Research Paper IMPACT FACTOR VALUE : 5.983 | E-ISSN NO : 2455-295X | VOLUME : 11 | ISSUE : 5 | MAY 2025

साइबर अपराध: भारत के आंतरिक सुरक्षा के लिए चुनौती

PURKHA RAM [1] | DR MADULIKA YADAV [2]

[1] RESEARCH SCHOLAR, TANTIA UNIVERSITY.

[2] RESEARCH SUPERVISOR, TANTIA UNIVERSITY.

ABSTRACT:

-

KEYWORDS:

-

PAPER ACCEPTED DATE:	PAPER PUBLISHED DATE:
17th May 2025	19th May 2025

1. आंतरिक सुरक्षा (Internal security):-

आंतरिक सुरक्षा का सामान्य अर्थ है कि किसी भी देश की अपनी सीमाओं के भीतर की सुरक्षा से है। किसी भी देश कि राष्ट्रीय सुरक्षा (National Security) में आंतरिक सुरक्षा की अहम भूमिका है। आंतरिक सुरक्षा कोई नवीन शब्दावली नहीं है। महान् कूटनीतिज्ञ चाणक्य द्वारा लिखित अर्थशास्त्र में भी आंतरिक सुरक्षा का उल्लेख मिलता है। जिसमें मुख्यतः चार अलग अलग प्रकार के खतरों का जिक्र है जिसमें 1. आंतरिक 2. बाहय 3. बाहय रूप से सहायता प्राप्त आंतरिक 4. आंतरिक रूप से सहायता प्राप्त बाहय

स्वतंत्रता के बाद से ही भारत की आंतरिक सुरक्षा हमेशा चुनौतीपूर्ण रहती है। जिसमें मुख्यतः नक्सलवाद, नृजातीय संघर्ष, भ्रष्टाचार, मादक द्रव्य व्यापार, आतंकवाद आदि। लेकिन उदारीकरण के बाद विभिन्न देशों के मध्य अंर्तनिर्भरता बढ़ने से आंतरिक सुरक्षा में नई प्रकार की चुनौतियां उभरकर सामने आई। इसमें सबसे प्रमुख तकनीकी विकास एवं संचार व प्रौधोगिकी के कारण साइबर अपराध एक मुख्य चुनौती बन गया है। साइबर स्पेस का उपयोग करते हुए अपराधी देश के आंतरिक हिस्सों में धार्मिक कट्टता, नृजातीयता, साइबर आतंकवाद झूठी अफवाहों के माध्यम से दंगे करवाना तथा देश की गोपनीय जानकारी चुराना, व्यक्तिगत जानकारी चुराना, महिलाओं एवं बच्चों की गरीमा का हनन करना आदि।

2. साइबर अपराध:-

साइबर अपराध वह अपराध है जिसमें कम्पयूटर, नेटवर्क या डिजिटल उपकरणों आदि का उपयोग करते हुए अपराधिक कार्यो को अंजाम देना शामिल है। साइबर अपराधी डिजीटल साक्षरता एवं साइबर सुरक्षा के आभाव का फायदा उठाकर इस अपराध को असानी से अंजाम दे रहे है।

साइबर अपराध की कोई भौतिक सीमा का निर्धारण नहीं होता है। साइबर अपराधी तकनीकी उपकरणों की सहायता से दूरस्थ स्थानों तक इस प्रकार के अपराधों को अंजाम देते है। साइबर अपराध की घटना दिन प्रतिदिन बढ़ती जा रही है। साइबर अपराधी विभिन्न साधनों के माध्यम से व्यक्तिगत जानकारी, व्यवस्थित जानकारी, बैकिंग डाटा आदि चुरा लेते है। तत्पश्चात उनका दुरूपयोग करते है।

जैसे जैसे इंटरनेट की प्रत्येक क्षेत्र तक पहुँच बढ़ी है वैसे वैसे आम आदमी की इंटरनेट की निर्भरता के कारण इस प्रकार के अपराध में अत्यधिक वृद्वि हुई है।

साइबर अपराध को बड़े स्तर पर सोशल मिडिया के माध्यम से अंजाम दिया जा रहा है। क्योंकि आम नागरिक की व्यक्तिगत जानकारी इन प्लेटफार्म पर उपलब्ध है जिनका उपयोग अपराधी आसानी से दुरूपयोग कर सकते है। मुख्य साइबर अपराध हैकिंग, फिशिंग, मैलवेयर, सेक्सटॉर्शन, डिजिटल अरेस्ट, सोशल इंजिनियरिंग आदि।

3. आंतरिक सुरक्षा को प्रभावित करने वाले साइबर अपराध

अ. साइबर अपराध द्वारा बुनियादी ढांचे को प्रभावित करना

किसी भी राष्ट्र का बुनियादी ढांचा यह होता है जिसमें राष्ट्र की सुरक्षा नेटवर्क, संचार, सार्वजनिक कार्यों का संगठन होता है। यह किसी भी राष्ट्र का मुख्य आधार होता है जैसे कीरसायन क्षेत्र, वाणिज्यिक क्षेत्र, संचार क्षेत्र, रक्षा क्षेत्र, आपातकालीन सेवा, स्वास्थ्य सेवा, परिवहन प्रणाली आदि।

ब. डाटा चोरी और निजता का हनन

अपराध के माध्यम में व्यक्तिगत जानकारी चुराना बैंक तथा वित्तीय संबंधी डाटा चोरी आदि इसमें शामिल है इसमें कंप्यूटर वायरस द्वारा कंप्यूटर तथा मोबाइल में रखे डाटा की चोरी करना है।

स. कंप्यूटर से संबंधित साइबर अपराध

a. Dos (Dential of Service)

इस हमले में एक साथ अधिक मात्रा में अटैक करके किसी नेटवर्क तथा सर्वर को बर्बाद किया जाता है इसमें डाटा की चोरी वर्तमान उत्तर को मिटाना तथा सिस्टम को कब्जे में लेकर फिरौती मांगना आदि शामिल है जैसा कि 2016 में पूरे मुंबई में इंटरनेट सेवा को बाधित कर दिया गया था।

b.फिशिंग (fishing)

इसमें एसएमएस फिशिंग तथा ईमेल फेसिंग का अधिक प्रयोग किया जाता है इसमें ईमेल या एसएमएस के माध्यम से लिंक भेजकर सिस्टम को कब्जे में लिया जाता है।

c. फार्मिंग (pharming)

इसमें हैकर्स द्वारा फर्जी वेबसाइट बनाकर इंटरनेट उपयोगकर्ता की गोपनीय जानकारी जुटा लेते हैं जैसे पासवर्ड, डेबिट कार्ड, क्रेडिट कार्ड नंबर आदि।

d. ऑनलाइन पायरेसी (Online Piracy)

इसमें किसी भी व्यक्ति एवं संस्था की बुद्धि एवं कलात्मक क्षमता की नकल करना तथा उसे गैर कानूनी रूप से प्रचार करना आता है

e. साइबर टेररिज्म (Cyber Terrorism)

साइबर आतंकवाद को आमतौर पर सूचना प्रणालियों, कार्यक्रम और डेटा के खिलाफ किसी भी पूर्व-निर्धारित, राजनीति से प्रेरित हमले के रूप में परिभाषित किया जाता है जो हिंसा की धमकी देता है या जिसके परिणाम स्वरूप हिंसा होती है। इसमें कोई भी साइबर हमला शामिल हो सकता है जो किसी देश, राज्य या शहर की लक्षित आबादी को डराता है या डर पैदा करता है, आमतौर पर महत्वपूर्ण बुनियादी ढ़ाचे को नुकसान पहुचाता है या बाधित करता है जो सामाजिक, आर्थिक, राजनीतिक और व्यावसायिक संचालन के लिए महत्वपूर्ण है।

सार्वजनिक इंटरनेट पर दिखाई देने वाले कंम्प्यूटर सर्वर, अन्य उपकरणों और नेटवर्क का उपयोग करके साइबर आतंकवादी इन कृत्यों को अंजाम दिया जाता है। सुरक्षित सरकारी नेटवर्क और अन्य प्रतिबंधित नेटवर्क अक्सर ऐसे कृत्यों का लक्ष्य होते हैं। अन्य लक्ष्यों में बैंकिंग उद्योग, सैन्य प्रतिष्ठान, बिजली संयंत्र, हवाई यातायात नियंत्रण केन्द्र और जल प्रणालियाँ शामिल हैं।

अमेरिकी संघीय जांच ब्यूरो (एफबीआई) साइबर आतंकवाद को किसी भी "सूचना, कंम्प्यूटर सिस्टम, कम्प्यूटर प्रोग्राम और डेटा के खिलाफ पूर्व-निर्धारित, राजनीतिक रूप से प्रेरित हमले के रूप में परिभाषित करता है, जिसके परिणामस्वरूप उपराष्ट्रीय समूहों या गुप्त एजेंटों द्वारा गैर-लड़ाकू लक्ष्यों के खिलाफ हिंसा होती है।" एफबीआई के अनुसार साइबर आतंकवादी हमला एक प्रकार का साइबर अपराध है जिसे स्पष्ट रूप् से शारीरिक नुकसान पहुँचाने के लिए डिज़ाइन किया गया है।

g. सोशल मीडिया के माध्यम से झूठी सूचना फैलाना (fake news on social media)

बहुत से लोग सोशल नेटवर्किंग साइटों पर सामाजिक, धार्मिक और राजनीतिक से जुड़ी अफवाहों को फैलाना है आम नागरिक की समझ नहींहोने के कारण इसका तेजी से फैल जाता है जिसे कई प्रकार की घटनाएं घटित होती है जैसे दंगे फेलना आदि।

द. महिलाओं और बच्चों के विरूद्ध साइबर अपराध

a. बाल यौन शोषण का प्रकाशन

बाल यौन शोषण की सामग्री जैसे चित्र तथा वीडियो समाहित होते हैं इसका प्रसार करना कानूनी अपराध बच्चों की यौन शोषण तथा अश्लीलता की वेबसाइट बनाना तथा उसकी ब्राउज करना आदि शामिल है।

b. महिलाओं के विरुद्ध साइबर अपराध

साइबर अपराध के माध्यम से महिलाओं के मानसिक रूप से प्रताड़ित करना, धमकाना, अश्लील चित्र और वीडियो को प्रचार प्रसार करना आदि।

4. साइबर अपराध से आंतरिक सुरक्षा को होने वाली चुनौतियां एवं निवारण:-

a. ***साईबर सुरक्षा तंत्र की कमी:-*** भारत में सरकारी एवं गैर सरकारी संस्थाओं के पास साइबर सुरक्षा तंत्र की कमी है। जैसे तकनिकी कार्मिक, उच्च गुणवत्ता युक्त सुरक्षा उपकरण, मॉनिटरिंग स्टाफ आदि।

b. ***सुरक्षा ऐजेन्सियों में साइबर सुरक्षा विशेषज्ञों की कमी:-*** भारत की केंद्रीय सुरक्षा ऐजेन्सियों एवं विभिन्न राज्यों की पुलिस के पास साइबर सुरक्षा विशेषज्ञों का आभाव है। जिससे साइबर अपराधियों को पकड़ने में कठिनाइयों का सामना करना पड़ता है।

c. ***मजबूत कानून का आभाव:-*** वर्तमान में साइबर अपराध से संबंधित कानून का आभाव है। इसके कारण अपराधी इसका फायदा उठाते है। मजबूत कानून के अभाव में दिन प्रतिदिन साइबर हॉटस्पॉट में वृद्धि हो रही है ।

d. ***सीमापार साइबर अपराधियों को पकड़ना:-*** साइबर अपराध को अंजाम देने वाले अपराधी अक्सर सीमा पार से संबंध रखते हैं अर्थात दूसरे देश में बैठकर साइबर अपराध को अंजाम देते है। वर्तमान में अंतराष्ट्रीय सहयोग के बिना अपराधियों को पकड़ना मुश्किल होता है।

5. आंतरिक सुरक्षा को मजबूत करने के लिए रणनीतियाँ

a. ***साइबर सुरक्षा उपकरणों में सुधार:-*** साइबर अपराध की सुरक्षा में काम आने वाले उपकरणों में सुधार करना। जैसे फायरवॉल प्रत्येक नेटवर्क में उच्च गुणवत्ता फायरवॉल को प्रयोग करना। साइबर सुरक्षा से जुड़ी तकनीकों को विकसित करना।

b. ***साइबर सुरक्षा कानून:-*** साइबर अपराध से निपटने के लिए मजबूत कानून का निर्माण करना। सीमापार अपराधियों को पकड़ने के लिए अंतराष्ट्रीय स्तर पर साइबर सुरक्षा से संबधित संगठन का निर्माण करना।

c. ***सार्वजनिक निजी साझेदारी:-*** साइबर अपराध से लड़ने के लिए सार्वजनिक एवं निजी क्षेत्र में मजबूत सहयोग की आवश्यकता है। कई बार साइबर अपराधी निजी संगठनों को निशाना बनाते है। निजी संगठनों की साइबर सुरक्षा की कमजोरियों की वजह से आंतरिक सुरक्षा प्रभावित होती है। इसलिए सार्वजनिक एवं नीजि संगठन मिलकर साइबर अपराध से लड़ सकती है। निरंतर सार्वजनिक एवं निजी क्षेत्र मिलकर भविष्य के संभावित खतरो से निपटने के लिए रणनितियां बना सकती है।

d. ***जागरूकता और प्रशिक्षण:-*** साइबर अपराध की अधिकतम घटनाएं जागरूकता के आभाव में होती है। साइबर अपराधी डिजीटल साक्षरता के आभाव का फायदा उठाते है। साइबर सुरक्षा को अकादमिक पाठ्यक्रम एवं अभियानों के माध्यम से आम आदमी तक पहुंचाना चाहिए। सुरक्षा ऐजंसियों को भी समय समय पर साइबर अपराधों की जानकारी एवं जांच का प्रशिक्षण देना चाहिए ताकि अपराधियों से प्रभावी ढंग से निपटा जा सके।

e. ***साइबर अपराध से रोकथाम की तकनीकों का विकास:-*** साइबर अपराध से निपटने के लिए इंटेलिजेंस का विकास करना चाहिए। जिसमें ।तजपपिबपंस प्दजमससपहमदबम और स्वचालित उपकरणों के माध्यम से इंटरनेट एवं नेटवर्क पर लगातार निगरानी रखनी चाहिए। प्रत्येक सरकारी एवं निजी संगठनों में साइबर सुरक्षा से संबधित निश्चित विशेषज्ञ लोगों की नियुक्ति करनी चाहिए। इन सभी रणनितियों का सामूहिक रूप से उपयोग कर साइबर अपराधों से आंतरिक सुरक्षा को मजबूत किया जा सकता है।

6. साइबर अपराध से निपटने के लिए भारत सरकार की प्रमुख पहलें-

a. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

- लॉन्च: 2019 में
- बेबासाइट: cybercrime.gov.in
- यह पोर्टल नागरिकों को आॅनलाईन साइबर अपराध की शिकायत दर्ज करने की सुविधा देता है। इसका उद्देश्य साइबर अपराधों को रोकना, जागरूकता बढ़ाना और प्रभावी ढंग से उनका समाधान करना हैं

विशेषताएँ:

- किसी भी प्रकार के साइबर अपराध जैसे फिशिंग, ऑनलाइन धोखाधड़ी, क्रेडिट/डेबिट कार्ड की धोखाधड़ी, पहचान की चोरी, बच्चों से संबंधित साइबर अपराध आदि की रिपोर्ट कर सकते है।
- महिलाओं और बच्चो के खिलाफ साइबर अपराधों के लिये एक समर्पित खंड भी है ।
- शिकायत दर्ज कराने की प्रक्रिया को सरल बनाया गया है ताकि कोई भी नागरिक आसानी से अपनी शिकायत ऑनलाइन कर सकें।
- शिकायत के आधार पर संबंधित राज्य या केन्द्र शासित प्रदेश की पुलिस कार्यवाही करती है।

b. इण् साइबर स्वच्छता केन्द्र

- लॉन्च: 2017 में मेइटी (Meity) द्वारा
- यह केन्द्र भारत में कंम्पूटर और इंटरनेट उपकरणों की सुरक्षा के लिये एक

महत्वपूर्ण पहल है।

उद्देश्य:

- यह पोर्टल नागरिकों और संगठनों को मालवेयर से निपटने में मदद करता है। इसके तहत विभिन्न उपकरणों को सुरक्षित रखने के लिये मालवेयर सफाई उपकरण उपलब्ध कराए जाते हैं।
- उपयोगकर्ताओं को संक्रमित उपकरणों को पहचाने और उसे साफ करने के लिये मार्गदर्शन प्रदान किया जाता है।

प्रमुख टूल्स:

- **M-Kavach** मोबाइल उपकरणों की सुरक्षा के लिए।
- **App Samvid** एप्लिकेशन व्हाइटलिस्टिंग सॉल्यूशन।
- **USB Pratirodh** उपकरणों के डेटा के अनाधिकृत उपयोग को रोकने के लिए।

c. बण् इंडियन साइबर क्राइम को ऑर्डिनेशन सेन्टर (Indian Cyber crime Coordination Centre)- I4C

- लॉन्च: 2020 में, गृह मंत्रालय द्वारा
- यह केन्द्र साइबर अपराधों से निपटने के लिये समग्र दृष्टिकोण अपनाता है। इसका मुख्य उद्देश्य एक केन्द्रिकृत प्लेटफार्म पर साइबर अपराधों की रिपोर्टिंग, जांच और उन्हें रोकने के लिये समन्वित प्रयास करना है।

कार्य

- विभिन्न कानून प्रवर्तन एजेसियों राज्यों और केन्द्र सरकार के बीच साइबर अपराधों से निपटने के लिये एक समन्वय मंच।
- साइबर अपराधों की रोकथाम के लिये रणनीतिक और नीति संबंधी सलाह प्रदान करता है।
- डेटा साझा करना और जांच के लिये डिजिटल साक्ष्य एकत्र करना।
- साइबर अपराधों के क्षेत्र में अनुसंधान और नवाचार को बढ़ावा देना।

d. साइबर जागरूकता अभियान

- सरकार द्वारा साइबर अपराध और ऑनलाइन धोखाधड़ी के प्रति जागरूता फैलाने के लिये विभिन्न अभियान चलाए जाते है। इन अभियानों का उद्देश्य नागरिकों को सुरक्षित ऑनलाइन व्यवहार करने और साइबर अपराधों से बचने के तरीके सिखाना है।

प्रमुख तत्व-

- **Stay safe Online अभियान:** इसके अन्तर्गत नागरिकों को ऑनलाइन खतरों के प्रति जागरूक किया जाता है, जैसे सोशल मीडिया पर सावधानी, सुरक्षित पासवर्ड का उपयोग, और संदिग्ध लिंक पर क्लिक न करना।
- स्कूलों और कॉलेजों में साइबर सुरक्षा पर कार्यशालाओं का आयोजन।
- विभिन्न भाषाओं में डिजिटल मीडिया, पोस्टर्स और वीडियों के माध्यम से साइबर सुरक्षा जानकारी उपलब्ध कराई जाती है।

e. इंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम(CERT-In)

- स्थापना: 2004 में
- एजेंन्सी का उद्देश्य: (CERT-In) एक राष्ट्रीय नोडल एजेंसी है जो साइबर सुरक्षा खतरों को पहचानने, उनसे निपटने और साइबर सुरक्षा उपायों के विकास में मदद करती है।

प्रमुख कार्य:

- साइबर हमलों में पहचान और जवाब।
- साइबर खतरों से निपटने के लिये विभिन्न संस्थानों और संगठनों को तकनीकी सहायता प्रदान करना।
- साइबर सुरक्षा घटनाओं की रिपोर्टिंग और उनके बारे में जागरूकता फैलाना।
- (CERT-In) नियमित रूप से साइबर सुरक्षा पर एडवाइजरी जारी करता है और सरकारी और निजी संस्थानों के साथ मिलकर काम करता है ताकि साइबर सुरक्षा के मानकों को बेहतर बनाया जा सकें।

f. डिजिटल पुलिस पोर्टल

- यह पोर्टल अपराध और आपराधिक ट्रैकिंग नेटवर्क सिस्टम के तहत भारत सरकार द्वारा विकसित किया गया है। इसका उद्देश्य राष्ट्रीय स्तर पर अपराधों और अपराधिक गतिविधियों का डेटाबेस तैयार करना है।

विशेषताएँ

- नागरिक अपने साइबर अपराधों से संबंधित एफआईआर दर्ज करा सकते है और उनकी स्थिति को ट्रैक कर सकते हैं।
- कानून प्रवर्तन एजेंसियों को देश भर में अपराधों की जांच और निगरानी के लिये डिजिटल डेटा उपलब्ध कराया जाता है।

g. साइबर क्राइम वॉलंटियर्स प्रोग्राम

- इस पहल का उद्देश्य साइबर सुरक्षा और साइबर अपराध की रोकथाम में नागरिकों की सक्रिय भागीदारी को बढ़ावा देना है।
- नागरिक इस कार्यक्रम के तहत स्वयसेवक बनकर साइबर अपराधों की पहचान करने, रिपोर्ट करने और साइबर सुरक्षा के क्षेत्र में योगदान दे सकते है।

h. डाटा प्रोटेक्शन बिल

- सरकार साइबर सुरक्षा के संदर्भ में डेटा की सुरक्षा को मजबूर करने के लिये डेटा प्रोटेशन बिल को पारित किया गया। इस बिल का उद्देश्य यह सुनिश्चित करना है कि नागरिकों की व्यक्तिगत जानकारी और डेटा साइबर अपराधों से सुरक्षित रहें।
- भारत सरकार की ये पहले साइबर अपराधों को नियंत्रित करने और साइबर सुरक्षा सुनिश्चित करने के लिए एक व्यापक दृष्टिकोण प्रस्तुत करती है। इसके तहत न केवल नागरिकों को रिपोर्टिंग के लिय प्लेटफार्म दिए गए है, बल्कि साइबर खतरों से निपटने के लिये तकनीकी सहयोग और जागरूकता भी प्रदान की जाती है।

7. निष्कर्ष

- साइबर अपराध एक तेजी से बढ़ती चुनौती है और आंतरिक सुरक्षा के लिये एक गंभीर खतरा बनता जा रहा है।
- साबइर अपराध से आंतरिक सुरक्षा के विभिन्न पहलुओं पर प्रतिकूल प्रभाव पड़ता डालता है, जैसे आर्थिक स्थिरता, महत्वपूर्ण बुनियादी ढ़ांचे की सुरक्षा, और जनता का विश्वास।
- साइबर अपराध ने आंतरिक सुरक्षा के पारंपरिक मा◌ॉडल को चुनौती दी है। अब, आंतरिक सुरक्षा केवल भौतिक सीमाओं की रक्षा तक सीमित नहीं है। बल्कि डिजिटल दुनिया में भी सुरक्षा सुनिश्चित करना आवश्यक है। सरकारों और सुरक्षा एजेंसियों को नई चुनौतियों का सामना करने के लिये साइबर को प्राथमिकता देनी चाहिये।
- साइबर अपराधों का अंतराष्ट्रीय प्रकृति का होना आंतरिक सुरक्षा को और अधिक जटिल बना देता है साइबर अपराधी भौगोलिक सीमाओं के परे काम कर सकते हैं। जिससे विभिन्न देशें को साथ मिलकर काम करने की आवश्यकता होती है।

अ. सिफारिशें और भविष्य के लिये उपाय-

- साइबर सुरक्षा उपायों का सुदृढ़ीकरण: सरकारें, संगठनों और व्यक्तियों को अपने अपने स्तर पर साइबर सुरक्षा उपायों को मजबूत करने की आवश्यकता है। इसमें तकनीकी निवेश, नए साइबर सुरक्षा नियम, और सार्वजनिक जागरूकता

कार्यक्रम शामिल करना चाहिए।

- सार्वजनिक - निजी सहयोगः सार्वजनिक और निजी क्षेत्रों के बीच सहयोग को बढ़ावा देने की आवश्यकता पर जोर दें, ताकि सूचनाओं का आदान प्रदान हो सकें और साइबर अपराध से निपटने के लिये एक मजबूत ढांचा बनाया जा सकें।
- साइबर अपराधों से निपटने के लिये कानूनी ढांचे को और सुदृढ़ करने की जरूरत है साथ ही अंतराष्ट्रीय सहयोग और नई साइबर सुरक्षा नीतियों की आवश्यकता पर भी जोर दें।
- नवाचार और प्रौद्योगिकी में निवेश: नए खतरों से निपटने के लिये एआई और मशीन लर्निंग जैसी तकनीकी मे निवेश करना भी एक महत्वपूर्ण कदम होगा इस पर बल दें कि साइबर अपराधों का पता लगाने और उनसे निपटने के लिये उन्नत निगरानी और डेटा विश्लेषण की तकनीकों को अपनाने की आवश्यकता है।

ब. भविष्य की दिशा -

- अनुसंधान और विकास की आवश्यकता - साइबर सुरक्षा पर शोध और विकास को प्राथमिकता देने की आवश्यकता पर बल दें। भविष्य के खतरे अधिक जटिल और उन्नत हो सकते हैं, इसलिये सरकारों और संगठनों को साइबर सुरक्षा अनुसंधान के लिये संसाधन आवंटित करना चाहिए।
- सतत् जागरूकता और अनुकूलनः साइबर अपराध लगातार विकसित हो रहें है इसलिए सतत जागरूकता और अनुकूलन की आवश्यकता हैं। हर स्तर पर साइबर सुरक्षा नीतियों और तकनीकों को समय समय पर अपडेट करने की आवश्यकता है।
- तत्काल कदम उठाने की आवश्यकता- साइबर अपराधों से उत्पन्न खतरों का मुकाबला करने के लिये तुंरत कार्यवाही की आवश्यकता है। अगर इस खतरे का समय पर समाधान नही किया गया तो इसका आंतरिक सुरक्षा पर दीर्घकालिक और गंभीर प्रभाव पड़ सकता है।
- सभी हितधारकों की भागीदारी - यह भी स्पष्ट करें कि साइबर अपराध से निपटने के लिये सभी हितधारकों-सरकार, निजी क्षेत्र, नागरिक समाज और अंतराष्ट्रीय समुदाय को एक साथ मिलकर काम करना होगा। साइबर अपराध एक वैश्विक समस्या है, और इसका समाधान भी वैश्विक दृष्टिकोण से ही संभव है।
- हम यह कह सकते है कि अगर सही नीतियों और रणनीतियों को अपनाया जाए, तो साइबर अपराधों से उत्पन्न चुनौतियों से प्रभावी ढ़ग से निपटा जा सकता है। साथ ही यह भी कह सकते है कि सरकारें और संगठन लगातार साइबर सुरक्षा में सुधार करने की दिशा में काम कर रहे हैं, जिससे आने वाले वर्षो में साइबर खतरों का बेहतर तरीके से सामना किया जा सकेगा।

REFERENCES

1. मानी का द्वितीय प्रकाशन, लीगल फ्रेमवर्क ऑन साइबर अपराध, कमलपब्लिशर (नई दिल्ली)
2. https://www.natstrat.org/articledetail/publications/cyber-crime-a-rising-threat-to-internal-security-119 html
3. साइबर अपराध ब्यूरो
4. प्रसाद आर.एस. (2004) साइबर अपराधः एक परिचय 3658, नाभी पब्लिकेशन।
5. प्रो. आर.के. चोबो, (द्वितीय संस्करण 2012), एक परिचय और साइबर कानून, कमला हाउस कोलकाता
6. https://cybercrime.gov.in/pdf
7. https://www.thehindu.com/sci-tech-technology/cybercrime-could-cost-the -world-almost-1-trillion/article33269047.ece/
8. प्रकाशक-भारत लॉ हाउस ,संस्करण . संस्करण 2022
9. इलाहाबाद लॉ एजेंसी फरीदाबाद 2010
10. https://www.cyberswachhtakendra.gov.in/(8)
11. https://www.cert-in-org.in/(14)
12. विकीपीडिया