theattackerhasaninalienable preferred standpoint in both regular terrorism and cyber-attacks. Onaccount of state-supported attacks, the difficulties are of a lot higher greatness(Cabaj,Kotulski,Księżopolski,&Mazurczyk,2018).Governmentsshouldguaranteethat their rules smear to cybercrimes and be wholly actualized and hold fast to; itis essential that the countries of the biosphere take measures to guarantee thatits punitive and technical law is satisfactory to address the difficulties

presentedbycybercrimes (Kumar,&Somani,2018).

Theavailability,confidentialityandtheintegrityofinformationinanyassociations are essential which endeavors must be set up to guarantee that theyare exceptionally secure because it is the significant cyber resource that makeseachassociationstandandinthemeantimedependedupon.Theinformationhasenteredbythe"cyber-terrorist"issomethingbeyondrecordswhichmayincorporatemessages,webapplications,webpages,andjustassomeindispensable operatingsystems. (Kumar, &Somani, 2018)

VII.   FUTURE STUDY AND SCOPE

This   paper   will   help   to   advance   the   scientific   interests   in   the explorationofcybersecurity,particularlytorespondtotheproceduralquestionsoftheprediction of future data and actions   significant   to   security   patterns.   This studysetsthebackgroundtobeginexecutingrulesforallintentionsasindicatedthroughthe usual security issues and answers   for   data   systems.   This   paper consolidatesmanyproceduresconnectedandmaybeimprovedtoservecybersecurityregardinganticipatingtheoperationallegitimacyofthemethodologiesofassessmentbenchmarks.Finally,theemphasisonlimiting,recouping,anddisposingofweaknessistheprimary,basicpatterns,andreactionstotheconstantexpandingprogress(Panchanatham,2015).

Over thenextfiveyears,cyber-crime may createseveredamageininformation technology. According to the researchers they have estimated anapproximate close to 6 trillion dollars loss. So, there would be a very bright scopeforpeoplewhoworkandresolvetheissuesrelatedtocyber-crimeandprovideallthenecessarysecuritymeasures.BigorganizationslikeCISCOwhichiscompletelyrelatedtonetworkingtechnologywhichisoneofthetoporganizationhasapproximately millions of openings related to cybersecurity because which is thefuture for the safety of Information technology. They are also wide opportunitiesin government-related fields and also defence field to save the countries securedatafromcyberattackers.

VIII.   CONCLUSION

Cyber-securityisbothabouttheinsecuritymadebyandthroughthisnewspace and about the practices or procedures to make   it   (progressively)   secure.Exertiontoverifythecyberspaceshouldgiveadefinitiveneedelsethe"information technology"   will   not   be   viably   used   by   clients.   The   terrorist   of thingstocomewillwinthewarswithoutdischargingashotjustbycrushingthecountry'snecessary substructure if steps are   not   taken   to   handle   the   pervasiveness   of   theexpansioninsuchacyber-attack.Theycanbringanunknownlookintothelivesofothers, regardlessofwhether they livenearbyorovertheglobe. The"cyber-terrorism"caninonemethodoralternatepromptsthedeathtoll just as causing severe harms. Though social media can utilize for cybercrimes,these organizations cannot stand to quit utilizing social media as it assumes anessential role in the attention of an organization. Cyber terrorism has guaranteednumerous innocentlives   and   in   the   meantime   render   numerous   homes   to aconditionoftheproblemthatisoccasionallycomingabouttomentalinjurytotheinfluenced families. Cyber terrorism stays vital issues of the present society. Notjust that the battle against Cyber terrorism is falling behind, current cybercrimeassaults are ending up progressively forceful and confrontational. Cybersecurityhas an intriguing parallel to terrorism. Guaranteeing the security of information,data,and correspondence isimpressivelyharder thanhackingintoa system.

REFERENCES

[1]   Bendovschi,A.(2015).Cyber-Attacks–Trends,PatternsandSecurityCountermeasures.ProcediaEconomicsandFinance,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). InnovativeBusiness Models: Supply chain finance. Netherlands: Business Innovation Observatory;European Union.

[4]   Gade,N.R.,&Reddy,U.G.(2014).AStudyOfCyberSecurityChallengesAndItsEmergingTrends On Latest Technologies.   Retrieved fromhttps://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:itseffectsonpsychologicalwell-being,publicconfidenceandpoliticalattitudes.JournalofCybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

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

[7]   Kumar, S., &Somani, V. (2018). Social Media Security Risks, Cyber Threats And RisksPrevention And Mitigation Techniques. International Journal of Advance Research inComputerScienceand Management,4(4), pp. 125-129.

[8]   Panchanatham,D.N.(2015).AcasestudyonCyberSecurityinE-Governance.InternationalResearchJournalofEngineeringandTechnology.

[9]   Samuel,   K.   O.,   &   Osman,   W.   R.   (2014).   Cyber   Terrorism   Attack   of   The ContemporaryInformationTechnologyAge:Issues,ConsequencesandPanacea.InternationalJournalofComputerScienceandMobileCom

puting, 3(5), pp.1082-1090.

[10]   Sharma,   R.   (2012).   Study   of   Latest   Emerging   Trends   on   Cyber   Security   and   its challengestoSociety.InternationalJournalofScientific&EngineeringResearch, 3(6).

[11]   Sreenu,M.,&Krishna,D.V.(2017).AGeneralStudyonCybe   AttacksonSocialNetworks.IOSRJournalofComputerEngineering(IOSR JCE),19(5),pp.01-04.

[12]   Sutton,D.(2017).CyberSecurity:APractitioner'sGuide.Swindon,UK:BCS,theCharteredInstitutefor IT.