Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0062

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

सायबर गुन्हेगारी प्रतिबंधित धोरणे, आव्हाने व उपाययोजना

डॉ. ज्योती जी. नाकतोडे व प्रा. आम्रपाली ए. भिवगडे
आठवले समाजकार्य महाविद्यालय, भंडारा

गोषवारा (Abstract)

सायबर गुन्हेगारी ही माहिती तंत्रज्ञानाच्या वेगवान प्रगतीमुळे उद्भवलेली एक गंभीर समस्या आहे. हॅकिंग, डेटा चोरी, ऑनलाइन फसवणूक, सायबर टेररिझम आणि रॅन्समवेअर हल्ले यांसारखे गुन्हे जागतिक स्तरावर वाढत आहेत. या संशोधनात सायबर गुन्ह्यांचे प्रकार, त्यांच्या प्रतिबंधासाठी उपलब्ध कायदे व धोरणे तसेच प्रभावी उपाययोजनांचा आढावा घेतला आहे. भारतामध्ये माहिती तंत्रज्ञान कायदा, २००० आणि राष्ट्रीय सायबर सुरक्षा धोरण (२०१३) यांसारखी धोरणे अस्तित्वात असली तरी त्यांची अंमलबजावणी अजूनही प्रभावी नाही.

सायबर गुन्हेगारी प्रतिबंधासाठी तांत्रिक उपाय, कठोर कायदे, जनजागृती आणि आंतरराष्ट्रीय सहकार्य महत्त्वाचे आहेत. सायबर सुरक्षा शिक्षण आणि डिजिटल साक्षरतेच्या प्रसारावर भर देणे आवश्यक आहे. प्रभावी सायबर सुरक्षा धोरणे केवळ तांत्रिक उपायांपुरती मर्यादित न राहता, कायदेशीर सुधारणा आणि समाजातील जागरूकता वाढवण्यावर भर देण्याची गरज आहे.

प्रस्तावना (Introduction):

सायबर गुन्हेगारी

नवनवीन तंत्रज्ञानामुळे सायबर गुन्हेगारी वाढत आहे. सायबर गुन्हेगारी म्हणजे संगणक, इंटरनेट किंवा डिजिटल तंत्रज्ञानाचा वापर करून केले जाणारे बेकायदेशीर कृत्य. यामध्ये डेटा चोरी, आर्थिक फसवणूक, हॅकिंगफिशिंग,सायबरस्टॉकिंग, रॅन्समवेअर हल्ले, आणि सायबर टेररिझम यांचा समावेश होतो. सायबर गुन्हे हे वैयक्तिक, व्यावसायिक तसेच शासकीय पातळीवर मोठ्य प्रमाणावर होत आहेत. इलेक्ट्रॉनिक यंत्र, इंटरनेट टेक्नॉलॉजी चा वापर करून व व्यतिगत माहितीला कुणी अडथला आणत असेल व स्वत: चा आर्थिक फायदा करून घेत असेल यामुळे व्यक्ती व समाजाचा शारीरिक, मानसिक व आर्थिक नुकसान होत असेल तर तो सायबर गुन्हा होय.

सायबर सुरक्षेची गरज व महत्त्व

सायबर सुरक्षेच्या अभावामुळे व्यक्ती, संस्था आणि देशाच्या सुरक्षिततेला धोका निर्माण होतो. त्यामुळे प्रभावी सायबर सुरक्षा धोरणे राबविणे अत्यंत आवश्यक आहे.

१. व्यक्तिगत स्तरावररू डेटा संरक्षण, गोपनीयता आणि सुरक्षित व्यवहार सुनिश्चित करण्यासाठी.
२. उद्योग क्षेत्रात: कंपन्यांच्या संवेदनशील माहितीची सुरक्षा आणि व्यवसायातील सातत्य टिकवण्यासाठी.
३. राष्ट्रीय सुरक्षा: सायबर टेररिझम आणि हॅकिंगपासून देशाच्या महत्त्वाच्या प्रणालींचे संरक्षण करण्यासाठी.

सायबर गुन्हेगारी रोखण्यासाठी सरकारने कठोर कायदे लागू करणे, नवीन तंत्रज्ञानाचा अवलंब करणे आणि जनजागृती करणे आवश्यक आहे.

सायबर गुन्हेगारीचे प्रकार (Types of Cyber Crimes)

१. डेटा चोरी व हॅकिंग (Data Theft & Hacking)

डेटा चोरी म्हणजे कोणत्याही व्यक्ती, कंपनी किंवा संस्थेच्या गोपनीय आणि संवेदनशील माहितीची परवानगीशिवाय चोरट्य मार्गाने मिळवलेली माहिती. हॅकिंगच्या माध्यमातून सायबर गुन्हेगार संगणक प्रणालीत बेकायदेशीर प्रवेश करून डेटा चोरू शकतात, तो बदलू शकतात किंवा नष्ट करू शकतात.

उदाहरणे, बँकिंग खात्यांची माहिती चोरून आर्थिक फसवणूक करणे. एखाद्या कंपनीच्या ग्राहक डेटाबेसमध्ये घुसखोरी करून तो चोरी करणे.

२. फिशिंग आणि ऑनलाईन फसवणूक (Phishing & Online Fraud)

फिशिंग हा सायबर गुन्हेगारांकडून वापरण्यात येणारा एक फसवणुकीचा प्रकार आहे, ज्यामध्ये बनावट ई–मेल, वेबसाइट किंवा संदेशाद्वारे वापरकर्त्यांची संवेदनशील माहिती (उदा. बँक खाते, पासवर्ड) चोरली जाते.

उदाहरणे:

बँकेच्या अधिकृत वेबसाइटसारखी बनावट वेबसाइट तयार करून वापरकर्त्यांची लॉगिन माहिती मिळवणे.

''तुम्ही लॉटरी जिंकली आहे'' अशा बनावट ई–मेलद्वारे आर्थिक फसवणूक करणे.

३. सायबर स्टॉकिंग आणि ट्रोलिंग (Cyber Stalking & Trolling)

सायबर स्टॉकिंग म्हणजे एखाद्या व्यक्तीचा वारंवार ऑनलाइन पाठलाग करणे, धमक्या देणे किंवा मानसिक त्रास देणे. सायबर ट्रोलिंगमध्ये व्यक्ती किंवा संस्थेविरुद्ध खोट्या बातम्या, आक्षेपार्ह टिप्पण्या आणि धमक्या दिल्या जातात.

उदाहरणे:

सोशल मीडियावर कोणालाही सतत त्रास देणे, धमक्या देणे किंवा बदनामी करणे.

महिलांना ऑनलाइन छेडछाड करून धमकावणे.

४. डार्क वेब व सायबर टेररिझम (Dark Web & Cyber Terrorism)

डार्क वेब हे इंटरनेटचा एक भाग आहे जो सामान्य सर्च इंजिनमध्ये दिसत नाही आणि मुख्यत: बेकायदेशीर कामांसाठी वापरला जातो. सायबर टेररिझममध्ये दहशतवादी गट इंटरनेटचा वापर देशाविरोधात कट रचण्यासाठी करतात.

उदाहरणे:

डार्क वेबवर ड्रग्स, शस्त्रास्त्रे आणि खोटे ओळखपत्रे विक्रीसाठी ठेवणे.

सरकारी वेबसाईट हॅक करून राष्ट्रीय सुरक्षेशी संबंधित माहिती चोरणे.

५. रॅन्समवेअर आणि मॅलवेअर हल्ले (Ransomware & Malware Attacks)

रॅन्समवेअर हा एक प्रकारचा सायबर हल्ला आहे, जिथे हॅकर्स संगणकातील डेटा लॉक करून त्याच्या मोबदल्यात पैसे (रॅन्सम) मागतात. मॅलवेअर (Malware) हा हानिकारक सॉफ्टवेअरचा प्रकार आहे, जो संगणक किंवा नेटवर्कला हानी पोहोचवतो

उदाहरणे:

Ransomware हल्ल्यामुळे हॉस्पिटलच्या सर्व रुग्ण डेटा लॉक करून फिरौती मागणे.

Trojan किंवा Worm सारख्या मॅलवेअरद्वारे संगणक प्रणाली दूषित करणे.

भारतातील सायबर सुरक्षेचे कायदे आणि धोरणे

भारतात डिजिटल क्रांतीमुळे इंटरनेटचा वापर मोठ्या प्रमाणात वाढला आहे. त्यामुळे सायबर सुरक्षेच्या गरजेची जाणीव वाढली असून, सरकारने विविध कायदे आणि धोरणे तयार केली आहेत.

१. माहिती तंत्रज्ञान कायदा, (2000 [IT Act] 2000)

भारतात सायबर गुन्ह्यांवर नियंत्रण ठेवण्यासाठी माहिती तंत्रज्ञान कायदा, २००० (Information Technology Act] 2000) लागू करण्यात आला. २००८ मध्ये यामध्ये काही महत्त्वाचे बदल करण्यात आले, जे डिजिटल व्यवहार आणि सायबर सुरक्षेशी संबंधित आहेत.

कलम ४३(A): कोणत्याही व्यक्तीच्या संमतीशिवाय डेटा किंवा माहिती चोरणे किंवा त्याचा गैरवापर केल्यास दंडात्मक कारवाई.

कलम ६६: संगणक प्रणालीमध्ये अनधिकृत प्रवेश केल्यास शिक्षेची तरतूद.

कलम ६६C: फसवणुकीच्या उद्देशाने इलेक्ट्रॉनिक स्वाक्षरी किंवा पासवर्डचा गैरवापर केल्यास तीन वर्षांची शिक्षा.

कलम ६७: ऑनलाइन अश्लील साहित्य प्रसारित केल्यास शिक्षेची तरतूद.

कलम ६९: राष्ट्रीय सुरक्षेसाठी सरकारला एखाद्या संगणक प्रणालीचा डेटा पाहण्याचा आणि अडवण्याचा अधिकार.

२. भारतीय दंड संहिता अंतर्गत सायबर गुन्ह्यांवरील तरतुदी

IT कायद्याच्या जोडीने भारतीय दंड संहिता (IPC) अंतर्गत देखील सायबर गुन्ह्यांवर कारवाई केली जाते.

कलम ४१९: ऑनलाईन फसवणूक आणि बनावट ओळखपत्रे वापरण्याच्या गुन्ह्यांसाठी शिक्षा.

कलम ४२०: ऑनलाईन फसवणुकीद्वारे आर्थिक लाभ मिळवल्यास सात वर्षांपर्यंतची शिक्षा.

कलम ४६८ आणि ४७१: बनावट डिजिटल कागदपत्रे तयार करणे किंवा त्यांचा गैरवापर करणे.

कलम ५००: ऑनलाईन माध्यमातून बदनामी (Defamation) केल्यास शिक्षेची तरतूद.

३. राष्ट्रीय सायबर सुरक्षा धोरण (National Cyber Security Policy & 2013)

भारतात सायबर सुरक्षेला बळकटी देण्यासाठी राष्ट्रीय सायबर सुरक्षा धोरण, २०१३ लागू करण्यात आले. या धोरणाचा उद्देश महत्त्वाच्या सरकारी आणि खाजगी क्षेत्रांच्या डिजिटल पायाभूत सुविधा (Critical Infrastructure) सुरक्षित ठेवणे हा आहे.

प्रमुख उद्दिष्टे:

भारतासाठी संपूर्ण सायबर सुरक्षा फ्रेमवर्क तयार करणे.
सरकारी आणि खाजगी भागीदारीच्या माध्यमातून सायबर सुरक्षेच्या उपाययोजना विकसित करणे.
डिजिटल गुन्ह्यांविरोधात प्रशिक्षण आणि जनजागृती कार्यक्रम राबवणे.
राष्ट्रीय सायबर सुरक्षा धोरण कार्यान्वित करण्यासाठी विशेष यंत्रणा स्थापन करणे.

४. CERT&In आणि अन्य संस्थांची भूमिका

CERT & In (Indian Computer Emergency Response Team)
CERT & In ही भारतातील सायबर सुरक्षेसाठी जबाबदार असलेली राष्ट्रीय संस्था आहे.

भूमिका आणि जबाबदाऱ्या:

संगणक आणि नेटवर्क सुरक्षेशी संबंधित आपत्तींचा (Cyber Incidents) वेळीच सामना करणे.
भारतातील सरकारी आणि खाजगी संस्थांना सायबर सुरक्षा उपाययोजना देणे.
सायबर हल्ल्यांविषयी माहिती गोळा करून त्यावर कारवाई करणे.
सरकारी वेबसाइट्स आणि इन्फ्रास्ट्रक्चर वरील सायबर हल्ल्यांपासून संरक्षण करणे.

इतर सायबर सुरक्षा संस्था:

१. राष्ट्रीय सायबर सुरक्षा समन्वयक (NCSC):
भारताच्या सायबर सुरक्षेच्या धोरणांचे नियोजन आणि अंमलबजावणी करण्यासाठी जबाबदार.

२. Cyber Crime Co ordination Centre :
सायबर गुन्ह्यांशी संबंधित तपास आणि गुप्तचर यंत्रणांना मदत करणारी संस्था

३. Data Security Council of India (DSCI):
सायबर सुरक्षेची जनजागृती वाढवणे आणि डिजिटल धोरणे विकसित करणे.

सायबर गुन्हेगारी प्रतिबंधासाठी धोरणात्मक उपाय (Policy Measures for Cyber Crime Prevention)

१. सायबर सुरक्षा जागरूकता आणि शिक्षण (Cyber Security Awareness & Education)

१. इंटरनेट वापरणाऱ्या प्रत्येक व्यक्तीने सुरक्षित पासवर्ड, OTP धोरणे, फिशिंग ईमेल्सपासून बचाव यांसारख्या मूलभूत सायबर सुरक्षेच्या संकल्पना समजून घ्याव्यात.
२. शाळा, महाविद्यालये आणि कार्यस्थळी सायबर सुरक्षा प्रशिक्षण कार्यक्रम राबवले जावेत.
३. डिजिटल व्यवहार करताना खबरदारी कशी घ्यावी, यावर मोफत ऑनलाइन कोर्सेस आणि वेबिनार्स आयोजित करावेत.
४. कर्मचाऱ्यांसाठी नियमित सायबर सुरक्षा प्रशिक्षण (Cyber Hygiene Training) बंधनकारक करावे.
५. कंपन्यांनी आपली डेटा प्रायव्हसी पॉलिसी मजबूत करावी आणि ग्राहकांची माहिती सुरक्षित ठेवण्यासाठी योग्य उपाययोजना कराव्यात.

२. तंत्रज्ञान–आधारित संरक्षण (Technology & Based Protection)

i) संवेदनशील डेटा सुरक्षित ठेवण्यासाठी एन्क्रिप्शन तंत्रज्ञानाचा वापर करावा.नेटवर्क सुरक्षा वाढवण्यासाठी फायरवॉल आणि VPN (Virtual Private Network) वापरणे आवश्यक आहे.
ii) कृत्रिम बुद्धिमत्ता (AI) आणि यंत्र शिक्षण (Machine Learning)AI आधारित सायबर सुरक्षा प्रणाली वापरून फिशिंग हल्ले, मालवेअर आणि क्क्रै हल्ले ओळखणे शक्य होते.
iii) मोठ्या प्रमाणावर होणाऱ्या सायबर हल्ल्यांचा पूर्वानुमान लावण्यासाठी यंत्र शिक्षण (Machine Learning) तंत्रज्ञानाचा उपयोग केला जाऊ शकतो.
iv) पारंपरिक पासवर्डऐवजी फिंगरप्रिंट, फेस–आयडी आणि आयरिस स्कॅन यांसारख्या सुरक्षित प्रमाणीकरण तंत्रांचा अवलंब करावा.

३. बँकिंग आणि ई–कॉमर्स क्षेत्रातील सुरक्षाव्यवस्था (Security Measures in Banking & E&Commerce)

i) २–स्टेप व्हेरिफिकेशन आणि OTP प्रणाली बंधनकारक करावी.
ii) आर्थिक व्यवहारांसाठी फिशिंग अटॅक्सपासून संरक्षण करणाऱ्या AI–आधारित प्रणाली लागू कराव्यात.
iii) बँकांनी फ्रॉड डिटेक्शन सॉफ्टवेअर वापरून संशयास्पद व्यवहारांची माहिती ग्राहकांना त्वरीत द्यावी.

iv) सुरक्षित पेमेंट गेटवे वापरावे आणि ग्राहकांना SSL प्रमाणपत्र असलेल्या वेबसाइट्सचाच वापर करण्याचा सल्ला द्यावा.

v) रिफंड आणि फ्रॉड प्रोटेक्शन धोरणे मजबूत कराव्यात.

४. सरकारी आणि खाजगी भागीदारी (Public&Private Partnership)

i) सरकार आणि IT कंपन्यांनी मिळून सायबर सुरक्षा संशोधन आणि विकास मध्ये गुंतवणूक करावी. मोठ्या तंत्रज्ञान कंपन्यांनी सरकारी यंत्रणांना सायबर गुन्ह्यांविरोधात डेटा विश्लेषण आणि सुरक्षा उपाय पुरवावे.

ii) आंतरराष्ट्रीय सहकार्य आणि माहिती शेअरिंग बुडापेस्ट कन्व्हेन्शन सारख्या आंतरराष्ट्रीय करारांमध्ये भारताने अधिक सक्रिय सहभाग घ्यावा.

iii) विविध देशांतील सायबर सुरक्षा संस्थांमध्ये माहिती शेअरिंग तंत्र विकसित करावे.

५. कठोर कायद्यांची अंमलबजावणी आणि न्यायप्रक्रियेत सुधारणा (Strict Law Enforcement & Judicial Reforms)

i) सायबर गुन्ह्यांची सुनावणी करण्यासाठी विशेष सायबर कोर्ट्स आणि तज्ज्ञ न्यायाधीशांची नेमणूक करावी.

ii) न्यायालयीन प्रक्रियेत विलंब टाळण्यासाठी Fast & Track Courts स्थापन करावेत.

iii) सायबर गुन्ह्यांसाठी शिक्षा अधिक कठोर करावी आणि आर्थिक फसवणुकीसाठी त्वरित भरपाई देण्याची यंत्रणा निर्माण करावी. डेटा चोरी, ऑनलाइन फसवणूक आणि सायबर स्टॉकिंगसाठी नवीन दंड संहिता तयार करावी.

iv) प्रत्येक राज्यात विशेष सायबर गुन्हे अन्वेषण यंत्रणा (Cyber Crime Investigation Units) स्थापन करावी.

v) पोलिसांना सायबर सुरक्षेचे अद्ययावत प्रशिक्षण देऊन त्यांचे कौशल्य वाढवावे.

आव्हाने आणि मर्यादा (Challenges and Limitations)

सायबर गुन्हेगारी प्रतिबंधित करण्यासाठी अनेक उपाययोजना केल्या जात असल्या तरी, काही मोठी आव्हाने आणि मर्यादा अद्यापही कायम आहेत.

१. डिजिटल साक्षरतेचा अभाव (Lack of Digital Literacy)

i) अनेक लोक सायबर गुन्ह्यांची संभाव्यता आणि सुरक्षेच्या मूलभूत तत्त्वांबाबत अनभिज्ञ असतात.

ii) ऑनलाईन फसवणूक, फिशिंग ईमेल्स, पासवर्ड सुरक्षा यांसारख्या गोष्टींबाबत जागरूकता नसल्यामुळे ते सहजपणे सायबर गुन्ह्यांचे बळी ठरतात.

iii) लहान शहरांमध्ये आणि ग्रामीण भागात तंत्रज्ञानाचा वापर वाढत असला तरी सायबर सुरक्षिततेविषयी माहिती कमी आहे.

iv) भारतातील ग्रामीण आणि निमशहरी भागात सायबर सुरक्षा शिक्षण आणि प्रशिक्षणाची कमतरता आहे.

v) सरकारने विविध डिजिटल शिक्षण उपक्रम राबवले असले तरी, प्रत्यक्षात याची प्रभावी अंमलबजावणी होत नाही.

२. आंतरराष्ट्रीय सहकार्याची कमतरता (Lack of International Cooperation)

i) सायबर गुन्हेगार अनेकदा वेगवेगळ्या देशांमधून हल्ले करतात, त्यामुळे त्यांच्यावर कारवाई करणे कठीण होते.

ii) विविध देशांमध्ये सायबर गुन्ह्यांविरोधातील कायदे वेगवेगळे असल्यामुळे आंतरराष्ट्रीय स्तरावर सहकार्य कमी असते.

iii) काही देश डेटा एक्सचेंज करण्यास तयार नसतात, त्यामुळे सायबर गुन्हेगारांचा मागोवा घेणे कठीण होते.

iv) बुडापेस्ट कन्व्हेन्शन सारख्या आंतरराष्ट्रीय सायबर सुरक्षा करारांमध्ये भारत अद्याप पूर्णत: सहभागी झालेला नाही.

३. गोपनीयतेचा मुद्दा आणि डेटा संरक्षण (Privacy Issues and Data Protection)

i) मोठ्या प्रमाणावर डेटा लीक आणि हॅकिंगचे प्रकार वाढले आहेत.

ii) डेटा संरक्षण आणि गोपनीयता धोरणे प्रभावीपणे राबवली जात नाहीत, त्यामुळे नागरिकांचा डेटा सुरक्षित नाही.

iii) मोठ्या कंपन्या (Google, Facebook, Amazon) वापरकर्त्यांचा डेटा मोठ्या प्रमाणावर गोळा करतात, त्यामुळे गोपनीयतेचे उल्लंघन होते.

iv) देशांतर्गत डेटा साठवण्याचे नियम अद्याप प्रभावीपणे राबवले जात नाहीत.

४. नवीन तंत्रज्ञानामुळे वाढणारे सायबर धोके (Emerging Cyber Threats Due to New Technology)

i) AI आधारित फसवणुकीचे तंत्र अधिक प्रगत होत आहे, ज्यामुळे चुकीची माहिती पसरवणे आणि खोटी व्हिडिओ सामग्री तयार करणे सोपे झाले आहे.

ii) AI आधारित स्वयंचलित हल्ले (Automated Cyber Attacks) करण्याच्या शक्यता वाढल्या आहेत.

iii) स्मार्टफोन, स्मार्ट होम डिव्हाइसेस, आणि IoT उपकरणांवर सायबर हल्ल्यांचे प्रमाण वाढले आहे.
iv) ब्लॉकचेन आणि क्रिप्टोकरन्सीच्या वाढत्या लोकप्रियतेमुळे सायबर गुन्हेगारांसाठी हे नवे लक्ष्य बनले आहे.
v) रॅन्समवेअर हल्ल्यांमध्ये बिटकॉइन आणि इतर क्रिप्टोकरन्सीचा वापर वाढला आहे, कारण त्याचा मागोवा घेणे अवघड असते.

निष्कर्ष (Conclusion)

सायबर गुन्हेगारी ही डिजिटल युगातील एक मोठी समस्या बनली आहे. डेटा चोरी, ऑनलाईन फसवणूक, रॅन्समवेअर हल्ले, सायबर टेररिझम आणि सोशल मीडिया गैरवापर यांसारख्या गुन्ह्यांचे प्रमाण वाढत आहे. यामुळे सामाजिक, आर्थिक आणि राष्ट्रीय सुरक्षेवर मोठा परिणाम होत आहे. प्रभावी सायबर सुरक्षा धोरणे आणि तंत्रज्ञानाच्या मदतीनेच या गुन्ह्यांना आळा घालता येऊ शकतो. सायबर गुन्हेगारी रोखण्यासाठी कठोर कायदे, आंतरराष्ट्रीय सहकार्य, डिजिटल साक्षरता, आणि अत्याधुनिक तंत्रज्ञानाचा वापर अनिवार्य आहे. सरकारने सायबर सुरक्षेसाठी धोरणात्मक सुधारणा कराव्यात आणि गुन्हेगारी विरोधी कठोर कारवाई करावी. आंतरराष्ट्रीय स्तरावर सहकार्य वाढवून जागतिक सायबर सुरक्षेचे नियम अधिक प्रभावी बनवावेत. सामान्य नागरिकांमध्ये सायबर सुरक्षेविषयी जागरूकता वाढवणे ही प्राथमिकता असावी. हे उपाय प्रभावीपणे राबवले, तर भविष्यात सायबर गुन्हेगारीचे प्रमाण कमी करता येईल आणि डिजिटल युग अधिक सुरक्षित करता येईल.

संदर्भ (References)

१. Das, S., Nayak, T., & Patnaik, S. (2020). "Cybercrime and Cybersecurity: A Study on Awareness and Preventive Measures." International Journal of Computer Applications, 175(3), 10-16.
२. Gupta, M., & Sharman, R. (2018). "Cybersecurity in India: Threats, Challenges, and Solutions." Springer Cybersecurity Handbook, 459-472.
३. भारत सरकार (Government of India) – राष्ट्रीय सायबर सुरक्षा धोरण (National Cyber Security Policy, 2013) L=ksr: Ministry of Electronics and Information Technology (MeitY) URL: https://www.meity.gov.in/
४. माहिती तंत्रज्ञान कायदा, २००० (The Information Technology Act, 2000) आणि त्यामधील सुधाकरण (Amendments in 2008, 2021)
५. IBM सायबर सिक्युरिटी ट्रेंड्स आणि धोके
L=ksr: https://www.ibm.com/security dt. 17-03-2025
६. www.ncsc.gov.org, dt. 16-03-2025