आज़ादी का अमृत महोत्सव

साईबर अपराध और पुलिस की तैयारियां

पुलिस अनुसंधान एवं विकास ब्यूरो
गृह मंत्रालय, भारत सरकार, नई दिल्ली

साइबर अपराध और पुलिस की तैयारियां

दीपक सक्सेना
सहायक कमाण्डेन्ट (राजभाषा)
केन्द्रीय रिजर्व पुलिस बल

पुलिस अनुसंधान एवं विकास ब्यूरो
गृह मंत्रालय, भारत सरकार, नई दिल्ली
वर्ष 2022

भारत सरकार, गृह मंत्रालय की हिन्दी सलाहकार समिति द्वारा दिनांक 23 मई, 1979 को आयोजित बैठक में निर्णय लिया गया था कि पुलिस, अपराध, कारागार एवं न्यायालयिक विज्ञान तथा पुलिस प्रशासन आदि विषयों पर हिन्दी में मौलिक पुस्तकें उपलब्ध कराने के लिए पं. गोविन्द वल्लभ पंत पुरस्कार योजना प्रतिस्थापित की जाए। तदनुसार 22 मार्च, 1980 को गृह मंत्रालय के अपर सचिव की अध्यक्षता में हुई बैठक में निर्धारित मापदंडों के अनुसार इस योजना को अंतिम रूप दिया गया। इस योजना के भाग 1 के अंतर्गत प्रकाशित मौलिक पुस्तकों को पुरस्कृत किया जाता है तथा भाग 2 के अंतर्गत दिए गए विषयों पर पुस्तक लेखन कार्य कराया जाता है। इसी के तहत यह पुस्तक प्रकाशित की जा रही है।

पुस्तक में दिए गए विचार लेखक के निजी हैं
इनसे पुलिस अनुसंधान एवं विकास ब्यूरो,
गृह मंत्रालय, भारत सरकार, नई दिल्ली की
सहमति आवश्यक नहीं है ।

प्रकाशक	-	पुलिस अनुसंधान एवं विकास ब्यूरो गृह मंत्रालय, एन.एच-8, महिपालपुर, नई दिल्ली – 110037
संपादक	-	सतीश चन्द्र डबराल
संपादन सहयोग	-	पिसाल विक्रम आनंदराव, अनुवादक
प्रथम संस्करण	-	2022
मुद्रक	-	स्मैट फॉर्मस, 3588, जी.टी.रोड़, दिल्ली-110007

आमुख

भारत की पुलिस व्यवस्था को सुदृढ़ बनाने के लिए पुलिस अनुसंधान एवं विकास ब्यूरो, गृह मंत्रालय, भारत सरकार द्वारा वर्ष 1982 से पुलिस, कारागार प्रशासन, अपराधशास्त्र तथा न्यायालयिक विज्ञान इत्यादि से संबंधित विभिन्न विषयों पर हिंदी में लेखन को बढ़ावा देने के लिए पं. गोविंद वल्लभ पंत पुरस्कार योजना चलाई जा रही है। इस योजना के भाग-एक के अंतर्गत इन विषयों पर वर्ष भर में हिंदी में प्रकाशित पांच उत्कृष्ट मौलिक पुस्तकों को पुरस्कृत किया जाता है। साथ ही, योजना के भाग-दो के अंतर्गत ब्यूरो द्वारा पुस्तक लेखन हेतु विषय देकर रूपरेखाएं आमंत्रित की जाती हैं। मूल्यांकन समिति द्वारा इन रुपरेखाओं को प्रकाशन योग्य पाए जाने पर ब्यूरो द्वारा इनका प्रकाशन किया जाता है। इस योजना के भाग एक के अंतर्गत ब्यूरो द्वारा अब तक उपर्युक्त विषयों की हिंदी में प्रकाशित 156 पुस्तकों को पुरस्कृत किया जा चुका है। भाग-दो के अंतर्गत अब तक ब्यूरो द्वारा 41 पुस्तकों का प्रकाशन किया जा चुका है।

पुलिस अनुसंधान एवं विकास ब्यूरो द्वारा वर्ष 2020 में साइबर अपराध और पुलिस की तैयारियां विषय पर रूपरेखा आमंत्रित की गई थी। वर्ष 2021 में योजना की मूल्यांकन समिति द्वारा की गई सिफारिशों के आधार पर "साइबर अपराध और पुलिस की तैयारियां" पुस्तक जिसके लेखक श्री दीपक सक्सेना हैं का प्रकाशन कार्य किया गया है । इस पुस्तक में साइबर अपराध का परिचय एवं उसके प्रकारों का विस्तृत रूप से वर्णन किया गया है । पुस्तक में समय के साथ प्रौद्योगिकी में बदलाव से साइबर अपराधों के बदलते स्वरूप को दर्शाया गया है। भारत में साइबर अपराधों को रोकने के लिए बनाएं गए अधिनियमों, नियमों/संहिताओं के महत्व और इनकी आवश्यकताओं का विस्तार पूर्वक वर्णन किया गया है ।

इस पुस्तक में साइबर अपराध की नवीन चुनौतियों की व्यापक रूप से जानकारी देने के साथ-साथ विभिन्न प्रकार की साइबर समस्याओं जैसे हैकिंग, डाटा चोरी, कंप्यूटर वायरस, डोस अटैक, विभिन्न फिशिंग, ऑनलाइन पायरेसी, अफवाह, बुलिंग, साइबर स्टॉकिंग, साइबर आतंकवाद इत्यादि पर प्रकाश डाला गया है।

पुस्तक में बढ़ते हुए साइबर अपराधों के विरूद्ध पुलिस की तैयारियों में केन्द्र सरकार की पहल और राज्यों द्वारा साइबर अपराध के उन्मूलन हेतु किए गए उपायों की जानकारी दी गई है ।

देश में साइबर अपराध की वास्तविकता को सही मायने में लोगों के सामने रखने के लिए पुस्तक में विभिन्न आंकड़ों को शामिल किया गया है। इस पुस्तक में सरल भाषा के प्रयोग का विशेष ध्यान रखा गया है जिससे पाठकों को विषय वस्तु को समझने में किसी प्रकार की कठिनाई का सामना न करना पड़े। आशा है कि यह पुस्तक साइबर अपराध से जुड़े विभिन्न जटिल पहलुओं को पाठकों के समक्ष सरल और सहज रूप में प्रस्तुत करने और जन-जन में "साइबर-जागरूकता" लाने के प्रयास में सफल होगी ।

महानिदेशक
पुलिस अनुसंधान एवं विकास ब्यूरो

प्राक्कथन

इक्कीसवीं सदी अपने साथ इलेक्ट्रानिकी एवं सूचना व संचार प्रौद्योगिकी की क्रांति लेकर आई है। आज के युग में कम्प्यूटर और सूचना व संचार प्रौद्योगिकी से जुड़े उपकरण तथा सुविधाएं मानव जीवन का सबसे अहम् हिस्सा बन गए हैं। सच कहें तो इन सुविधाओं के बिना आधुनिक युग के कार्यकलापों की कल्पना भी नहीं की जा सकती। आज के दौर में मानव की कम्प्यूटर तथा सूचना व संचार प्रौद्योगिकी पर निर्भरता इतनी बढ़ गई है कि सामान्य बातचीत से लेकर व्यापार, व्यवसाय, सरकारी कामकाज, शिक्षा, बैंकिग लेनदेन, खरीद-फिरोख्त जैसी सभी गतिविधियां ऑनलाईन या डिजिटल माध्यमों से ही चल रही हैं। वर्ष 2020 तक भारत में इंटरनेट प्रयोगकर्ताओं की संख्या 70 करोड़ तक पहुंच गई थी और वर्ष 2025 तक इसके लगभग 97.4 करोड़ तक पहुंचने की उम्मीद है। इंटरनेट प्रयोगकर्ताओं की दृष्टि से भारत, चीन के बाद विश्व में दूसरे स्थान पर है।

नई प्रौद्योगिकी ने न केवल सामाजिक, आर्थिक व राजनैतिक जगत में क्रांति का संचार किया है, बल्कि अपराध जगत भी इससे अछूता नहीं रहा है। वस्तुत: अपराध जगत में कम्प्यूटर एवं सूचना व संचार प्रौद्योगिकी ने ऐसे तीव्रगामी बदलाव किए हैं कि आज समूचा विश्व अपराधों की तेजी से बदलती प्रकृति से चिंतित है और विश्व का हर देश अपराधों के प्रौद्योगिकी-समर्थित नए स्वरूप यानी 'साइबर अपराधों' से निपटने के लिए प्रयत्नशील है। वर्ल्ड-वाइड-वेब ने जहां हमें बहुत ही बेहतर ढंग से संपर्क बनाने में समर्थ बनाया है, वहीं इसके अस्तित्व के साथ साइबर अपराधों और साइबर आतंकवाद जैसे ख़तरे भी सामने आए हैं। साइबर अपराधों की सबसे बड़ी ख़ासियत यह है कि इनमें अपराधियों को गुमनामी या झूठी पहचान जैसी सहूलियतें मिल जाती हैं और अपराध के बाद पकड़े जाने या सजा पाने का डर उनमें बहुत कम देखा जाता है, जो बढ़ते साइबर अपराधों की सबसे बड़ी वजह है।

बढ़ते साइबर अपराध समूचे विश्व के साथ भारत के लिए भी गहरी चिंता का विषय हैं। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो के अनुसार भारत में वर्ष 2017 में 21,796 साइबर अपराध, वर्ष 2018 में 27,248 साइबर अपराध और वर्ष 2019 में 44,546 साइबर अपराध घटित हुए। देश में बढ़ते साइबर अपराधों को लेकर स्थिति उस समय और भी स्पष्ट हो गई जब हाल ही में गृह मंत्रालय के हवाले से यह जानकारी

दी गई कि मार्च 2021 से पहले के 18 महीनों में 'राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल' पर 3.17 लाख साइबर अपराधों की शिकायतें मिलीं और 5,771 एफ.आई. आर. दर्ज की गई।[1] गौरतलब है कि देश में घटित होने वाले सभी प्रकार के साइबर अपराधों और खास तौर पर महिलाओं एवं बच्चों के विरुद्ध घटित होने वाले साइबर अपराधों की ऑनलाईन शिकायत दर्ज कराने की सुविधा नागरिकों को प्रदान करने हेतु गृह मंत्रालय द्वारा 30 अगस्त 2019 को यह पोर्टल लोकार्पित किया गया था।

देश में बढ़ते साइबर अपराधों के पीछे कम्प्यूटर, इंटरनेट, मोबाइल फोन, स्मार्ट फोन और डिजिटल माध्यमों का बढ़ता प्रयोग ही एक मात्र कारण नहीं है, बल्कि जनता में "साइबर-जागरूकता" और "साइबर-समझ" की कमी ने भी इनमें सबसे ज्यादा योगदान दिया है। साइबर अपराधों की रोकथाम को लेकर पुलिस बलों द्वारा की जा रही तैयारियां और इंतजाम उस समय अप्रभावी सिद्ध हो जाते हैं, जब जनता अपनी अनुभवहीनता, अनभिज्ञता और उदासीनता की वजह से साइबर अपराधियों की नापाक कोशिशों का शिकार हो जाती है।

पुलिस अनुसंधान एवं विकास ब्यूरो ने "साइबर अपराध और पुलिस की तैयारियां" विषय पर पुस्तक के लेखन का अप्रतिम अवसर प्रदान कर इस दिशा में तथ्यों के विस्तृत अनुसंधान एवं विश्लेषण का मार्ग प्रशस्त किया है। इन्हीं विश्लेषणों और तथ्यगत अनुसंधानों के फलस्वरूप इस पुस्तक को एक सारगर्भित स्वरूप दिया जा सका है। तदनुसार इस पुस्तक में साइबर अपराधों की अवधारणा, उदभव एवं इतिहास से लेकर साइबर अपराधों के प्रकारों, साइबर अपराधियों की प्रकृति, आंकड़ों के विस्तृत विश्लेषण, विभिन्न मामलों के संदर्भ सहित उल्लेख, केन्द्र सरकार की अनूठी पहलों, पुलिस बलों के अनुकरणीय प्रयासों तथा बहुविध तैयारियों और साइबर अपराधों की रोकथाम के बारे में अभिनव सुझावों को शामिल करने का भरसर प्रयास किया गया है। इस पुस्तक का मूल ध्येय यही है कि जन-जन में "साइबर-जागरूकता" लाने और "साइबर-समझ" विकसित करने को सबसे ज्यादा महत्व दिया जाए, ताकि साइबर अपराधों के घटित होने की संभावनाएं न्यूनतम स्तर तक लाई जा सकें और पुलिस बल अपने प्रयोजनमूलक प्रयासों में सफल होते हुए जनता के बीच पहले से बेहतर विश्वसनीय छवि कायम कर सकें।

-दीपक सक्सेना

1 https://www.thehindu.com/sci-tech/technology/317-lakhs-cybercrimes-in-india-in-just-18-months-says-govt/article34027225.ece

अनुक्रमणिका

अध्याय 1

साइबर अपराध : एक परिचय

दुनिया को आज हम जिस रूप में देखते हैं, उसके बारे में यदि गहराई से सोचें तो हमें उसके तीन मूल आधार दिखाई देते हैं-

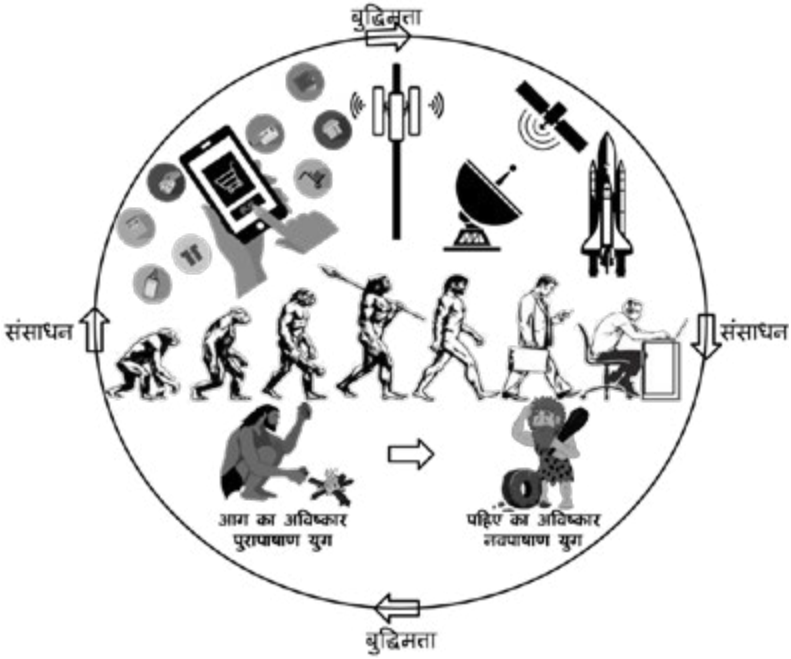
पहला : पृथ्वी पर मानव का अस्तित्व,

दूसरा : उत्पत्ति से ही अपने जीवन को सहज व सुरक्षित बनाने के लिए मानव द्वारा अपनी आवश्यकताओं के अनुरुप की गईं व्यवस्थाएं तथा अविष्कार, यानी विज्ञान।

और

तीसरा : मानव द्वारा अपनी प्रवृत्तियों एवं बुद्धिमत्ता से विकसित सभ्यता एवं संस्कृति।

पृथ्वी पर मानव ही एक मात्र ऐसा प्राणी है, जिसने सबसे पहले अपनी ज्ञानेन्द्रियों के माध्यम से प्राप्त अनुभवों को अपने बौद्धिक विकास का आधार बनाया। मानव ने अपनी बुद्धिमत्ता से संसाधन विकसित किए और संसाधनों का विकास करके उनके सहारे आगे बढ़ते हुए इस विश्व को आज की अत्याधुनिक अवस्था तक पहुंचाया। निसंदेह इस पूरी प्रक्रिया में मानव का बौद्धिक विकास निरंतर जारी रहा और अनंतकाल तक जारी रहेगा। इस प्रकार मानव सभ्यता में बुद्धिमत्ता से संसाधनों के विकास और फिर संसाधनों से बुद्धिमत्ता के विकास का यह चक्र निरंतर चलता रहा है और चलता रहेगा।



यही वो कारण है कि आज मानव इस संसार के समस्त कार्यकलापों का कर्ताधर्ता है। इस बात से कदापि इंकार नहीं किया जा सकता कि इस पृथ्वी पर अपनी उत्पत्ति से लेकर अब तक मानव ने अपने अस्तित्व, सहूलियतों और स्वार्थों के लिए हर संभव प्रयास किए हैं। सच्चे अर्थों में आज इस दुनिया का यह नित्य बदलता स्वरूप मानव के सतत प्रयासों की ही देन है। लेकिन ऐसा भी नहीं है कि मानव के द्वारा उन्नति की दिशा में किया गया हर प्रयास हमेशा सकारात्मक परिणाम देने वाला रहा हो। मानव द्वारा विकसित सभ्यता, संस्कृति और विज्ञान से जुड़ी कई व्यवस्थाएं और अविष्कार ऐसे भी रहे हैं, जिसका स्वयं मानव द्वारा ही दुरूपयोग किया गया है। अतीत में मानव सभ्यता और संस्कृति की कई व्यवस्थाएं कुरीतियों का रूप ले चुकी हैं और अंततया उनका उन्मूलन करना पड़ा है। इसी प्रकार, विज्ञान और प्रौद्योगिकी भी अनेकों बार वरदान की बजाय अभिशाप सिद्ध हो चुके हैं।

निसंदेह, संसार में नेकी और बदी, पाप और पुण्य, भलाई और बुराई सदैव साथ-साथ चलते आए हैं। संसार में अच्छाई के साथ बुराई का अस्तित्व सदैव बना रहा है। सच तो ये है कि यदि अच्छाई का अहसास न होता तो बुराई का अनुभव भी न होता और यदि बुराई न होती तो मानव को अच्छाई का कोई महत्व कभी समझ नहीं आता। शुरुआत से ही इस दुनिया में अच्छाई और बुराई के बीच की ये ज़द्दोज़हद बरकरार रही है। मानवीय दृष्टिकोण से दुनिया के हर कार्यकलाप को अच्छाई और बुराई के तराज़ू में तोला जा सकता है और मूल रुप से यही वह आधार है, जिसने दुनिया भर की मानव सभ्यताओं के बीच नीति और कानून जैसी व्यवस्थाओं को जन्म दिया है।

विश्वविख्यात यूनानी दार्शनिक अरस्तु (384-322 ईसा पूर्व) भौतिकी, आध्यात्म, कविता, नाटक, संगीत, तर्कशास्त्र, राजनीतिशास्त्र, नीतिशास्त्र, जीवविज्ञान सहित कई विषयों के महान विद्वान थे। उन्होंने कहा था "मनुष्य एक सामाजिक प्राणी है"। यानि समुदाय और समाज में रहना मनुष्य की जन्मजात प्रवृत्ति है। मनुष्य की इसी विलक्षणता के कारण मानव-सभ्यता आज यहां तक पहुंच सकी है। समुदायों और समाजों में रहने की प्रवृत्ति ने ही मनुष्य को सही-ग़लत, उचित-अनुचित और नैतिक-अनैतिक आचरणों की पहचान सिखायी है। इसी आधार पर मनुष्य ने अपने-अपने देश व समाजों में अच्छे और बुरे कर्मों को परिभाषित किया है और फिर बुरे कर्मों या अपराधों के लिए उनकी गंभीरता के अनुरुप सज़ा का प्रावधान रखा है। दूसरे शब्दों ने मनुष्य ने उत्तरोत्तर विकास करते हुए अपने देश, काल और वातावरण के अनुसार नीति व न्याय के सिद्धांतों का निर्माण किया है, जो यह परिभाषित करते हैं कि मानव या उसके समाज के लिए क्या उचित है और क्या अनुचित, क्या पुण्य और क्या पाप, क्या कर्तव्य है और क्या अपराध! विश्व की अलग-अलग सभ्यताओं और समाजों में निरंतर विकसित होते हुए मनुष्य ने प्राचीन काल से ही कुछ न कुछ ऐसे कृत्य किए हैं, जिन्हें नीति और न्याय के सिद्धांतों की दृष्टि से अनुचित माना जाता रहा है और अपराधों की श्रेणी में रखा जाता

रहा है। सच कहें तो अपराधों की सम्पूर्ण अवधारणा का उद्भव तभी से माना जा सकता है, जब से मानव ने सभ्य होना आरंभ किया था। अपराध मानवीय-व्यवहार का ही एक स्वरूप हैं। अपराध की मूल अवधारणा को समझने के लिए विद्वानों द्वारा दी गई अपराध की कुछ परिभाषाओं का संदर्भ यहां प्रासंगिक है :-

सदरलैण्ड के अनुसार; "अपराध सामाजिक मूल्यों के लिये ऐसा घातक कार्य है जिसके लिये समाज दण्ड की व्यवस्था करता है।" [1]

थोर्सटन सेलिन के अनुसार; "अपराध मानवीय समूहों के व्यवहार के आदर्श नियमाचारों का उल्लंघन हैं।"[2]

पॉल टप्पन के अनुसार; "अपराध एक समिप्राय कार्य या अनाचरण है जो दण्ड के कानून का उल्लंघन करता हैं।"[3]

डां. सेथना के अनुसार; "ऐसा कोई भी कार्य अपराध अथवा त्रुटि है जो किसी विशेष समय पर राज्य द्वारा निर्धारित कानून के अनुसार दण्डनीय हो।"[4]

समग्र रूप से अपराध के संदर्भ में सैद्धांतिक रूप से यही बुनियादी निष्कर्ष निकल कर सामने आता है कि अपराध वह कृत्य है जो अनैतिक होने के कारण कानून के सिद्धांतों के विरूद्ध है और जिसके लिए दण्ड का प्रावधान विद्यमान है।

इस अवधारणा को यदि और निकट से समझें तो सामान्यत: अपराध का अर्थ ऐसे किसी कृत्य या आचरण से है, जिसे समाज अपनी व्यवस्थाओं

1 https://en.wikipedia.org/wiki/Edwin_Sutherland
2 https://nptel.ac.in/content/storage2/courses/109103022/pdf/mod5/lec28.pdf
3 Ibid.
4 https://www.examinationbuzz.com/2021/03/apradh-ki-kanooni-avdharna.html

पर खतरा मानते हुए अनैतिक या गैरकानूनी करार देता है। सच कहें तो नियम-कानूनों के बिना समाज में शांति-व्यवस्था की कल्पना भी नहीं की जा सकती, क्योंकि कानून ही तो यह परिभाषित करता है कि कौन से कृत्य या आचरण समाज के लिए हानिकारक हैं और वो कौन सी संस्थाएं हैं जो कानून के अनुसार व्यवस्थाएं बनाने के लिए उत्तरदायी हैं। वस्तुतः कानून के तहत दंड के प्रावधान इसी उद्देश्य से रखे जाते है कि समाज के सदस्यों को एक-दूसरे और शासन एवं कानून-व्यवस्था के प्रति ऐसे व्यवहार से रोका जा सके जो विधि-सम्मत सामाजिक, आर्थिक व राजनैतिक व्यवस्थाओं पर कुठाराघात करते हों। इसीलिए हर देश के कानून में कुछ कृत्यों को वर्जित बताते हुए "अपराध" के रूप में परिभाषित किया गया है।

अपराध कई किस्म के होते हैं और प्रत्येक अपराध एक अलग किस्म की क्षति पंहुचाता है। कुछ अपराध मनुष्य के लिए घातक होते हैं जैसे-लूट, हत्या, बलात्कार, तो कुछ अपराध सम्पत्ति को क्षति पंहुचाते हैं, जैसे- चोरी या आगजनी, वहीं कुछ अपराध शासन एवं कानून-व्यवस्था को नुकसान पहुंचाते हैं जैसे- न्याय प्रक्रिया में बाधा डालना, राजद्रोह इत्यादि। इसी प्रकार कुछ अपराध नैतिकता के विरुद्ध होते हैं, जैसे- अश्लीलता, जुआ-सट्टा आदि।

मानवीय व्यवहार का एक अंतर्निहित स्वरुप होने के कारण मानव के भीतर आपराधिक प्रवृत्तियां निसंदेह प्रारंभिक काल से ही पनपती रही हैं। इससे यह ज़ाहिर तौर पर कहा जा सकता है कि जैसे-जैसे मानव सभ्यता, संस्कृति और विज्ञान का विकास होता आया है, मानव समाज में विद्यमान आपराधिक प्रवृत्तियां भी नित्य नया स्वरुप धारण करती रही हैं। विश्व में मानव सभ्यता का चरणबद्ध विकास होने के साथ-साथ सामाजिक, आथिक, राजनैतिक, वैज्ञानिक, तकनीकी और जनसंख्या संबंधी परिवर्तनों के अनुरुप आपराधिक

प्रवृत्तियां भी अपना स्वरूप बदलती रही हैं। कालांतर में आपराधिक प्रवृत्तियों ने समाज की हर करवट पर एक नई करवट ली है। जब-जब सभ्यता और समाज आधुनिकता की ओर बढ़े हैं अपराधियों ने भी बड़े ही शातिराना अंदाज में उसी तेज़ी से आगे बढ़ते हुए नित्य नए अपराधों को अंजाम दिया है।

मानव सभ्यता के विकास के साथ पनपती आपराधिक प्रवृतियों की इस मूल अवधारणा पर चर्चा के बाद अब बात आती है इस पुस्तक की मूल विषय-वस्तु यानि साईबर अपराध की अवधारणा, उदभव और इतिहास के चिंतन एवं विश्लेषण की।

साइबर अपराध की अवधारणा

साइबर अपराध की अवधारणा अपने आप में बहुत ही व्यापक है, किन्तु इसे समझना इतना जटिल भी नहीं है। यदि कुछ जटिल है, तो वह है, साइबर अपराधों से जूझना। साइबर शब्द का प्रयोग आज बहुत ही व्यापक अर्थों में किया जाता है, किन्तु इसकी सम्पूर्ण अवधारणा और वर्तमान परिपेक्ष्य में इसके प्रयोग के आयामों को समझने के लिए सबसे पहले इस शब्द की उत्पत्ति के बारे में जानना सबसे ज़्यादा ज़रूरी है। दरअसल, यहां सबसे पहले यह जानना प्रासंगिक है कि आख़िर ये 'साइबर' शब्द आया कहाँ से? इसका प्रयोग किन अर्थों को लेकर आगे बढ़ा? और आज सूचना एवं संचार प्रोद्यौगिकी के इस युग में किन-किन व्यापक अर्थों में इसका प्रयोग किया जा रहा है? हालांकि तकनीकी विशेषज्ञों के बीच इस शब्द के उद्भव और इसके अर्थों को लेकर निरंतर मतभेद बने रहे हैं, किन्तु यदि इस शब्द की जीवन-यात्रा पर एक नज़र डालें तो हम इस शब्द के समग्र अस्तित्व को आसानी से समझ सकते हैं।

वस्तुत: सभी भाषाओं में 'साइबर (Cyber)'शब्द अपनी इसी वर्तनी और उच्चारण के साथ व्यापक रूप से अपनी पैठ बना चुका है, अर्थात मानक रूप में इसका कोई और नाम या अन्य पर्यायवाची कहीं नहीं मिलता है। अतएव हिन्दी भाषा में भी यह शब्द इसी स्वरूप अर्थात'साइबर'के रूप में प्रचलित है। अपने रोज़मर्रा के जीवन में आज हम साइबर-स्पेस, साइबर-जोन, साइबर-कैफे, साइबर-अटैक जैसे अनेक शब्द पढ़ते, सुनते और इस्तेमाल करते हैं। किन्तु मूल रूप से 'साइबर' शब्द की उत्पत्ति जिस शब्द से मानी जाती हैं, वह शब्द है 'साइबरनेटिक्स'।

सबसे पहले, 1940 के दशक के अंतिम वर्षों में 'साइबरनेटिक्स' शब्द का प्रयोग एक ऐसी पद्धति के लिए किया गया था, जो मानव और मशीनों के बीच नियंत्रण और संचार का माध्यम बनी।[5] उस समय 'साइबरनेटिक्स' के कार्यक्षेत्र में मूल रूप से कम्प्यूटर-विज्ञान, इंजीनियरिंग, जीव-विज्ञान तथा इन क्षेत्रों में हो रही प्रगति से जुड़ी गतिविधियां शामिल थीं।

'साइबरनेटिक्स' शब्द की उत्पत्ति यूनानी (ग्रीक) शब्द kubernētēs से मानी जाती है, जिसका अंग्रेजी पर्याय है- Pilot या Steersman, यानि विमान-चालक या खेवैया। दूसरे शब्दों में इसे एक पथ-प्रदर्शक या मार्गदर्शक भी कहा जा सकता है। इसे सीधे अर्थों में समझें तो उस जमाने में 'साइबरनेटिक्स' का अर्थ एक ऐसी पद्धति से था, जो कम्पयूटर-विज्ञान, इंजीनियरिंग या जीव-विज्ञान आदि के क्षेत्रों में मानव के द्वारा, भविष्य के लक्ष्यों की प्राप्ति के उद्देश्यों से, विभिन्न संसाधनों और मशीनों आदि के बेहतर से बेहतर प्रयोग में एक मार्गदर्शक या पथ-प्रदर्शक की भूमिका निभा रही थी। इस प्रकार से 'साइबरनेटिक्स' का संबंध ऐसी गतिविधियों से था, जो इन सभी क्षेत्रों में भविष्य के अत्याधुनिक ढांचे और कार्यविधियों को तैयार करने का लक्ष्य रखती थीं। दरअसल 'साइबर' शब्द 'साइबरनेटिक्स' का ही संक्षिप्त

5 https://www.thefreedictionary.com/cyberneticians

व नवनिर्मित स्वरूप था, जिसका प्रयोग बदलते वैश्विक परिवेश में प्रत्यक्ष रूप से कम्प्यूटर-विज्ञान और इन्टरनेट से जुड़े सभी क्षेत्रों एवं संसाधनों के प्रतिनिधि-पर्याय के रूप में किया जाने लगा। धीरे-धीरे 'साइबर' शब्द इस क्षेत्र में कई नए शब्द गढ़ने का एक 'सशक्त' उपसर्ग (Prefix) बनता चला गया। तभी तो 'साइबर' शब्द के मेल से अब तक लगभग 500 से भी अधिक शब्द गढ़े जा चुके हैं और इनमें से अधिकांश प्रयोग की दृष्टि से बेहद प्रचलित हैं, जैसे- साइबर-अटैक, साइबर-सिक्यूरिटी, साइबर-कम्यूनिटी, साइबर-पार्क इत्यादि।

निसंदेह, वर्तमान परिवेश में 'साईबर' शब्द को एक सरल तरीके से, किन्तु अर्थ की दृष्टि से बहुत ही व्यापक रूप से कुछ इस प्रकार परिभाषित किया जा सकता है- "साइबर यानि वह वस्तु, स्थान, या पद्धति जिसका संबंध कम्पयूटर या परस्पर जुड़े कम्प्यूटरों के समूहों अर्थात कम्प्यूटर-नेटवर्क/ इंटरनेट और उनसे जुड़े अन्य संचार माध्यमों से हो'।

अब यदि इस'साइबर' शब्द को'अपराध' का उपसर्ग (Prefix) बना दिया जाए तो जो नया युग्म-शब्द तैयार होता है, वह है साइबर-अपराध। साइबर शब्द से भली-भांति परिचित होने के पश्चात हम सीधे तौर पर कह सकते हैं कि साइबर-अपराध का तात्पर्य उन ग़ैरकानूनी गतिविधियों से है जिन्हें कम्प्यूटर-नेटवर्क एवं सूचना और संचार प्रौद्योगिकी से जुड़े इलेक्ट्रानिक उपकरणों तथा इन्टरनेट के माध्यम से या उनकी मदद से अंजाम दिया जाता है।

'साइबर अपराध एक ऐसा अपराध है जिसमें कम्प्यूटर एवं नेटवर्क का इस्तेमाल किया जाता है। इस श्रेणी में गैरकानूनी ढंग से म्यूजिक फाइलों को डाउनलोड करने से लेकर ऑनलाइन बैंक खातों से पैसा चुराना तक कई किस्म के अपराध आते हैं। साइबर अपराधी हमेशा धन के लालच में साइबर अपराध नहीं करते। साइबर अपराधों में गैर-आर्थिक अपराध भी शामिल होते हैं। इसमें कई तरह की धोखाधड़ी जैसे नौकरी संबंधी धोखाधड़ी,

विवाह संबंधी धोखाधड़ी, संवेदनशील व्यक्तिगत जानकारी (जैसे-आधार से जुड़ी सूचनाएं, क्रेडिट/डेबिट कार्ड की जानकारी, बैंक खाते की जानकारी इत्यादि) की चोरी और गलत इस्तेमाल, सोशल मीडिया पर किसी व्यक्ति की मानहानि, कम्प्यूटर वायरस का प्रसार इत्यादि सभी शामिल होता है।[6]

सामान्य अपराधों की भांति साइबर-अपराधों में भी ऐसे कृत्य एवं आचरण शामिल होते हैं, जो अनैतिक हैं और समाज व कानून-व्यवस्था को क्षति पंहुचाते हैं। फिर भी साईबर अपराध, सामान्य अपराधों से इसलिए भिन्न हैं, क्योंकि इन्हें अलग तरीकों से अंजाम दिया जाता है। मसलन, आम तौर पर एक अपराधी किसी पर हमला करने के लिए बंदूक, चाकू या किसी धारदार हथियार का प्रयोग करता है, लेकिन साइबर जगत की यदि बात की जाए तो यहां अपराध या हमले प्रत्यक्ष नहीं बल्कि परोक्ष रूप से किसी कम्प्यूटर-नेटवर्क अथवा संचार माध्यमों के जरिये किए जाते हैं।

हालांकि कई बार कम्पयूटर का इस्तेमाल साईबर अपराधों के अलावा पारम्परिक किस्म के अपराधों में भी किया जाता है, लेकिन जहां तक साइबर अपराध का प्रश्न है, इसमें कम्प्यूटर एवं सूचना-प्रौद्योगिकी की मदद से अंजाम दिए जाने वाले कुछ खास किस्म के अपराध शामिल होते हैं, जैसे- जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, कम्प्यूटर से व्यक्तिगत सूचनाएं चुराना, फ़िशिंग, अवैध डाउनलोडिंग, साइबर स्टॉकिंग, वायरस प्रसार और ऐसी ही कई अन्य प्रकार की आपराधिक गतिविधियां।साईबर अपराधों की श्रेणी में कम्पयूटर-इंटरनेट एवं सूचना व संचार प्रौद्योगिकी से जुड़े संसाधनों का प्रयोग करते हुए अंजाम दिए जाने वाले कई अन्य किस्म के संगठित अपराध भी आते हैं, मसलन-किसी के बैंक खाते का विवरण हासिल कर वहां से सारी गोपनीय जानकारी चुरा लेना या किसी कम्पनी का विवरण चुरा लेना और फिर उसे अपने गलत इरादों के लिए इस्तेमाल में

6 https://cybercrime.gov.in/pdf

लाना। इन ग़ैरकानूनी गतिविधियों में कई बार तो किसी कम्प्यूटर या नेटवर्क का इस्तेमाल किसी अपराध को अंजाम देने के लिए किया जाता है और कई बार अपराधियों द्वारा किसी व्यक्ति या संस्था के कम्पयूटर को साईबर हमले का शिकार भी बनाया जाता है।

यथार्थ रुप से साईबर अपराध ऐसे अपराध हैं जो कम्पयूटर, इंटरनेट एवं सूचना-संचार माध्यमों से किसी व्यक्ति या व्यक्तियों के समूह को निशाना बना कर किए जाते हैं तथा इनमें अपराधियों का मकसद किसी व्यक्ति या संस्था की छवि धूमिल करने से लेकर उसे शारीरिक या मानसिक क्षति पहुंचाना या उसकी धन-सम्पत्ति को नुकसान पहुंचाने तक कुछ भी हो सकता है। इन अपराधों में अत्याधुनिक सूचना एवं संचार प्रौद्योगिकी और उससे जुड़े संसाधनों का इस्तेमाल होता है और ऐसा करके अपराधी अपने शिकार को प्रत्यक्ष व परोक्ष रुप से भारी नुकसान पहुंचा सकते हैं। साईबर अपराधों को अंजाम देने के लिए अपराधी प्राय: चेटरूम, ई-मेल, नोटिस बोर्ड, इंटरनेट व सोशल मीडिया पर बने लोगों व संस्थाओं के समूहों तथा मोबाईल फोन व स्मार्ट फोन आदि को ज़रिया बनाते हैं, जहां मनचाहा शिकार बड़ी ही आसानी और तेज़ी से उनके चंगुल में फंस जाता है। आज के युग में साईबर अपराधों ने एक और बड़ी चुनौती सामने रख दी है और वो है अश्लीलता फैलाना तथा निजता यानि प्राईवेसी को ख़तरा, जिसमें संचार माध्यमों के इस्तेमाल से किसी व्यक्ति की बेहद निजी तस्वीरें या वीडियो व अन्य जानकारी हासिल कर जग-जाहिर कर दी जाती हैं या उसका इस्तेमाल कर मानवीय प्रतिष्ठा को अपूर्णनीय क्षति पहुंचाई जाती है।

विश्व स्तरीय व्यापक दृष्टिकोण से देखें तो साईबर अपराध किसी राष्ट्र की सुरक्षा और उसकी अर्थव्यवस्था के लिए भी बहुत बड़ा ख़तरा सिद्ध हो रहे हैं। नित्य विकसित होती सूचना-प्रौद्योगिकी ने अंतरराष्ट्रीय स्तर पर ऐसे अवसर उपलब्ध करा दिए हैं, जिनमें एक देश या कोई आंतकी संगठन बड़ी ही

चालाकी से सूचना व संचार प्रौद्योगिकी का सुनियोजित प्रयोग किसी अन्य देश के विरुद्ध साईबर हथियार के रुप में कर सकता है।

साईबर अपराधों का उद्भव और इतिहास

क. विश्वस्तरीय परिदृश्य

ये बात बहुत ही आसानी से समझी जा सकती है कि मानव ने अपने जीवन को सरल और सहज बनाने के लिए शुरु से ही प्रयास आरंभ कर दिए थे। इस संसार में मनुष्य ही वो प्राणी है, जिसने अपने अस्तित्व और सहूलियतों के लिए दुनिया के बाकी प्राणियों की अपेक्षा सबसे तेज़ प्रयास किए हैं और इस तथ्य को कभी भी किसी प्रमाण की आवश्यकता नहीं रही है। मानव ने आग और पहिए से लेकर आज की अत्याधुनिक दुनिया तक अविष्कार ही अविष्कार किए हैं। समाज में रहना और परस्पर जुड़ना मनुष्य की जन्मजात प्रवृत्तियों में से एक हैं और यही वह कारण है जिसके चलते मनुष्य शुरु से ही आपस में एक दूसरे की जरूरतों को पूरा करता आया है। मानव सभ्यता की यही व्यवस्था उसके विकास का मूल आधार बनी है। आवश्यकताओं के अनुसार मनुष्य ने मांग और उसकी पूर्ति की पृष्ठभूमि को आधार बना कर जो सिद्धांत गढ़े हैं, उन्हीं ने इस दुनिया में बुनियादी रूप से अर्थव्यव्था और उसके साथ कई अन्य व्यवस्थाओं को जन्म दिया है, जिनके दम पर आज ये पूरी दुनिया कायम है।

प्रकृतिवश एक सामाजिक प्राणी होने के नाते मनुष्य ने परस्पर संपर्क को आदि काल से ही बढ़ावा दिया है। निश्चित रूप से मानव ने सबसे पहले आपसी संवाद हेतु सांकेतिक विधियां अपनाई होंगी, जो आगे चल कर नए-नए स्वरूपों में संचार का माध्यम बनी। इसके बाद ही भाषाओं का विकास हुआ और संपर्क के बुनियादी साधन विकसित किए गए। इस प्रकार विज्ञान का हाथ थाम कर मानव शनै: शनै: अत्याधुनिक सूचना व संचार क्रांति तक

आ पहुंचा। इस बीच परपस्पर प्रत्यक्ष संपर्क और वार्तालाप के अलावा एक दूसरे से दूर रह कर भी संदेशों के आदान-प्रदान हेतु मानव ने कई तरकीबें इज़ाद की। इनमें आग और धुंए के संकेतों के इस्तेमाल से लेकर संदेश वाहकों या कबूतरों के माध्यम से पत्र व चिट्ठियां भेजना भी शामिल है और इसके बाद दूरभाष यंत्रों के माध्यम से संवाद, तार, टेलीग्राम आदि की व्यवस्थाएं भी शामिल हैं तथा कम्प्यूटर युग की क्रांतिकारी दृश्य-श्रव्य संचार सुविधाएं भी शामिल हैं। सूचना एवं संचार प्रौद्योगिकी से जुड़े साधन आज इतने समर्थ, सुलभ व लोकप्रिय हो गए हैं कि भौतिक दूरियां होने के बावजूद भी मनुष्य एक दूसरे के बारे में दूर रह कर भी सब कुछ जान, देख व समझ सकता है। ऐसे में सूचना व संचार माध्यमों से अपराध को अंजाम देना कई वर्षों पहले से ही आसान हो गया है।

दरअसल अपराध को समझना, मानव सहजवृत्ति को समझना ही तो है। निसंदेह मानव की जो चाहत सीधे-सच्चे व आसान रास्ते से पूरी नहीं होती, उन्हें या तो वह नैतिकतापूर्वक अपने भीतर ही दबा लेता है या फिर साम-दाम-दण्ड-भेद की नीति से या झूठ, झल-कपट, हेराफेरी, चोरी, डकैती और अपराधों के जरिये पूरा करने कोशिश करता है और ऐसी ही मनोवृत्तियों से मानव के भीतर आपराधिक प्रवृत्तियां प्रबल होती जाती हैं। निश्चित रुप से साइबर अपराधों का उद्भव भी मानव के भीतर मौजूद ऐसी ही आपराधिक मनोवृत्तियों की पृष्ठभूमि पर हुआ है, फर्क सिर्फ इतना है कि इन अपराधों में वह शीरीरिक बल और हथियारों के प्रयोग के स्थान पर सूचना व संचार माध्यमों का इस्तेमाल करते हुए अपने मकसद की पूर्ति के लिए शातिराना मानसिक क्षमताओं से काम लेने लगा है।

यह शाश्वत सत्य है कि विकार सदैव किसी न किसी व्यवस्था में ही उत्पन्न होते हैं, क्योंकि विकार प्रकृति से ही परजीवी होते हैं। जिस प्रकार समाज में अपराध सार्वभौमिक रुप से पनपते रहे हैं, वैसे ही साइबर जगत के

अस्तित्व में आने के बाद ही साइबर अपराधों की अवधारणा सामने आई है। चूंकि साइबर अपराधों का संबंध सीधे तौर पर कम्प्यूटर, इंटरनेट और सूचना एवं संचार प्रौद्योगिकी के संसाधनों से है, इसलिए निश्चित तौर पर इन अपराधों का उद्भव भी कम्प्यूटर एवं इंटरनेट के अविष्कार तथा विकासक्रम से जुड़ हुआ है। सूचना एवं संचार प्रौद्योगिकी द्वारा कायम सुविधाजनक एवं जनकल्याणकारी व्यवस्थाओं के बीच आपराधिक प्रवृत्तियों ने अपना कार्य बहुत ही शुरुआती दौर में आरंभ कर दिया था। साईबर अपराध के उद्भव की यदि बात की जाए तो इसे बस तभी से माना जा सकता है, जब से कम्प्यूटर की ख़ोज हुई। इसलिए साइबर अपराधों के उदभव एवं विकासक्रम को जानने के लिए कंप्यूटर प्रौद्योगिकी के विकासक्रम पर दृष्टिपात प्रासंगिक प्रतीत होता है।

इस दिशा में किए गए विश्लेषणों से ज्ञात होता है कि विश्व के पहले इलेक्ट्रॉनिक डिजिटल कम्प्यूटर को इयोवा यूनिवर्सिटी के भौतिक-शास्त्र एवं गणित के पूर्व प्राध्यापक जॉन विंसेन्ट एटानासोफ और इसी यूनिवर्सिटी के एक पूर्व छात्र क्लिफोर्ड बैर्री ने मिल कर सन् 1937 से 1942 तक किए गए अथक प्रयासों एवं अनुसंधानों के बाद तैयार किया था। इसीलिए इस पहले इलेक्ट्रॉनिक डिजिटल कम्प्यूटर का नाम 'एटानासोफ-बैरी कम्प्यूटर (एबीसी) रखा गया था।[7]

7 https://www.ece.iastate.edu/the-department/history/history-of-computing/

क्लिफोर्ड बैर्री अपने एबीसी कम्प्यूटर के साथ

विश्व के पहले डिजिटल कम्प्यूटर के 1943 में अस्तित्व में आने के बाद लगभग अगले दो दशकों तक अपराध जगत में कम्प्यूटरों का इस्तेमाल नहीं हो सका। ऐसा इसलिए था कि वास्तव में इन कम्प्यूटरों के माध्यम से अपराधों को अंजाम देने के बारे में कोई सोच भी नहीं सकता था। बड़े आकार की इलेक्ट्रानिक कम्प्यूटर मशीनों को संचालित करने की अनुमति कुछ ही लोगों को होती थी और ये कम्प्यूटर आपस में जुड़े हुए (नेटवर्क्ड) भी नहीं होते थे तथा बहुत थोड़े से लोग ही इन पर कार्य करना जानते थे, इसलिए उस समय ख़तरे की संभावनाएं न के बराबर थीं।[8]

अपराधियों द्वारा कम्प्यूटरों के इस्तेमाल की रिपोर्टें सबसे पहले 1960 के दशक में सामने आईं। यह वो समय था जब ज्यादातर कम्प्यूटर मेनफ्रेम सिस्टम थे। 1946 में कई कम्पनियों ने व्यवसायिक रूप से उपयोगी मेनफ्रेम कम्प्यूटरों के विकास पर काम करना आरंभ कर दिया था। 1951 में UNIVAC

8 https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

(Universal Automatic Computer) बनाया गया और इसका प्रयोग जनगणना के प्रयोजनार्थ किया गया।[9] 4 नवम्बर, 1952 को कोलम्बिया ब्रॉडकास्टिंग सिस्टम न्यूज़ ने रेमिंगटन रैंड यूनिवेक कम्प्यूटर का इस्तेमाल चुनाव परिणामों के अनुमान हेतु किया था, जिसके सटीक अनुमान प्राप्त हुए थे।[10]

1960 के आते-आते संयुक्त राज्य में 5000 मेनफ्रेम कम्प्यूटर हो गए थे और 1970 तक इनकी संख्या बढ़कर 80,000 तक जा पहुंची, जबकि 50,000 मेनफ्रेम कम्प्यूटर संयुक्त राज्य से बाहर दूसरे देशों में प्रयुक्त हो रहे थे। इसलिए यह कहना अतिश्योक्ति नहीं होगी कि 1960 के दशक से ही कम्प्यूटर अपराधों का चलन भी शुरू हो गया था। हालांकि 1960 एवं 1970 के दशकों के कम्प्यूटर अपराध आज की दुनिया के साइबर-अपराध से निसंदेह भिन्न थे। एक तो उस समय इंटरनेट नहीं था और दूसरे मेनफ्रेम कम्प्यूटर दूसरे कम्प्यूटरों से जुड़े हुए नहीं होते थे।[11] 1960 में विकसित मेनफ्रेम कम्प्यूटर केन्द्रीयकृत कम्प्यूटिंग सिस्टम के रूप में काम करते थे और लोकल नेटवर्क कनेक्शन एवं रिमोट डायल-अप कनेक्शन के माध्यम से कई टर्मिनल इस केन्द्रीयकृत कम्प्यूटिंग सिस्टम से जुड़े रहते थे। प्रयोगकर्ता अपनी टेक्सट-बेस्ड कमाण्ड्स इन टर्मिनलों के माध्यम से दर्ज करते थे और ये टर्मिनल इन कमाण्ड्स को मैनफ्रेम को भेज देते थे, जहां सम्पूर्ण प्रोसेसिंग की जाती थी। इसके बाद प्रोसेसिंग का जो भी परिणाम निकलता था उसे वापस टर्मिनल को भेज दिया जाता था, जो टर्मिनल पर दिखाई भी देता था।[12]

9 Susan W.Brenner, CYBER CRIME : Criminal Treats from Cyberspace, First Indian Addition-2012, Pentagon Press, New Delhi, pp.10.

10 https://www.poynter.org/reporting-editing/2014/today-in-media-history-in-1952-a-univac-computer-helped-cbs-news-predict-the-winner-of-the-presidential-election.

11 Susan W.Brenner, CYBER CRIME : Criminal Treats from Cyberspace, First Indian Addition-2012, Pentagon Press, New Delhi, pp.10-11

12 https://networkencyclopedia.com/mainframe/

1960 के दशक का एक मेनफ्रेम कम्प्यूटर

दरअसल, मेनफ्रेम कम्प्यूटर आकार में इतने बड़े होते थे कि उन्हें रखने के लिए एक पूरा कमरा चाहिए होता था। साथ ही विशेष किस्म के एक एयर-कंडीशनिंग सिस्टम की भी आवश्यकता होती थी ताकि इस मशीन के वैक्यूम ट्यूब ज्यादा गर्म होकर कम्प्यूटर के भीतर सूचनाओं को नुकसान न पहुंचा सकें। अब चूँकि मेनफ्रेम अन्य किसी कम्प्यूटर से जुड़े नहीं होते थे और उनके इस्तेमाल में एक जटिल प्रक्रिया अपनानी पड़ती थी, इसलिए उनके साथ छेड़खानी करके कम्प्यूटर अपराधों को अंजाम देना बहुत थोड़े लोगों के हाथ की बात थी। वस्तुत: सीधे तौर इन मेनफ्रेम कम्प्यूटरों के संचालन से जुड़े भीतरी लोग ही इस तरह के कृत्यों को अजांम दे सकते थे। अत: इस जमाने में जितने भी कम्प्यूटर-अपराध घटित हुए वे इसी व्यवस्था के इर्दगिर्द बने रहे। ये कर्मचारी कभी अन्य कर्मचारियों की जासूसी करने के लिए उनकी गोपनीय जानकारियां पढ़ लेते थे, तो कभी डांट-डपट व अनुशासनात्मक कार्रवाई का बदला लेने के लिए कम्प्यूटरों को अथवा उनमें सुरक्षित सूचनाओं को अंदरूनी क्षति पहुंचा देते थे। इस दौर में ऐसे अपराध होते रहे, लेकिन जो सबसे ज्यादा आम अपराध थे वे आर्थिक क्षति पहुंचाने संबंधी अपराध थे, क्योंकि संस्था के कर्मचारी मेनफ्रेम कम्प्यूटरों को अपने आर्थिक फायदों के

लिए भी प्रयोग में लाने लगे थे।[13]

उदाहरणतया- 1960 के दशक के मध्य में 'वाल स्मिथ' नामक व्यक्ति एक कम्पनी में काम करता था। उसके पास एक छोटा यूनीवेक कम्प्यूटर था, जिससे वह अपनी कम्पनी को कम्प्यूटर संबंधी सेवाएं प्रदान किया करता था। समय के साथ स्मिथ को ये लगने लगा था कि कम्पनी उसका गलत इस्तेमाल कर रही थी और उसके द्वारा कमाए गए धन में से भी उसे ही ठग रही थी। ऐसे में स्मिथ ने यह फैसला किया कि वह कम्पनी के खातों और कम्प्यूटिंग सिस्टम तक पहुंच कर अपने नुकसान की भरपाई करेगा। तब उसने कुछ फर्जी कम्पनियां बनाईं और अपने नियोक्ता को काल्पनिक सेवाएं देते हुए फर्जी बिल थमाना शुरु कर दिया। इसके बाद स्मिथ ने बिलिंग की प्रक्रिया को पूरा करने के लिए कम्प्यूटर का गलत इस्तेमाल किया तथा कम्पनी को होने वाले लाभ की राशि भी कम दिखाना शुरु कर दिया तथा बची हुई लाभ की राशि खुद ही रखने लगा। वो अपने इस गोरखधंधे में इतना सफल हुआ कि एक साल में 2,50,000 डॉलर तक कमाने लगा, जो 1960 के दशक में उस छोटे से शहर में रहने वाले एक एकाउंटेन्ट के लिए बहुत बड़ी रकम थी। स्मिथ ने बाद में कहा कि इस तरह के गबन को अपने मालिकों से छिपाना बहुत आसान था, क्योंकि वे मानते थे कि कम्प्यूटरों से निकलने वाले आंकड़े सौ फीसदी सही होते हैं। छह साल तक लगातार इस तरह का गबन करने के बाद जब स्मिथ ने मोटी रकम कमा ली तो वह नौकरी छोड़ने के बारे में सोचने लगा। तब उसने जानबूझ कर एक गलती कर दी और उस पर आपराधिक आरोप लगाए गए। जांच में स्मिथ ने अपनी गलती मान ली क्योंकि उसे भरोसा था कि उसे ज्यादा से ज्यादा 18 महीने की सजा सुनाई जाएगी और यह सजा उन लाखों डॉलर्स के आगे बहुत छोटी थी जो उसने अब तक कमा लिए थे। दुर्भाग्यवश न्यायालय ने उसे 10 वर्षों के कारावास की

13 Susan W.Brenner, CYBER CRIME : Criminal Treats from Cyberspace, First Indian Addition-2012, Pentagon Press, New Delhi, pp.10-11

सजा सुनाई, लेकिन इस बीच स्मिथ ने कॉलेज डिग्री हासिल कर ली और बहुत से कैदियों को भी पढ़ाया, जिसका नतीजा ये हुआ कि उसे साढ़े पांच साल में ही पे-रोल पर रिहा कर दिया गया। अब वो जेल से बाहर था और एक लखपति भी बन चुका था, जिसे कभी काम करने की जरूरत नहीं थी। इस तरह लखपति बनने की स्मिथ की कहानी भले ही अनूठी हो मगर उसका अपराध अनूठा नहीं था। उस दौरान कम्प्यूटर गबन के ऐसे कई मामले उजागर हुए थे और इनमें से कई तो ऐसे थे, जिनकी रिपोर्ट भी नहीं की गई थी।[14]

हालांकि इससे पहले 1950 के दशक के अंत से फोन फ्रेकिंग की घटनाएं भी शुरू हो चुकी थी और यहां उनका जिक्र इसलिए प्रासंगिक है कि हैकिंग, जिसके बारे में आगे विस्तार से चर्चा की जाएगी, टेलीफोन से उतना ही ताल्लुक रखता है, जितना कि कम्प्यूटरों से। 'फोन फ्रेक(Phone Phreak) उसे कहा जाता था जो अपने व्यक्तिगत लाभ के लिए टेलीफोन प्रणालियों का अध्ययन, परीक्षण और तकनीकी छेड़खानी कर उनका बेजा इस्तेमाल करता था। दरअसल, फोन फ्रेकिंग 1950 के दशक के अंत में शुरू हुई थी तथा 1960 के दशक के दौरान और 1970 के दशक की शुरुआत में इसका विश्व भर में खूब बोलबाला था। फोन फ्रेक घंटों तक टेलीफोन नेटवर्क पर नम्बर डायल करके ये समझने की कोशिश करते थे कि यह प्रणाली आखिर किस प्रकार काम करती है। वे क्लिक्स(clicks), क्लंक्स(clunks), बीप्स(beeps) और बूप्स (boops) की आवाजें सुनते रहते थे, ताकि उन्हें यह पता चल सके कि टेलीफोन काल्स किस तरह आगे भेजी जाती हैं। ये लोग टेलीफोन कम्पनियों की गोपनीय किताबों को भी पढ़ते रहते थे। धीरे-धीरे वो यह सीख लेते थे कि टेलीफोन कम्पनी के ऑपरेटरों और कर्मियों की तरह किस प्रकार बर्ताव किया जाए। इतना ही नहीं वे टेलीफोन कम्पनियों के कूड़ेदानों (ट्रेश-बिन) को भी खंखालते थे, ताकि कुछ गोपनीय दस्तावेज

14 Susan W.Brenner, CYBER CRIME : Criminal Treats from Cyberspace, First Indian Addition-2012, Pentagon Press, New Delhi, pp.11-12

उनके हाथ लग सकें। रात के समय वे चोरी-छिपे टेलीफोन कम्पनियों की इमारतों में घुस कर अपने टेलीफोनों को एक्सचेंज से जोड़ दिया करते थे। इन लोगों ने कुछ बहुत ही उन्नत व छोटे-छोटे इलेक्ट्रॉनिक यंत्र भी इजाद किए थे, जिन्हें ब्लू बॉक्स, ब्लैक बॉक्स और रेड बॉक्स कहा जाता था, जिससे वे मनचाहे नेटवर्क को खोज कर उस पर मुफ्त टेलीफोन काल्स कर सकते थे।[15] सीधे तौर पर फोन फ्रेकिंग मुफ्त टेलीफोन काल्स करने के लिए टेलीफोन सिगनलों का अवैध रूप से इस्तेमाल था। फ्रेकिंग में लम्बी दूरी की कॉल्स को जोड़ने या भेजने के लिए टेलीफोन कम्पनियों द्वारा इस्तेमाल की जाने वाली विशेष किस्म की ध्वनियों (tones) को समझ कर उनका गलत इस्तेमाल किया जाता था। दरअसल इन ध्वनियों की तरह ध्वनियां निकाल कर फ्रेकिंग करने वाले लोग पूरी दुनिया में कहीं भी मुफ्त टेलीफोन कॉल्स कर सकते थे।। कुल मिला कर यह संचार उपकरणों से गैरकानूनी छेड़खानी करके अंजाम दिया जाने वाला एक संगठित अपराध था, जो 1983 में उस समय स्वत: अस्तित्वहीन हो गया जब टेलीफोन कम्पनियों ने कॉमन चैनल इंटर-ऑफिस सिगनलिंग (सीसीआईएस) किस्म की टेलीफोन लाईनों का प्रयोग आरंभ कर दिया, जिसमें सिगनलिंग का ध्वनि की तारों से कोई सरोकार नहीं रहता था।[16]

वैसे तो कम्प्यूटर एवं इंटरनेट पर आधारित साइबर अपराधों की शुरुआत मूलतः हैकिंग से ही मानी जाती है। उपरोक्त अनुच्छेदों में उल्लिखित तथ्यों के अनुसार 1960 के दशक में देखे गए कम्प्यूटर अपराधों के मामले भी मूलतया हैकिंग पर ही आधारित कहे जा सकते हैं। इस दशक में द्वेषपूर्ण हैकिंग की सबसे पहली घटना मैसाचुसेट्स इंस्टीट्यूट ऑफ टेक्नालॉजी (एमआईटी) में घटित हुई थी और यहीं से हैकिंग की संस्कृति भी शुरु हुई। मैसाचुसेट्स पूर्वोत्तर संयुक्त राज्य अमेरिका के न्यू इंग्लैंड क्षेत्र में एक राज्य

15 http://www.historyofphonephreaking.org/faq.php
16 https://www.britannica.com/topic/phreaking

है। दरअसल, 1960 के दशक के मध्य तक ज्यादातर कम्प्यूटर बड़े-बड़े मेनफ्रेम होते थे, जिन्हें वातानुकूलित कमरों में बंद रखा जाता था। ये मशीनें बहुत कीमती होती थी और इसीलिए कुछ प्रोग्रामर ही इन तक पहुंच सकते थे। एमआईटी संस्थान के कुछ छात्र कम्प्यूटरों और उनकी प्रोग्रामिंग में काफी रुचि रखते थे, लेकिन उनकी समस्या ये थी कि संस्थान के मेनफ्रेम कम्प्यूटरों तक केवल उनके प्राध्यापक एवं प्रोगामर ही जा सकते थे। हालांकि पहले भी इन कम्प्यूटरों तक पहुंचने वालों ने हैकिंग के प्रयास किए थे और उस समय इन प्रयासों के मकसद आर्थिक या कोई राजैनतिक किस्म का लाभ उठाना नहीं होता था। हैकिंग करने वाले ज्यादातर लोग जिज्ञासु व उपद्रवी प्रवृति के होते थे अथवा हैकिंग के ऐसे प्रयास सिस्टम को और ज्यादा बेहतर व दक्ष बनाने के लिए जानबूझ कर किए जाते थे। सन् 1967 में आईबीएम ने अपने यहां कुछ स्कूली बच्चों को अपने कम्प्यूटरों पर हाथ अजमाने के लिए बुलाया। इन छात्रों ने न केवल दी गई अनुमति के अनुसार कम्प्यूटरों का संचालन करके देखा, बल्कि वे इनके भीतर अनाधिकृत प्रवेश कर सिस्टम लैंग्वेज सीखने का भी प्रयास करने लगे और कम्प्यूटर के अन्य हिस्सों से भी छेड़खानी करने लगे। कम्पनी के लिए यह एक बहुत बड़ी सीख थी, क्योंकि कम्पनी इस अभ्यास से कम्प्यूटर सिस्टम की सुरक्षा के प्रति सजग हो चुकी थी और उसने रक्षात्मक उपायों की दिशा में अनुसंधान शुरू कर दिया था। इतना ही नहीं इस प्रयोग के बाद से कम्प्यूटर के विकास में लगे अनुसंधानकर्ताओं व निर्माताओं ने एक नई रक्षात्मक सोच के साथ काम करना शुरु कर दिया। दरअसल ये एथिकल हैकिंग(Ethical Hacking) का एक उदाहरण था, जिसका इस्तेमाल आज भी बहुत प्रासंगिक है। इसके बाद जैसे कम्प्यूटरों का आकार छोटा होता चला गया, कई बड़ी-बड़ी कम्पनियों ने ऐसी प्रौद्योगिकी के विकास में निवेश करना आरंभ कर दिया, जिससे उनका डाटा और सिस्टम सुरक्षित रहें। अब कम्प्यूटर सिस्टम और उसमें समाहित डाटा को तालों में बंद रखना व्यर्थ था, क्योंकि उन तक ज्यादा से ज्यादा लोग पहुंचने लगे थे

और यहीं से "पासवर्ड" जैसे सुरक्षा उपायों का इस्तेमाल शुरू हो गया।[17]

आज की दुनिया के साइबर अपराधों में कम्प्यूटर, इंटरनेट, स्मार्ट फोन, मोबाइल फोन तथा सभी संचार सुविधाओं का अत्यधिक इस्तेमाल देखा जा रहा है। वस्तुत: आज के इन अपराधों की जड़े मानव सभ्यता के इतिहास में ही दबी हुई हैं। हम जानते हैं कि बुनियादी तौर पर संचार सुविधाओं का अविष्कार कम्प्यूटरों से भी कई वर्षों पहले हुआ था। दरअसल दूरसंचार की शुरुआत 1844 में सेमुअल मोर्स द्वारा अविष्कृत टेलीग्राफ सिस्टम से हुई थी। इसके बाद 1870 के दशक में इलेक्ट्रिक टेलीफोन का अविष्कार हुआ। दो तरफा संचार में सक्षम पहली व्यवसायिक टेलीफोन प्रणाली की स्थापना 1878-1879 में न्यू हैवन और लंदन के बीच हुई थी।[18] निसंदेह दूरसंचार ने कम्प्यूटरों एवं इंटरनेट के विकास में ऐसा सहयोग दिया है कि दूरसंचार के बिना कम्प्यूटर और इंटरनेट प्रौद्योगिकी की कल्पना भी नहीं की जा सकती थी। साइबर अपराधों की ऐतिहासिक पृष्ठभूमि के इस विश्लेषण में यह जानना भी प्रासंगिक प्रतीत होता है कि आखिर अपराध जगत में तकनीक का दुरुपयोग कब से और कैसे आरंभ हुआ। वस्तुत: कम्प्यूटरों के अविष्कार से पहले ही हैकर्स ने अपना काम शुरू कर दिया था। वे फोन-नेटवर्क, पंच-कार्ड मशीनों और टेलीग्राफ सिस्टम में सेंध लगाने लगे थे। इनमें से कुछ हैकर्स ये सब कुछ अपने फायदे के लिए करते थे तो कुछ अन्य परोपकारी उद्देश्यों के लिए। इस बारे में किए विस्तृत विश्लेषण और अनुसंधान से हमें तकनीक-आधारित अपराधों की एक लम्बी फेहरिस्त मिलती है, जो यह दर्शाती है कि दरअसल आपराधिक प्रवृत्तियों ने इन संसाधनों का दुरुपयोग टेलीग्राफ के अविष्कार के बाद से ही आरंभ कर दिया था। यहां मुख्य रुप से 1834 में टेलीग्राफ सिस्टम के अविष्कार से लेकर सूचना प्रौद्योगिकी के

17 https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

18 https://www.technofunc.com/index.php/domain-knowledge-2/telecom-industry/item/history-of-telecommunications-industry.

अत्याधुनिक स्वरूप में आने अर्थात वर्ष 2000 तक के कुछ प्रकरणों का उल्लेख उदाहरण स्वरूप किया गया है, ताकि हमें यह समझने में आसानी हो कि तकनीक-आधारित अपराधों की प्रवृत्तियां संचार सुविधाओं और कम्प्यूटरों के विकासक्रम के साथ ही विकसित होती आयी हैं-

1. 1834 में कुछ चोरों ने फ्रांस के टेलीग्राफ सिस्टम को हैक कर लिया था और वित्तीय बाजार से जुड़ी जानकारियां चुरा ली थीं। कदाचित यह दुनिया का पहला साइबर हमला था।[19]

2. 1870 में एक नवयुवक को स्विचबोर्ड ऑपरेटर के काम पर लगाया गया था, चूंकि वह टेलीफोन कॉल्स को डिस्कनेक्ट करता सकता था और रिडॉयरेक्ट भी कर सकता था, इसलिए उसने इस सुविधा का लाभ अपने व्यक्तिगत हितों के लिए उठाना शुरू कर दिया था। इसे हैकिंग की शुरूआत ही कहा जा सकता है।[20]

3. 1878 में, यानी अलेक्ज़ेंडर ग्रहम बेल द्वारा टेलीफोन के अविष्कार के महज दो वर्षों बाद, टेलीफोन कम्पनी ने न्यूयॉर्क में कुछ किशोरों को इसलिए नौकरी से निकाल दिया था कि वे जानबूझकर ग्राहकों की कॉल्स को इधर-उधर जोड़ देते थे या डिसक्नेक्ट कर देते थे। टेलीफोन के अविष्कार के बाद शुरूआती दौर में ग्राहकों की टेलीफोन कॉल्स को टेलीफोन ऑपरेटरों द्वारा स्विचबोर्ड के माध्यम से जोड़ा जाता था। उस समय किशोर बालकों को इस काम पर लगाया गया था, क्योंकि वे पहले टेलीग्राफ सिस्टम पर काम कर चुके थे। लेकिन वास्तव में वे उद्दण्ड निकले और उनका ध्यान इस बात पर ज्यादा केंद्रित

19 https://slate.com/technology/2018/10/what-an-1834-hack-of-the-french-telegraph-system-can-teach-us-about-modern-day-network-security.html

20 https://www.ukessays.com/essays/media/cyber-crime-in-the-21st-century-media-essay.php

रहने लगा कि यह सिस्टम आख़िरकार काम कैसे करता है और वे टेलीफोन के कनेक्शनों को ठीक से जोड़ने की बजाय उनसे छेड़खानी व हंसी-मजाक करने लगे थे। टेलीफोन कॉल्स हैकिंग का ये एक और उदाहरण था।[21]

4. 1903 में नेविल मासक्लेइन ने एक जीवंत टेलीग्राफ प्रदर्शन को हैक कर लिया था और इसीलिए उसे दुनिया का पहला हैकर कहा जाता है। मासक्लेइन ने वायरलैस टेलीग्राफ के बाजार में उतरने तक की प्रतीक्षा नहीं की और उसके सबसे पहले प्रदर्शन में ही ख़लल डाल दिया। वायरलैस टेलीग्राफ के जनक गुल्येलमो मार्कोनी उस दिन एक प्रदर्शन के माध्यम से यह बता रहे थे कि उनका यह उपकरण किस प्रकार कार्य करता है। मार्कोनी जनता के सामने यह सिद्ध करना चाहते थे कि वायरलैस टेलीग्राफ बिल्कुल सुरक्षित था और इस पर जो भी संदेश भेजे जाते थे वे पूरी तरह सुरक्षित व गुप्त होते थे। नेविल मास्केलाइन जो पेशे से एक जादूगर, अन्वेषक और वायरलैस तकनीकि का जानकार था, ने अपमानजनक मॉर्स कोड संदेश भेज कर मार्कोनी के वायरलैस टेलीग्राफ को हैक कर लिया। जब प्रदर्शन शुरू हुआ तो प्रारंभिक संदेश को रिकॉर्ड करने के बाद वायरलैस टेलीग्राफ पहले तो बार-बार 'रेट्स' शब्द को दोहराने लगा और फिर अंग्रेजी की कविता की एक पंक्ति सुनाने लगा। इस सब से मार्कोनी बहुत अपमानित हुए। हालांकि नेविल मासक्लेइन ने खुद ही पत्र लिख कर यह उजागर कर दिया कि यह सब उसकी करामात थी और वह नहीं चाहता था कि लोग बिना तारों वाले एक उपकरण पर अपने संदेश भेजें, जो सुरक्षित नहीं होंगे।[22]

21 https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/

22 https://listverse.com/2018/05/14/10-early-hackers-from-before-the-invention-of-the-home-computer/

5. 1939 में द्वितीय विश्व-युद्ध के दौरान बेल्टचेली पार्क में कोडब्रेकर्स के रूप में तैनात एलेन टूरिंग और गोर्डोन बेलकेम्न ने BOMBE नाम की इलेक्ट्रो मैकेनिकल मशीन बनाई थी, जिससे उन्होंने जर्मन इनिग्मा के कोड ब्रेक कर लिए थे।[23]

6. 1940 में हिटलर की नाजी सेना के कब्जे वाले फ्रांस में विरोधी संस्था के एक सदस्य और कम्प्यूटर के पंच-कार्ड विशेषज्ञ रेने कार्मिल्ले ऐसी मशीनों को संभालते थे, जिसमें फ्रांस की विची सरकार अपने डाटा की प्रोसेसिंग करती थी। जब रेने को यह पता चला कि नाजी सेना के लोग यहूदियों का पता लगाने हेतु डाटा-प्रोसेसिंग में पंच-कार्ड का प्रयोग करना चाहते हैं तो उन्होंने अपनी मशीन उन्हें उपलब्ध करा दी और बाद में इस मशीन को हैक करते हुए उनकी योजना को नाकाम कर दिया। इसीलिए रेने कार्मिल्ले को दुनिया का पहला एथिकल हैकर (Ethical Hacker) कहा जाता है, जिन्होंने द्वितीय विश्व युद्ध में फ्रांस के यहूदियों के लिए तैयार कम्प्यूटरीकृत डाटा को नेस्तनाबूद कर दिया था।[24]

7. 1955 में संयुक्त राज्य अमेरिका में फोन हैकिंग या 'फोन फैक' की घटना सामने आई। दरअसल डेविड कॉनडॉन नामक युवक ये समझने की कोशिश का रहा था कि टेलीफोन पद्धति कैसे काम करती है। यही कोशिश करते करते उसने अपने टेलीफोन में एक खास किस्म की सीटी बजाई। कहा जाता है कि वो धुन 'डेवी क्रोकेट कैट' और 'केनरी बर्ड कॉल फ्लूट' की धुन थी। इत्तेफाकन उसकी सीटी से जो आवाज निकली वो एक 'सीक्रेट कोड' थी जिसे टेलीफोन सिस्टम ने पहचान लिया और यह समझ लिया कि डेविड कॉनडॉन उनका एक

23 https://www.cryptomuseum.com/crypto/bombe/
24 https://daily.jstor.org/wwii-and-the-first-ethical-hacker/

कर्मचारी है। फिर क्या डेविड को दूर बैठे एक टेलीफोन ऑपरेटर से जोड़ दिया गया, जो ये समझ रहा था कि डेविड उसका ही सहकर्मी है और वह ऑपरेटर बिना किसी शुल्क डेविड को मनचाहे फोन नम्बरों से जोड़ देता था। डेविड ने यह सब कुछ भले ही बहुत थोड़े पैसों के लिए किया था, लेकिन वो आने वाले समय के लिए फोन फ्रैक और हैकिंग जैसे अपराधों को नई दिशा दे गया था।[25]

8. 1962 में मैसाचुसेट्स इंस्टीट्यूट ऑफ टेक्नालॉजी (एमआईटी) ने छात्रों की निजता और समयावधि को सुनिश्चित करने के लिए पहली बार कम्प्यूटरों पर पासवर्ड का उपयोग किया। इस संस्थान के एक छात्र एलेन शेर ने एक ऐसा पंच-कार्ड तैयार किया जिससे कम्प्यूटर ने सभी पासवर्डों का प्रिंट उसे दे दिया और इस तरह वह दूसरे लोगों के स्थान पर लॉग इन करके ज्यादा समय तक कम्प्यूटर पर बैठने में सफल हो गया। उसने ये पासवर्ड अपने दोस्तों को भी दे दिए तथा इन छात्रों ने अपने अध्यापकों के एकाउंट्स भी हैक कर लिए और अवांछित संदेश भेज कर उनका मजाक बनाया।[26]

9. 1969 में एक अनजान व्यक्ति ने वाशिंगटन यूनीवर्सिटी के कम्प्यूटर सेंटर पर एक कम्प्यूटर में ऐसा छोटा सा प्रोग्राम इंस्टॉल कर दिया जो दिखाई नहीं देता था। यह प्रोग्राम खुद की कई सारी कॉपियां तब तक बनाता रहता था (खरगोशों की तरह बढ़ता रहता था), जब तक कि कम्प्यूटर ओवरलोड होकर काम करना बंद न कर दे। इसे रेबिट वायरस का नाम दिया गया और ऐसा माना जाता है कि यही दुनिया का सबसे पहला कम्प्यूटर वायरस था।[27]

25 https://listverse.com/2018/05/14/10-early-hackers-from-before-the-invention-of-the-home-computer/

26 https://www.herjavecgroup.com/history-of-cybercrime/

27 https://listverse.com/2018/05/14/10-early-hackers-from-before-the-invention-of-the-home-computer/

10. 1970-1995 के बीच केविन मिटनिक ने दुनिया के सबसे सुरक्षित नेटवर्कों में सेंध लगाई थी, जिसमें नोकिया और मोटोरोला जैसी कम्पनियां भी शामिल थी। वह अपनी व्यापक 'सोशल इंजीनियरिंग' तरकीबों के जरिये इन कम्पनी के कर्मचारियों को फुसला लेता था और उनसे विभिन्न कोड व पासवर्ड जान कर इन कम्पनियों के कम्प्यूटरों में भीतर तक सेंध लगा लेता था। केविन उस जमाने का सबसे कुख्यात साईबर अपराधी था।[28]

(सोशल इंजीनियरिंग एक ऐसी कला है जिसमें हैकिंग की तकनीकी तरकीबों की बजाय किसी संस्था के कर्मचारियों की मनोवृत्तियों का फायदा उठा कर उस संस्था की इमारत, कम्प्यूटरों और डाटा तक अपनी पहुंच बनाई जाती है।[29])

11. 1973 में न्यूयॉर्क के एक बैंक के रोकड़िया ने कम्प्यूटर का इस्तेमाल कर 2 मिलियन डॉलर का गबन किया था।[30]

12. 1981 में इयान मर्फी, जिसे उसके प्रशंसक 'कैप्टन जेप' के नाम से बुलाते थे, ने अमेरिकन टेलीफोन एंड टेलीग्राफ नेटवर्क को हैक कर लिया था और इसकी घड़ी का समय कुछ इस प्रकार बदल डाला था कि यह नेटवर्क व्यस्तम घंटों में भी किफायती दरों के बराबर प्रभार वसूलने लगा था। इयान मर्फी ही वह पहला व्यक्ति था जिसे साइबर अपराध के आरोप में दण्डित किया गया था।[31]

13. 1988 में कॉर्नेल यूनिवर्सिटी, न्यूयॉर्क के एक स्नातक छात्र रॉर्बट

28 https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/

29 https://www.csoonline.com/article/2124681/what-is-social-engineering.html

30 https://www.le-vpn.com/history-cyber-crime-origin-evolution/

31 https://www.le-vpn.com/history-cyber-crime-origin-evolution/

मोर्रिस ने सबसे पहला इंटरनेट वॉर्म (Internet Worm) बनाया, जिसके पीछे उसका मकसद web के आकार-विस्तार को जानना था। इस वॉर्म को 1988 में मैसाचुसेट्स इंस्टीट्यूट ऑफ टेक्नालॉजी (एमआईटी) के एक कम्प्यूटर पर छोड़ा गया, जिसका उद्देश्य ये जाहिर करना कि इस वॉर्म को एक छात्र द्वारा विकसित किया गया था। इस प्रकार के अभ्यास में किसी भी तरह की क्षति की संभावना नहीं थी, लेकिन जल्द ही यह अभ्यास एक विद्वेषपूर्ण "डिनाइयल-ऑफ-सर्विस-अटैक' के रूप में तबदील हो गया, क्योंकि इस वॉर्म का एक बग (Bug) पूरी कम्प्यूटर प्रणाली में फैलने लगा और कम्प्यूटरों को एक के बाद एक इतनी तेजी से संक्रमित करने लगा, जिसके बारे में मोर्रिस ने कभी कल्पना भी नहीं की थी। इससे पहले कि मोर्रिस इस बात को समझ पाता और प्रोग्रामरों को इस वॉर्म को नष्ट करने की युक्ति बता पाता, बहुत नुकसान हो चुका था। जब ये मालूम हुआ कि इस वॉर्म का रचियता मोर्रिस था तो उस पर 'कम्प्यूटर फ्रॉड एंड एब्यूज एक्ट' के प्रावधानों का उल्लंघन करने के लिए मुकद्मा चलाया गया तथा दण्डित किया गया।[32]

('Denial of Service Attack या DoS Attack' एक ऐसा हमला है जिससे किसी कम्प्यूटर/मशीन अथवा नेटवर्क को इस प्रकार ठप्प कर दिया जाता है कि उसके यूज़र्स उससे सम्पर्क स्थापित न कर सकें।[33])

14. 1989 में एक डिस्केट (Diskette) यह दर्शाते हुए एड्स(AIDS) के कई अनुसंधानकर्ताओं और संयुक्त राष्ट्र की एक प्रसिद्ध पत्रिका के

32 https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/

33 https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

अनेकों पाठकों को भेजी गई, कि इसमें एड्स से संबंधित जानकारियां हैं, जबकि वास्तव में इसमें ट्रोजन हॉर्स (कम्प्यूटरों क्षति पहुंचाने वाला एक प्रोग्राम) समाहित था।[34] (ट्रोजन होर्स या ट्रोजन एक ऐसा प्रोग्राम है जो दिखने में तो सही अनुभव होता है, परन्तु यदि इसे चलाया जाता है तो इस के प्रभाव भयंकर होते है। इसका इस्तेमाल एक हैकर (Hacker) किसी पासवर्ड को तोडने के लिए कर सकता है। यह हार्ड डिस्क के सारे डेटा (Data) और प्रोग्राम को मिटा देता है। दूसरे किसी वायरस की तुलना में ट्रोजन खुद को अनुलिपि नहीं करता है। इसी की मदद से हैकर कंप्यूटर का नियंत्रण सुदूर बैठे दूसरे कंप्यूटर से कर सकता है।)

15. 1994 में रोम एयर डव्लपमेंट सेंटर जो संयुक्त राज्य की वायुसेना का एक अनुसंधान केन्द्र, के प्रशासकों ने एक दिन पाया कि उनके नेटवर्क पर 'स्नीफर' नाम का एक पासवर्ड इन्सटॉल किया गया है, जिसके 100 से भी अधिक प्रयोगकर्ता है। जांच में पता चला कि डाटास्ट्रीम को बॉय और कुजी नामक दो हैकरों ने इस हमले को अंजाम दिया था।[35]

16. 1995 में रूस के एक सॉफ्टवेयर इंजीनियर व्लादिमिर लेविन ने सेंट पीटर्सबर्ग स्थित अपने घर पर बैठे-बैठे सिटी बैंक न्यूयॉर्क के सूचना-प्रौद्योगिकी तंत्र में सेंध लगा कर कई फर्जी लेनदेन कर डाले थे और पूरी दुनिया के लोगों को 10 मिलियन डॉलर्स का नुकसान पहुंचाया था।[36]

17. 1998-2007 : मैक्स बटलर ने संयुक्त राज्य सरकार की वेबसाइट

34 https://www.herjavecgroup.com/history-of-cybercrime/
35 https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/
36 https://www.vpnmentor.com/blog/20-biggest-hacking-attacks-time/

को 1998 में हैक किया था तथा उसे वर्ष 2001 में 18 महीनों की सजा सुनाई गई थी। वर्ष 2003 में जेल से रिहा होकर उसने साइबर हमलों के लिए वाईफाई तकनीक का इस्तेमाल किया और मालवेयर प्रोग्राम का प्रसार करते हुए क्रेडिट कॉर्डों की जानकारी चुराने लगा। वर्ष 2007 में जब उसे पकड़ा गया तो उसने ऐसे फर्जीबाड़े के साथ लाखों क्रेडिट कार्डों की जालसाजी और लगभग 86 मिलियन डालर की फर्जी खरीद-फिरोख्त में अपनी संलिप्तता कबूल की।[37]

18. 1999 में जॉनाथन जेम्स नाम 15 वर्षीय बालक ने संयुक्त राज्य के रक्षा विभाग के कम्प्यूटरों में सेंध लगा कर वहां उनके सर्वरों में एक 'बैकडोर' स्थापित कर दिया, जिसके माध्यम से वह विभिन्न सरकारी संगठनों से आने वाले हजारों आंतरिक इमेल संदेशों को पढ़ सकता था। इनमें वे इमेल भी शामिल थे जिनमें विभिन्न सैन्य कम्प्यूटरों के लिए बाकायदा यूजरनेम एवं पासवर्ड होते थे। इन सूचना का इस्तेमाल कर वह नासा के सॉफ्टवेयर का एक हिस्सा चुराने में कामयाब रहा, इसके बाद इन कम्प्यूटर सिस्टम को 3 सप्ताह के लिए बंद कर दिया गया।[38]

19. 2000 में कैनेडियन हाईस्कूल के 15 वर्षीय छात्र माइकल केलसे उर्फ माफिया-बॉय ने कई प्रतिष्ठित व्यवसायिक वेबसाईटों पर 'डिस्ट्रीब्यूटेड-डिनाइयल-ऑफ-सर्विस-अटैक' किए थे, जिसमें अमेजन, सीएनएन, इ-बे और याहू सहित कई वेबसाइट शामिल थी। एक उद्योग विशेषज्ञ का अनुमान था कि इस हमले में लगभग 1.2 बिलियन डॉलर्स का नुकसान हुआ था।[39]

37 https://blog.tmb.co.uk/cyber-criminals

38 https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

39 https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

उपरोक्त घटनाओं से हमें साइबर अपराधों के उदगम, विकासक्रम और सामान्य प्रवृत्तियों को समझने में मदद मिलती है। संचार एवं कम्प्यूटर प्रौद्योगिकी के शुरुआती दौर में इस प्रकार के अपराधों को ज़्यादातर असंतुष्ट लोगों या धोख़ेबाज़ कर्मचारियों द्वारा ही अंजाम दिया जाता था। 1980 के दशक तक कम्प्यूटरों को भौतिक रुप से नुकसान पहुंचाए जाने का डर बना ही रहता था। उस समय आपराधिक प्रवृत्ति के लोग अपनी आधिकारिक मौजूदगी का फायदा उठा कर अपने आर्थिक लाभ के लिए कम्प्यूटरों में समाहित डाटा में बदलाव कर देते थे या फिर बदला लेने के लिए डाटा को नुकसान पहुंचा देते थे। हमने ये भी देखा कि आपराधिक प्रवृत्ति के लोगों ने टेलीग्राफ एवं टेलीफोन की शुरुआत से ही अपने मनो-विनोद या दूरसंचार सेवाओं की चोरी के उद्देश्य से उनके अनाधिकृत प्रयोग में कोई कसर नहीं छोड़ी। जैसे-जैसे दूरसंचार क्रांति सूचना-प्रौद्योगिकी जगत का अभिन्न हिस्सा बनती चली गई, वैसे-वैसे अपराधियों ने संचार पद्धति, कम्पयूटर सिस्टम और नेटवर्क में सेंध लगाना भी सीख लिया। 1980 के दशक में प्रोग्रामरों ने घातक सॉफ्टवेयर भी विकसित कर लिए, जिनमें ऐसे साफ्टवेयर भी शामिल थे जो अपनी ही प्रतिकृतियां बना कर पर्सनल कम्प्यूटर को क्षति पहुंचा सकते थे। जनवरी 1983 में इंटरनेट के आने के बाद दुनिया भर के कम्प्यूटरों तक इसकी पहुंच होने लगी। इंटरनेट की लोकप्रियता और बढ़ते प्रयोग के साथ-साथ ही अपराधियों ने कमजोर सुरक्षा-प्रबंधों वाले कम्प्यूटर सिस्टमों पर धावा बोलते हुए दहशत फैलाने और अपने आर्थिक तथा राजनैतिक लाभों के लिए इंटरनेट का भी दुरुपयोग शुरु कर दिया। 1990 के दशक में दुनियाभर में कम्प्यूटर एवं सूचना प्रौद्योगिकी की सहायता से किए जाने वाले आर्थिक अपराधों की घटनाएं तेजी से बढ़ने लगीं। इसके साथ ही साइबर जगत से जुड़े अन्य सुरक्षा खतरों में दिन-ब-दिन तेजी से वृद्धि होने लगी। नतीजतन, साइबर अपराधों से केवल सारी दुनिया को हर वर्ष भारी आर्थिक नुकसान उठाना पड़ रहा है, बल्कि विश्व भर के देशों को एक बहुत बड़ी

रकम हर वर्ष साइबर-सुरक्षा प्रबंधों पर खर्च करनी पड़ रही है। एक रिपोर्ट के अनुसार, वर्ष 2020 में पूरे विश्व को साइबर अपराधों से अनुमानत: 9 करोड़ 45 लाख यू.एस. डॉलर्स का नुकसान उठाना पड़ा है और इस बीच पूरी दुनिया के द्वारा साइबर अपराधों की रोकथाम के लिए 1 करोड़ 45 लाख यू.एस. डॉलर्स की धनराशि के खर्च का भी अनुमान है।[40]

ख. भारतीय परिदृश्य

भारत में दूरभाष यानी टेलीफोन सेवाएं सन् 1914 में शिमला से आरंभ हुई थी। भारत में कम्प्यूटर युग की शुरुआत 1952 में हुई थी, जब भारतीय सांख्यिकीय संस्थान, कलकत्ता में पहला एनालॉग कम्प्यूटर स्थापित किया गया था। इसके बाद वहां वर्ष 1955 में पहला डिजिटल कम्प्यूटर, जो एक ब्रिट्रिश एचईसी 2एम कम्प्यूटर था, किया गया। इसके साथ ही भारत, जापान के बाद एशिया का दूसरा ऐसा देश बन गया था, जिसने कम्प्यूटर तकनीक को अपनाया था। इसके बाद भारत ने कम्पयूटर निर्माण के क्षेत्र में अपनी ओर से पहल आरंभ कर दी थी और इस दिशा में पहला स्वदेशी कम्प्यूटर TIFRAC 1960 में तैयार कर लिया था। इसके बाद 1966 में भारतीय सांख्यिकीय संस्थान और जादवपुर यूनिवर्सिटी द्वारा ISIJU नामक ट्रांजिस्टर युक्त कम्प्यूटर बनाया गया। इसी बीच वर्ष 1965 में कम्प्यूटर सोसाइटी ऑफ इंडिया की स्थापना की गई। इसके बाद वर्ष 1970 में इलेक्ट्रॉनिक्स विभाग की स्थापना की गई, जिसका उद्देश्य सार्वजनिक क्षेत्र कम्प्यूटरों के प्रयोग का बढ़ावा देना था। 1978 में आईबीएम के साथ दूसरी निजी क्षेत्र की कम्पनियों ने भी कम्प्यूरों का निर्माण आरंभ किया। वर्ष 1984 सेंटर फॉर द डेवलेपमेंट ऑफ टेलेमैटिक्स(सी-डॉट) की स्थापना की गई। आगे चल कर, वर्ष 1988 में सेंटर फॉर डेवलेपमेंट ऑफ एडवांस कम्प्यूटिंग(सी-डेक) की भी

40 https://www.thehindu.com/sci-tech/technology/cybercrime-could-cost-the-world-almost-1-trillion/article33269047.ece

स्थापना की गई। सी-डेक के वैज्ञानिकों ने वर्ष 1990 में सुपर कम्प्यूटर का प्रोटोटाईप मॉडल तैयार कर लिया था, जिसे इसी वर्ष ज्यूरिख़ में आयोजित सुपर कम्प्यूटिंग शो में बहुत ख्याति मिली। इसके साथ ही भारत दुनिया के देशों को पीछे छोड़ते हुए अमेरिका के बाद दूसरे पायदान पर आ खड़ा हुआ था। 1 जुलाई 1991 को भारत ने पूर्णत: निजी प्रयासों से परम-8000 सुपर कम्प्यूटर बना कर इतिहास रच दिया था।

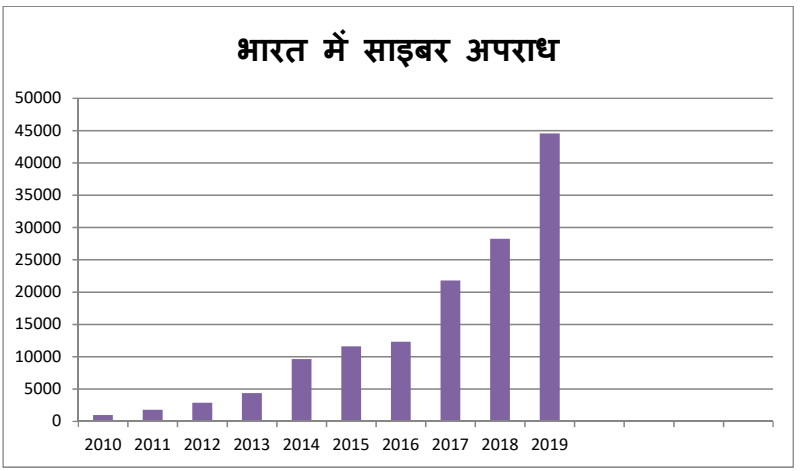
स्पष्ट है कि भारत अपनी सरजमीं पर वर्ष 1952 से आरंभ हुए कम्प्यूटर युग के बाद निरंतर तरक्की करता आया है और कम्प्यूटरीकरण के क्षेत्र उसने विश्वस्तरीय कीर्तिमान स्थापित किए हैं। भारत में इंटरनेट सेवाएं 15 अगस्त 1995 को विदेश संचार निगम लिमिटेड द्वारा आरंभ की गई थीं।। वर्ष 1998 में सरकार ने निजी क्षेत्र सेवा-प्रदाताओं को भी इंटरनेट सेवाओं के लिए प्राधिकृत कर दिया था। भारत में कम्प्यूटरों एवं इंटरनेट के सार्वजनिक उपयोग में आने के बाद से ही साइबर अपराधों का सिलसिला, धीरे-धीरे ही सही लेकिन, आरंभ हो गया। भारत में सबसे पहले पंजीकृत हुए साइबर अपराध के प्रकरणों में से एक मामला याहू बनाम आकाश अरोरा का था।[41] यह प्रकरण 1999 में घटित हुआ था। इस मामले में प्रतिवादी आकाश अरोरा पर याहू का ट्रेडमार्क या डोमेन नेम 'yahooindia.com' के प्रयोग का आरोप था। दूसरा प्रकरण विनोद कौशिक और अन्य बनाम माधविका जोशी और अन्य का प्रकरण था, जिसमें न्यायालय ने यह निर्णय दिया था कि पति और ससुर के ई-मेल एकाउंट को उनकी अनुमति के बिना देखना सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा—43 का उल्लंघन है।[42]

उल्लेखनीय है कि इसी दौरान भारत सरकार ने साइबर अपराधों से निपटने के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 लागू कर दिया था और इसके

41 http://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html.

42 Ibid.

बाद सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 भी जारी किया गया। विगत वर्षों में भारत में पंजीकृत साइबर अपराधों की ओर यदि दृष्टि डाले तो यह स्पष्ट हो जाता है कि यहां साइबर अपराध दिन-ब-दिन बढ़ते ही जा रहे हैं। राष्ट्रीय अपराध ब्यूरो द्वारा प्रस्तुत आंकड़े वाकई चिंताजनक हैं। ब्यूरो के अनुसार देश में वर्ष 2010 में 966, 2011 में 1791, 2012 में 2876 और 2013 में 4356 साइबर अपराध पंजीकृत किए गए।[43] इसके बाद वर्ष 2014 में 9622, वर्ष 2015 में 11592, वर्ष 2016 में 12317, वर्ष 2017 में 21796, वर्ष 2018 में 28248 और वर्ष 2019 में 44546 साईबर अपराध पंजीकृत किए गए। भारत में साइबर अपराधों की तेजी से बढ़ती संख्या को यह ग्राफ और स्पष्ट रूप से दर्शाता है-



इन आंकड़ों के अवलोकन से यह स्पष्ट होता है कि भले ही भारत में साइबर अपराधों की शुरूआत दुनिया के देशों से बहुत बाद में हुई हो, लेकिन यहां साइबर अपराधों का आंकड़ा बहुत तेजी से बढ़ रहा है। मसलन- वर्ष 2010 के मात्र 966 मामले 10 वर्ष में 44000 को पार करने करने लगे हैं।

43 https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/18-Cyber%20Crimes_2013.pdf

समग्र रूप से देखें तो आज सूचना व संचार प्रौद्योगिकी से जुड़े कम्प्यूटर, लेपटॉप व मोबाईल फोन तथा स्मार्ट फोन जैसे अनेक अत्याधुनिक संसाधन पूरी दुनिया में जगह-जगह और जन-जन के पास मौजूद हैं। स्थिति यह है कि जिसके पास कुछ नहीं है उसके पास भी कम से कम एक मोबाईल फोन तो है ही, क्योंकि अब मोबाइल फोन के बिना जीना मानव के लिए यकीनन असंभव सा है। नगण्य कहे जाने वाले आंकड़ों को छोड़ कर, इस दुनिया का हर आदमी अब संचार क्रांति का हिस्सा बन चुका है। सच में संचार क्रांति ने सारी दुनिया आदमी की मुट्ठी में समेट कर रख दी है। इसका दूसरा पहलू ये भी है कि आज हम सब हर समय संचार माध्यमों और सूचना-प्रौद्योगिकी से जुड़े रहते हैं। हमारे जीवन की अधिकांश जरूरतें अब ऑनलाईन लेनदेन से पूरी होती हैं। विश्व भर में अब नागरिकों के डिजीटल विवरण रखने का भी दौर चल पड़ा है। भारत जैसे विकासशील देशों में भी नागरिकों की अद्वितीय व्यक्तिगत पहचान का नया पर्याय बन चुके आधार कार्ड से लेकर अनेकानेक विवरण और सुविधाएं डिजिटल एवं ऑनलाईन हो चुकी हैं।

सूचना-प्रौद्योगिकी के इस युग में पुलिस बलों के सामने सबसे बड़ी चुनौती ये है कि आखिर डिजिटल दुनिया की अंधी दौड़ में बदलती आपराधिक प्रवृत्तियों का पूर्वानुमान लगा कर अपराधों की नित्य नई किस्मों को किस प्रकार रोका जाए? ऐसा इसलिए भी है, क्योंकि हम साइबर-अपराधों की अवधारणा को तो समझ सकते हैं और उनकी अब तक की प्रवृत्तियों से कुछ हद तक उनकी गंभीरता व संभावनाओं का अनुमान लगा कर रोकथाम के प्रयास भी कर सकते हैं, किन्तु सूचना-प्रौद्योगिकी के ज्ञान का गैर-कानूनी मकसद से इस्तेमाल करने वाले अपराधियों का दिमाग नहीं पढ़ सकते। कुल मिला कर दुनिया भर में साईबर अपराध दिन-ब-दिन बढ़ते ही जा रहे हैं और इनकी रोकथाम के लिए जन-जन का साईबर अपराधों के विषय में जागरूक होना सबसे पहली और सबसे प्रमुख आवश्यकता है। इसीलिए पुस्तक के सबसे पहले पृष्ठ पर एक नए शब्द "साइबर-समझ" का उल्लेख किया गया

है, क्योंकि जब तक जनता में 'साइबर-समझ' विकसित नहीं होगी, साइबर अपराध होते रहेंगे और इन पर दण्डात्मक कार्रवाई के लिए अनिश्चित समय तक चलने वाली प्रक्रियाओं से जांच एजेंसियां काम के बोझ तले दबती रहेगीं। वहीं दूसरी ओर पीडितों को सही समय पर न्याय नहीं मिल सकेगा।[44]

44 https://www.bhaskar.com/local/mp/news/9-investigation-officers-in-mp-cyber-cell-only-3-in-bhopal-pending-1900-complaints-to-each-one-how-will-the-cases-be-resolved-in-15-days-under-such-circumstances-128304586.html

अध्याय 2

साइबर अपराधों के प्रकार और सूचना-प्रौद्योगिकी के साथ बदलती प्रकृति

साइबर अपराध वस्तुत: वो अपराध हैं, जिन्हें सूचना व संचार प्रौद्योगिकी से जुड़े संसाधनों के साथ विश्व-व्यापी इलेक्ट्रानिक नेटवर्क में अंजाम दिया जाता है। साइबर अपराध अंतरराष्ट्रीय और देशव्यापी स्तर पर बहुत ही सुनियोजित तरीके से अंजाम दिए जाते हैं और इसका शिकार कोई भी, कहीं भी बन सकता है। साइबर अपराधों के घटित होने की संभावनाएं उतनी ही व्यापक है, जितना आज के प्रदूषित पर्यावरण और वातावरण में एक इंसान या जीव का किसी जानलेवा रोक से ग्रसित होना। इसमें फर्क सिर्फ इतना है कि रोगग्रस्त होने पर हम शारीरिक जोखिम उठाते हैं, जबकि साइबर अपराधों से होने वाले नुकसान की हम कल्पना भी नहीं कर सकते, क्योंकि इसमें नुकसान की सीमा अपराधियों के आघात पर निर्भर करती है और जब तक इस ख़तरे की आहट हम तक पहुंचती है तब तक बहुत बड़ा नुकसान हो चुका होता है। जिस प्रकार आधुनिक युग में रोग के कीटाणू अपनी प्रवृत्ति को बदल कर मानव-जाति को अनेकानेक प्रकार के नुकसान पहुंचा रहे हैं, उसी प्रकार मानवजाति के भीतर पनपने वाली आपराधिक मानसिकताएं आधुनिक सूचना व संचार क्रांति का सहारा लेकर अपने फायदे और नाजायज तरक्की के लिए आक्रमक रूप धारण कर चुकी हैं और नित्य नए साइबर अपराधों को अंजाम देने पर आमदा है।

इस पुस्तक के प्रथम अध्याय में समाहित तथ्यों से यह स्पष्ट होता है कि साइबर अपराधों का सीधा संबंध संचार एवं सूचना प्रौद्योगिकी से है। मानव ने जब से संचार माध्यमों को जरिया बना कर गैरकानूनी कृत्यों को अंजाम

देना शुरु किया, दरअसल तभी से साइबर अपराधों की शुरुआत भी मानी जानी चाहिए। हमने देखा कि वर्ष 1834 में कतिपय चोरों ने फ्रैंच टेलीग्राफ सिस्टम को भेद कर वित्तीय बाजार की कुछ अहम जानकारियां चुरा ली थीं और यही घटना विश्व का पहला साइबर हमला कही जाती है। जैसे-जैसे संचार सुविधाएं बढ़ती गईं, और कम्प्यूटरों एवं इंटरनेट के आगमन के साथ सूचना-प्रौद्योगिकी का नया दौर शुरु हुआ तथा दुनिया में संचार व सूचना प्रौद्योगिकी की क्रांति आगे बढ़ती चली गई, वैसे-वैसे दुनिया भर में साइबर अपराधों का स्वरूप भी बदलता चला गया। क्रमिक रूप से देखा जाए तो सबसे पहले टेलीग्राफ नेटवर्क में सेंध लगाना, फिर टेलीफोन कॉल्स के बीच आपराधिक उद्देश्यों से हस्तक्षेप करना, वायरलैस टेलीग्राफी के संदेशों को अंतरग्रहित करना, सैन्य प्रयोग में आने वाले कूट-संकेतों को बीच में ही ग्रहण करके उनका अनधिकृत इस्तेमाल करना, कम्प्यूटरों तथा टेलीफोन नेटवर्क में सेंध लगा कर सूचनाएं चुराना या कोई नया कोड व प्रोग्राम भेज कर अपने शिकार को किसी प्रकार की क्षति पहुंचाना और वायरस का प्रयोग कर संचार व सचूना प्रौद्योगिकी तंत्र को सोची-समझी साजिश के तहत भारी क्षति पहुंचाना तथा आज के दौर में इन सब सुविधाजनक माध्यमों का बड़ी ही शातिर तरकीबों से इस्तेमाल कर सामाजिक, राजनीतिक एवं आर्थिक पृष्ठभूमि पर अपराधों को अंजाम देना, साइबर अपराधों के दीर्घकालीन विकासक्रम को दर्शाता है। मोटे तौर पर हम साइबर अपराधों को तीन प्रमुख भागों में विभाजित कर सकते हैं-

1) व्यक्ति के विरुद्ध किए जाने वाले साइबर अपराध
(जैसे-साइबर बुलिंग/स्टॉकिंग,अश्लीलता फैलाना, बाल यौन शोषण सामग्री का प्रसार)

2) संपत्ति के विरुद्ध किए जाने वाले साइबर अपराध
(जैसे-हैकिंग, फिशिंग, डोस अटैक, वायरस/रेनसमवेयर अटैक, डाटा-चोरी आदि)

3) सरकार के विरुद्ध किए जाने वाले साइबर अपराध
(जैसे- साइबर जासूसी और साइबर आतंकवाद)

दरअसल साइबर अपराध सूचना और संचार प्रौद्योगिकी से ऐसे जुड़े हाइटैक अपराध हैं, जिनकी कोई सीमा नहीं है। सच कहें तो साइबर अपराधों की कोई सर्वमान्य परिभाषा भी नहीं है। आज सूचना और संचार प्रौद्योगिकी के अपने सबसे विकसित स्तर पर आने तक साईबर अपराधों ने जो स्वरूप धारण कर लिए हैं, उन्हें हम निम्नवत रूप से समझ सकते हैं-

1. अनधिकृत पहुंच या हैकिंग-

किसी भी कम्प्यूटर, कम्प्यूटरीकृत डिवाइज या कम्प्यूटर नेटवर्क में अनधिकृत पहुंच या घुसपैठ कर डाटा से छेड़खानी करना हैकिंग है। हैकिंग उस कम्प्यूटर सिस्टम या नेटवर्क के सीधे सम्पर्क में आकर या दूर बैठ कर दोनों की तरीकों से की जा सकती है। ज्यादातर हैकिंग का मकसद वित्तीय अपराधों को अंजाम देना या किसी वेबसाइट के डाटा में परिवर्तन करना होता है, जैसे-

1) किसी बैंक के खाताधारकों के खातों से दूसरे खाते में पैसे हस्तांतरित करना।

2) किसी व्यक्ति के डेबिट/क्रेडिट कार्ड की जानकारी चुरा कर उसका दुरूपयोग करना।

3) किसी वेबसाइट के डाटा को अनधिकृत तरीके से बदल देना या नुकसान पहुंचाना।

सही मायनों में हैकिंग साइबर अपराध की दुनिया का वो सबसे प्रचलित शब्द है, जिसने साइबर अपराधों की अवधारणा विकसित करने में सबसे अहम भूमिका निभाई है। आज साइबर जगत के जितने भी अपराध हैं उन सबका जनक हैकिंग ही है। शेष सभी साइबर अपराध किसी न किसी रूप में हैकिंग से ही प्रेरित और प्रभावित दिखाई देते हैं। सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008) की धारा-43(ए) एवं धारा-66 तथा भा.द.सं. की धारा-379 एवं धारा-406 के अंतर्गत हैकिंग एक दण्डनीय अपराध है।

उदाहरणार्थ-

वर्ष 2018 में पूणे स्थित कॉसमॉस बैंक पर एक साइबर हमला किया गया। इस दुस्साहसी साइबर हमले ने पूरे बैंकिंग क्षेत्र को उस समय झकझोर कर रख दिया था, जब ये पता चला कि हैकर्स ने कॉसमॉस बैंक से 94.42 करोड़ रुपयों पर हाथ साफ कर दिया है। दरअसल हैकर्स ने बैंक के एटीएम सर्वर को हैक कर लिया था और अनेकों वीज़ा एवं रुप्पी कार्डधारकों के विवरण हथिया लिए थे। जैसे ही इस हैकिंग का इशारा मिला 28 देशों में बैठी हैकर्स की गैंग ने बिना किसी देरी के पैसा निकाल लिया। यह पैसा कनाडा, हाँगकाँग और भारत सहित 28 देशों के विभिन्न एटीएम काउन्टरों से निकाला गया। इसमें से 14 करोड़ रुपए स्वीफ्ट सिस्टम के माध्यम से

हाँगकॉग स्थित एक बैंक को हस्तांतरित किए। बाकी के 80 करोड़ रुपए जिस समय विभिन्न एटीएम काउन्टरों से निकाले गये, उस समय मालवेयर का हमला जारी था, जिससे वीज़ा और रुप्पी डेबिट कार्डों का पेमेंट गेटवे ऑपरेट हो रहा था।[1]

हैकर्स, एथिकल हैकर्स और क्रैकर्स

- हैकर्स - हैकर्स किसी भी कम्प्यूटर सिस्टम की बारीक से बारीक जानकारी रखने का काम करते हैं। हैकर्स ज्यादातर प्रोग्रामर्स होते हैं। हैकर्स ऑपरेटिंग सिस्टम्स और प्रोग्रामिंग लैंग्वेज की नवीनतम जानकारी रखते हैं। वे अपने इस ज्ञान को बढ़ाने की कोशिश हर समय करते रहते हैं।
- एथिकल हैकर्स –इथिकल हैकर्स कम्प्यूटर प्रयोगकर्ताओं के लिए मददगार होते हैं, जो उन्हें नुकसान से बचाते हैं और गड़बड़ियों की जानकारियाँ देते हैं।
- क्रैकर्स – क्रैकर्स वे लोग होते हैं जो बिना अनुमति के दूसरे के कम्प्यूटर के जरिए उसके सर्वर तक पहुँचकर उसमें संग्रहीत सूचनाओं में फेरबदल कर देते हैं। कैकर्स किसी भी साइट में जाकर कुछ न कुछ गड़बड़ करने के लिए ही जाने जाते हैं।

2. डाटा चोरी-

किसी संस्था या व्यक्ति के कम्प्यूटर नेटवर्क से अनधिकृत व्यक्ति द्वारा बिना अनुमति डाटा की कॉपी करना या उसे साझा करना डाटा चोरी की श्रेणी में आता है। सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008) की धारा-43(बी) , धारा-66(ई) एवं धारा-67(सी) तथा भा.द.सं. की धारा-379,

1 https://www.kratikal.com/blog/5-biggest-cyber-attacks-in-india

धारा-405 एवं धारा-420 और कॉपीराईट एक्ट के प्रावधानों के अंतर्गत यह एक दण्डनीय अपराध है।

उदाहरण –

सीबीआई ने वर्ष 2018 में फेसबुक यूजर्स का डाटा चोरी होने के मामले में एक प्रारंभिक जांच की थी। इस जांच से पता चला कि ग्लोबल साइंस प्राइवेट लिमिटेड ने "thisisyourdigitallife" नाम से एक एप्लिकेशन बनाया था। फेसबुक की प्लेटफॉर्म पॉलिसी के अनुसार इस एप्लिकेशन को शैक्षणिक और अनुसंधान उद्देश्यों के लिए यूजर्स का कुछ विशिष्ट डाटा एकत्र करने की अनुमति दी गई थी। लेकिन इस एप्लिकेशन ने फेसबुक यूजर्स और उनके दोस्तों के नेटवर्क के डाटा को भी अवैध तरीके से एकत्र कर लिया। फेसबुक ने सीबीआई को बताया कि इस एप्लिकेशन का उपयोग भारत में 335 यूजर्स ने किया था, लेकिन इस एप्लिकेशन के माध्यम से इन यूजर्स के दोस्तों को भी निशाना बनाया गया और 5.62 लाख लोगों का डाटा बिना उनकी जानकारी के अवैध रूप से चुरा लिया गया।। सीबीआई के मुताबिक़ ग्लोबल साइंस रिसर्च लिमिटेड ने 2014 में कैम्ब्रिज एनालिटिका के साथ मिलकर आपराधिक साजिश की थी और व्यापारिक दृष्टिकोण से अवैध रूप से चोरी किए हुए डाटा के उपयोग का अधिकार कैंब्रिज एनालिटिका को दे दिया था। ब्रिटेन की इन दोनों कंपनियों के खिलाफ आपराधिक साजिश और सूचना-प्रौद्योगिकी कानून के उल्लंघन का मामला दर्ज किया गया था।[2]

3. कम्प्यूटर वायरस का प्रसार-

कम्प्यूटर वायरस एक प्रकार का कम्प्यूटर प्रोग्राम ही है, जो अपनी प्रतिकृति या अनुलिपि तब तक बनाता रहता है, जब तक कोई कम्प्यूटर

2 https://www.aajtak.in/crime/cyber-crime/story/indian-facebook-users-data-stolen-cbi-filed-case-against-cambridge-analytica-1196204-2021-01-22

या कम्प्यूटरीकृत डिवाइज ओवरलोड होकर ठप्प न हो जाए। वायरस के प्रसार का मकसद आम तौर पर कम्प्यूटर या नेटवर्क प्रणाली को संक्रमित कर उसके डाटा को नुकसान पहुंचा कर उसे बाधित करना होता है। विभिन्न प्रकार के मालवेयर (Malware) और एडवेयर (Adware) में भी इस शब्द का प्रयोग सामान्य अर्थों में किया जाता है। वायरस एक कम्प्यूटर से दूसरे कम्प्यूटर में तभी फैलता है जब इसका होस्ट किसी असंक्रमित कम्प्यूटर में लाया जाता है। उदाहरण के लिए एक प्रयोगकर्ता के द्वारा इसे किसी नेटवर्क या इंटरनेट पर भेज कर या किसी हटाये जाने योग्य माध्यम, जैसे सीडी(CD) या यूएसबी ड्राइव (USB Drive) के द्वारा दूसरे कम्प्यूटरों तक फैलाया जा सकता है। प्राय: लोग कम्प्यूटरों में पाए जाने वाले वायरस ओर स्पाईवेयर आदि की ओर ज्यादा ध्यान नहीं देते, लेकिन नेटवर्क अथवा सिस्टम की अन्य कड़ियों के जरिये ये वायरस दूसरे कम्प्यूटरों या डिवाइस तक पहुंच जाते हैं। कम्प्यूटर वायरस या स्पाईवेयर ज्यादातर मामलों में डाउनलोडिंग, हैकिंग, कम्पयूटर नेटवर्क, वाईफाई कनेक्शन और यूएसबी ड्राईव या सीडी इत्यादि के माध्यम से फैलते हैं। दरअसल, वायरस का प्रसार सूचना-प्रौद्योगिकी जगत में एक संगठित व्यापार के रूप में बदस्तूर जारी है। वायरस का प्रसार इतना व्यापक होता है कि कोई व्यक्ति अनजाने में ही इस अपराध का दोषी बन सकता है। सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008) की धारा-43(सी) एवं धारा-66 तथा भा.द.सं. की धारा-268 के प्रावधानों के अंतर्गत वायरस प्रसार एक दण्डनीय अपराध है।

उदाहरण-

वर्ष 2016 में महाराष्ट्र सरकार के 150 कम्प्यूटर एक वायरस हमले के जरिये लॉक कर दिए गए थे। इस वायरस का नाम लॉकी रेनसमवेयर रखा गया था, जिसकी वजह से 10 दिनों में 150 कम्प्यूटरों की फाइलें एन्क्रिप्ट हो गई थी, हालांकि सूत्रों के अनुसार इन फाइलों के बैकअप मौजूद थे। साइबर अपराध

जगत में इस प्रकार के हमले एक खतरनाक कम्प्यूटर वायरस के जरिये अंजाम दिए जाते हैं तथा प्रयोगकर्ता की फाइलों की रिकवरी के लिए 'बिटकॉइन' के रूप में फिरौती मांगी जाती है। साइबर विशेषज्ञों के अनुसार अधिकांश कम्प्यूटर वायरसों की तरह रेनसमवेयर भी प्राय: फर्जी ईमेल, स्पेम या फर्जी कम्प्यूटर साफ्टवेयर अपडेट के माध्यम से आते हैं। जब प्राप्तकर्ता इसके लिंक या अटैचमेंट पर क्लिक करता है तो वायरस उसके कम्प्यूटर की फाइलों को एनक्रिप्ट कर देता है। गौरतलब है कि बिटकॉइन एक तरह की क्रिप्टोकरेंसी है, जिसका कोई भौतिक स्वरूप नहीं होता। इसके जरिये विश्व में कहीं भी ऑनलाइन लेनदेन किया जा सकता है। मतलब आप कुछ भी बेच व खरीद सकते हैं और बैंकों से व्यवहार भी कर सकते हैं। हैकर इस तरह के कामों के लिए बिटकॉइन का इस्तेमाल अपनी पहचान छिपाने के लिए करते हैं।[3]

भारत में बिटकॉइन के लेनदेन को कानूनी मान्यता प्राप्त नहीं है, लेकिन भारत में भी बिटकॉइन या इसके जैसी दूसरी क्रिप्टोकरेंसी में निवेश करने वालों की कमी नहीं है। हालांकि भारत में डिजिटल करेंसी बिल 2021 के आने के साथ ही बिटकॉइन एवं क्रिप्टोकरेंसी के प्रयोग संबंधी स्थिति स्पष्ट होने की संभावना है।[4]

4. डोस(DoS-Denial of Service) अटैक-

डोस अटैक को 'डेनाइअल ऑफ सर्विस अटैक' कहते हैं। इस हमले के द्वारा हैकर्स किसी नेटवर्क या मशीन को उसके प्रयोगकर्ता के लिए ही अनुपलब्ध कर देते हैं। इस हमले का मुख्य उद्देश्य प्रयोगकर्ता को किसी सेवा के उपयोग से वंचित रखना होता है, जैसे-इंटरनेट का प्रयोग आदि। इस प्रकार के हमले का हैकर्स बहुत बड़े पैमाने पर इस्तेमाल करते हैं और उन सभी सेवाओं को

3 https://ndtv.in/mumbai-news/locky-ransomware-locked-maharashtra-ministrys-computers-1412886

4 https://hindi.moneycontrol.com/news/market-news/crypto-currency-will-be-banned-in-india-what-to-do-if-you-have-invested-in-bitcoin_255751.html

प्रयोगकर्ताओं के लिए बाधित कर देते हैं जो कि इंटरनेट से जुड़ी हुई होती हैं। डोस हमले में नेटवर्क या मशीन को ओवरलोड कर दिया जाता है जिस कारण लोग उस पर काम नहीं कर पाते। ऐसा हमला करके नेटवर्क या मशीन को बेकाम करने के लिए सिर्फ एक कंप्यूटर और एक इंटरनेट कनेक्शन की आवश्यकता होती है। दरअसल, ज्यादातर वेबसाइट इस तरीके से बनाई जाती हैं कि वे किसी भी समय एक निश्चित मात्रा में सूचनाओं के आदान-प्रदान को संभाल सकें। डोस हमला उस वेबसाइट को एक के बाद एक अनुरोधों की बौछार से ऐसे भर देता है कि वेबसाइट ओवरलोड हो जाती है और उसका सर्वर दुष्प्रभावित हो जाता है। इससे उस वेबसाइट के असल प्रयोगकर्ता उसके उपयोग से वंचित रह जाते हैं। इसी तरह का हमला जब बड़े पैमाने पर, वेबसाइट को ओवरलोड करने के लिए मैलवेयर से संक्रमित कई कम्प्यूटरों का इस्तेमाल करते हुए किया जाता है, जिन्हें बोटनेट (Botnet) कहा जाता है, तो उसे 'डिस्ट्रीब्यूटेड डोस अटैक' कहते हैं। सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008) की धारा-43(ई) ,(एफ) एवं (जी) में इस तरह के अपराधों के लिए दण्ड का प्रावधान है।

उदाहरण-

वर्ष 2016 में मुम्बई के इंटरनेट सेवा प्रदाताओं पर डोस हमला किया गया था, जिसे भारत का अब तक का सबसे बड़ा डोस हमला कहा जाता है। इस हमले की तीव्रता 200 गीगाबाईट/प्रति सेकेण्ड आंकी गई थी। इस हमले के कारण मुम्बई के प्रयोगकर्ताओं को इंटरनेट की बहुत ही धीमी गति का सामना करना पड़ा था। उस समय ये भी कहा जा रहा था कि इस डिस्ट्रीब्यूटेड डोस अटैक को मुम्बई के इंटरनेट सेवा प्रदाताओं द्वारा खुद ही अंजाम दिया गया था, जिसका मकसद समझ नहीं आ रहा था। हालांकि अनुमान ये लगाया जा रहा था कि इस प्रकार का हमला ब्लैकमेलिंग या अपने व्यवसायिक प्रतिद्वंद्वी को मजा चखाने या कुछ उपद्रवियों द्वारा मजाक के मकसद किया गया था। इस हमले का काफी बुरा असर पड़ा और खास

तौर पर इसमें ग्राहकों की विश्वसनीयता खोने का बहुत बड़ा डर था। अपनी तरह का यह पहला मामला था, जिसके लिए मुम्बई पुलिस ने अपराध की एफआईआर दर्ज की थी।[5]

5. फिशिंग (Phishing)-

फिशिंग एक प्रकार की इलेक्ट्रॉनिक जालसाजी है। जिस प्रकार मछली पकड़ने के लिये कांटे में चारा लगाकर डाला जाता है और चारा खाने के लालच या धोखे में आकर मछली कांटें में फंस जाती है। ठीक उसी प्रकार हैकर्स द्वारा इंटरनेट प्रयोगकर्ताओं को ईमेल या इंस्टेन्ट मैसेज के माध्यम से प्रलोभन देकर की गई धोखाधड़ी को फिशिंग कहते हैं। साइबर अपराधी फिशिंग को अंजाम देने के लिए नकली ईमेल या संदेश भेजते हैं, जो किसी प्रतिष्ठित कम्पनी, बैंक, क्रेडिट कार्ड कम्पनी, ऑनलाइन शॉपिंग के नाम से भेजा जाता है और हू-ब-हू उस संस्था की तर्ज पर ही तैयार किया जाता हैं, ताकि प्रयोगकर्ता आसानी से धोखा खा जाए। अब यदि प्रयोगकर्ता सतर्क न हो तो वह ऐसे ईमेल या संदेश के झांसे में आ जाता है। ऐसे फर्जी ईमेल या संदेश का मकसद प्रयोगकर्ता की बेहद निजी जानकारियां चुराना होता है, जैसे- प्रयोगकर्ता का पूरा नाम, यूजर आईडी एवं पासवर्ड, मोबाइल नम्बर या टेलीफोन नम्बर, निवास का पता, बैंक खाता नम्बर, एटीएम/डेबिट/क्रेडिट कार्ड का नम्बर एवं उसका पिन, सीवीवी नम्बर या वेलिडेशन कोड और प्रयोगकर्ता की जन्मतिथि आदि। इस तरह के ईमेल से की जाने वाली फिशिंग 'ईमेल फिशिंग' कहलाती है, लेकिन फिशिंग के कई और भी रूप हैं-

1. **स्पीर फिशिंग (Spear Fishing)** – इसमें कोई हमलावर ईमेल या संदेश भेज कर सीधे किसी विशेष संस्था या व्यक्ति को अपना शिकार बनाता है। सामूहिक फिशिंग से बिल्कुल विपरीत, इस प्रकार की

5 https://www.firstpost.com/tech/news-analysis/internet-service-providers-in-mumbai-targeted-in-ddos-attack-3685981.html

फिशिंग में हमलावर अपने शिकार के बारे में व्यक्तिगत जानकारियां जुटा लेते हैं, ताकि वे अपनी कामयाबी की संभावनाओं को बढ़ा सकें। सामान्यत: इस प्रकार की फिशिंग में व्यक्तिगत जानकारियों का प्रयोग करते हुए एक ऐसी विश्वसनीय छवि बना कर किसी संस्था या व्यक्ति को ईमेल/संदेश भेजा जाता है, जिस पर वह आसानी से भरोसा करके साइबर अपराधियों को मनचाही जानकारियां दे देता है।

2. **एसएमएस फिशिंग (SMS Fishing) –** इस प्रकार की फिशिंग को स्मिशिंग भी कहा जाता है। इसमें फिशिंग को अंजाम देने के लिए एसएमएस का इस्तेमाल किया जाता है।

3. **फार्मिंग (Pharming) –** फार्मिंग एक ऐसा अपराध है जिसमें हैकर्स इंटरनेट प्रयोगकर्ता को असली के स्थान पर किसी फर्जी वेबसाइट पर भेज देते हैं। यह नकली वेबसाइट इंटरनेट प्रयोगकर्ता की गोपनीय जानकारियां, जैसे-यूज़रनेम, पासवर्ड और डेबिट/क्रेडिट कार्ड का डाटा आत्मसात कर लेती है अथवा प्रयोगकर्ता के कम्प्यूटर पर कोई मालवेयर स्थापित कर देती है। फार्मिंग करने वाले अपराधी ज्यादातर वित्तीय क्षेत्र से जुड़ी वेबसाइट, जिनमें बैंक की वेबसाइटें, ऑनलाइन पेमेंट प्लेटफॉर्म या ई-कॉमर्स डेस्टीनेशन शामिल होते हैं, बना कर इंटरनेट पर लॉच कर देते हैं, जिनका खास मकसद प्रयोगकर्ताओं की जानकारी चुराना होता है, ताकि उसका गलत फायदों के लिए इस्तेमाल किया जा सके। फार्मिंग हमले इस लिए ज्यादा कारगर होते हैं, क्योंकि ये प्रयोगकर्ता के साथ उसके कम्प्यूटर को भी नुकसान पहुंचाते हैं। इसका तकनीकी पक्ष ये है कि जब कभी किसी प्रयोगकर्ता को किसी वेबसाइट पर जाना होता है तो वह उसका यूआरएल दर्ज करता है। बस इसी यूआरएल को एक डीएनएस सर्वर द्वारा एक विशेष आई.पी. नम्बर से जोड़ दिया जाता है। डीएनएस

सर्वर का अर्थ है, डोमेन नेम सिस्टम (Domain Name System) सर्वर, जिसे इंटरनेट की फोन-बुक भी कहा जा सकता है। इसे इस प्रकार समझा जा सकता है कि डीएनएस सर्वर एक फोन-बुक है और यूआरएल एक (वेबसाइट का) नाम तथा आई.पी. एड्रेस इसका फोन नम्बर है। अपराधी बड़ी आसानी से इस फोन-बुक रुपी डीएनएस सर्वर में नाम के आगे लिखें फोन नम्बर यानी आई.पी. नम्बर को अपनी चुनिंदा नकली वेबसाइट के आई.पी. नम्बर से बदल देते हैं। आज के दौर में फार्मिंग एक प्रचलित साइबर अपराध बन चुका है।

4. **व्हेलिंग अटैक (Whaling Attack) –** जहां एक ओर साधारण फिशिंग में किसी भी व्यक्ति या व्यक्ति के समूहों को निशाना बनाया जाता है और स्पीर फिशिंग में किसी व्यक्ति विशेष को अपना शिकार बनाया जाता है, वहीं व्हेलिंग अटैक इन दोनों से चार कदम आगे का अपराध है। इसमें किसी कम्पनी या संस्था के प्रमुख पदाधिकारियों को निशाना बनाया जाता है और वो भी इस प्रकार से कि इस हमले के शिकार ये समझ बैठते हैं कि उन्हें मिला तथाकथित ईमेल संदेश उनके ही संगठन के किसी बहुत वरिष्ठ अधिकारी ने भेजा है। अपराधियों की ऐसी साजिश उनके लिए सोशल-इंजीनियरिंग का बहुत कारगर हथियार बन जाती है, क्योंकि संगठन के सदस्य अपने से बहुत वरिष्ठ और महत्वपूर्ण पदाधिकारी के अनुरोध को प्रथम-दृष्टया नजरअंदाज नहीं कर पाते और जल्दबाजी में वो काम कर जाते है, जो अपराधियों को उनके मकसद तक पहुंचा देता है।

क्या है सोशल-इंजीनियरिंग ?

वस्तुत: सोशल-इंजीनियरिंग अपने आप में कोई अपराध नहीं है, जब तक कि उसे किसी आपराधिक मकसद से अंजाम न दिया जाए। सामान्य अर्थों में सोशल इंजीनियरिंग का तात्पर्य ऐसी तरकीबों, संवाद या सम्प्रेषण से है, जिसके जरिये कोई व्यक्ति किसी दूसरे व्यक्ति का भरोसा जीत कर उससे अपने मन-माफ़िक काम करवाने में कामयाब रहता है। जैसा कि इस वाक्य से स्पष्ट है- 'मैंने बातों-बातों में उसकी नाराज़गी का राज़ उगलवा लिया।' इस प्रकरण में मेरे द्वारा अमूक व्यक्ति से उसकी नाराज़गी का राज़ उगलवाने की कोशिश सकारात्मक उद्देश्य से की गई और इस उद्देश्य से मेरे द्वारा अपनाई गई तरकीबें और वाकपटुता सोशल इंजीनियरिंग का उदाहरण है। लेकिन यही सोशल इंजीनियरिंग तब आपराधिक हो जाती है, जब कोई व्यक्ति छल या कपट से वार्तालाप, संवाद, ईमेल, मैसेजिंग आदि के जरिये किसी दूसरे व्यक्ति का विश्वास जीत कर उसकी गोपनीय या व्यक्तिगत जानकारी हासिल कर लेता है, ताकि इनका इस्तेमाल वह अपने नापाक मनसूबों को पूरा करने में कर सके। इस प्रकार से साइबर अपराधों की दुनिया में सोशल इंजीनियरिंग की बहुत बड़ी भूमिका रहती है।

5. **वॉइस फिशिंग (Voice Phishing or Vishing)** – इसे टेलीफोन या मोबाइल द्वारा की जाने वाली धोखाधड़ी भी कहा जाता है। भारत जैसे देशों में वॉइस फिशिंग सबसे ज्यादा घटित होने वाला अपराध है। इस तरह के अनेकों मामले रोजना देखने और सुनने को मिलते हैं तथा उनकी शिकायतें भी दर्ज की जाती हैं। इस तरह की धोखाधड़ी में अपराधी किसी विश्वसनीय व प्रतिष्ठित संस्थान जैसे- बैंक, बीमा कम्पनी या सरकारी विभाग के नाम से लोगों को फोन करते हैं और

लोगों को उनके खातों या अन्य सुविधाओं के प्रति जिज्ञासु बना कर उनकी व्यक्तिगत जानकारियां जैसे- बैंक खाता संख्या, डेबिट/क्रेडिट कार्ड के नंबर व सीसीवी नं. इत्यादि जान कर धोखाधड़ी की घटनाओं को अंजाम देते हैं। पहले ये अपराधी लोगों को उनका बैंक खाता बंद होने, एटीम/डेबिट/क्रेडिट कार्ड की सेवाएं बंद होने आदि का झांसा देकर उनकी व्यक्तिगत जानकारियां हासिल किया करते थे। विगत वर्ष से इस तरह की साइबर ठगी के लिए अपराधियों ने लोगों से बैंक/वित्तीय संस्थानों में केवायसी (KYC- Know Your Customer) विवरण अपडेट न होने के बहाने से उनकी व्यक्तिगत जानकारियां हासिल करने का नुस्खा अपनाया है। रिजर्व बैंक के अनुसार वर्ष 2020 के दौरान पूरे भारत में 8700 से अधिक बैंक-धोखाधड़ी के मामले सामने आए हैं।[6]

बहरहाल, फिशिंग किसी भी तरह की हो, वह एक दण्डनीय अपराध है, जिसके बारे में सूचना प्रौद्योगिकी अधिनियम, 2000 (यथा-संशोधित 2008) की धारा 66(डी) और भा.द.सं. की धारा—419, 463, 465 एवं 468 में दण्डात्मक प्रावधान उल्लिखित हैं।

6. **ऑनलाईन पायरेसी (Online Piracy)-** वस्तुत: सृजनशीलता एक वरदान है। यदि कोई व्यक्ति या संस्था अपनी बौद्धिक व कलात्मक क्षमताओं से किसी वस्तु, कृति या सुविधा का सृजन करता है तो यह नितांत रुप से उसकी अपनी बौद्धिक संपदा होती है तथा वह व्यक्ति या संस्था यह कदापि नहीं चाहता कि उसकी कृति या सृजनात्मक कार्य की नकल की जाए और उसे गैर-कानूनी रुप से प्रचारित-प्रसारित या इस्तेमाल किया जाए। बौद्धिक संपदा के इसी अधिकार की रक्षा

6 https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases/

के लिए भारत में प्रतिलिप्याधिकार अधिनियम यानी कॉपीराइट एक्ट 1957 लागू किया गया है। वस्तुत: पायरेसी का शाब्दिक अर्थ है किसी साहित्य या सृजनात्मक कृति की चोरी। वैधानिक दृष्टि से देखा जाए तो हर उस वस्तु या सामग्री की नकल करना पायरेसी है, जिसे कॉपीराइट अधिनियम के तहत बौद्धिक संपदा के रूप में संरक्षण प्राप्त है। पिछले दशकों में सूचना-प्रौद्योगिकी की सहज-उपलब्धता के चलते पायरेसी एक आम बात हो गई है। उदाहरण के लिए आज की दुनिया में सीडी राईटर लगभग हर कम्प्यूटर का अभिन्न अंग है और संगीत या वीडियो फाइलों की कॉपी करना बहुत आसान हो गया है। यानि पायरेसी खुले आम बेधड़क चल रही है। और तो और लोगों को यह अहसास भी नहीं होता कि वे इंटरनेट से किसी फाइल/साफ्टवेयर को बिना अनुमति डाउनलोड करके और उसकी प्रतियां या कॉपी बना कर या फिर उसे प्रसारित या इस्तेमाल कर अनजाने में ही ऑनलाईन पायरेसी जैसा अपराध कर बैठते हैं। सॉफ्टवेयर की नकल तैयार कर सस्ते दामों में बेचना भी साइबर क्राइम के अन्तर्गत आता है, इससे साफ्टवेयर कम्पनियों को भारी नुकसान उठाना पड़ता है। वस्तुत:, इस तरह जाने-अनजाने ही सही मगर, साईबर पायरेसी एक दण्डनीय अपराध है, जिस पर सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008), कॉपीराइट एक्ट,1957 (यथासंशोधित, 2012), सिनेमोटोग्राफ एक्ट, 1952 और भा.द.सं. के संगत प्रावधान लागू होते हैं, जो अलग-अलग मामलों के आधार पर भिन्नता रखते हैं।

7. **अफवाह फैलाना-** बहुत से लोग सोशल नेटवर्किंग साइटों पर सामाजिक, वैचारिक, धार्मिक और राजनैतिक अफवाह फैलाने का काम करते हैं और आम नागरिक उनके इरादें समझ नहीं पाते तथा जाने-अनजाने में ऐसे लिंक्स को शेयर करते रहते हैं। वस्तुत: इन इलेक्ट्रॉनिक माध्यमों से झूठी जानकारी या अफवाह फैलाना सूचना प्रौद्योगिकी

अधिनियम, 2000(यथा-संशोधित 2008) की धारा-66(ए) के तहत दण्डनीय अपराध है। इसके अलावा सूचना प्रौद्योगिकी (मध्यवर्ती संस्थानों के लिये दिशा-निर्देश) नियम, 2018 में यह स्पष्ट रूप से कहा गया है कि मध्यवर्ती संस्थानों को कम्प्यूटर-संसाधनों का प्रयोग करने वाले लोगों को नियम-कानूनों तथा गोपनीयता-नीति के बारे में अनिवार्य रूप से बताना चाहिए ताकि वे ऐसी कोई भी जानकारी प्रस्तुत, प्रदर्शित, अपलोड, परिवर्तित, प्रकाशित, अपडेट या साझा न करें, जिससे लोक-स्वास्थ्य व सुरक्षा तथा महत्वपूर्ण सूचना-तंत्र को नुकसान पहुंचता हो। दरअसल, इलेक्ट्रॉनिकी और सूचना-प्रौद्योगिकी मंत्रालय द्वारा सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008) के बाद सूचना प्रौद्योगिकी (मध्यवर्ती संस्थानों के लिये दिशा-निर्देश) नियम, 2018 लागू करने का मूल उद्देश्य यही था कि झूठी खबरों को फैलने से रोका जाए और इंटरनेट पर बढ़ती अश्लीलता पर अंकुश लगाया जाए, सोशल मीडिया प्लेटफॉर्म के दुरूपयोग को रोका जाए और प्रयोगकर्ताओं को सुरक्षा प्रदान की जाए।

8. **साइबर बुलिंग-** बुलिंग(Bullying) का शाब्दिक अर्थ है डराना-धमकाना या बदमाशी करना। कानूनी रूप से बुलिंग जानबूझ कर किए जाने वाले किसी ऐसे कृत्य को कहा जाता है, जो भले ही अपराध की चेष्टा से न किया गया हो, लेकिन इससे किसी व्यक्ति को शारीरिक या मानसिक, कष्ट, पीड़ा या तकलीफ पहुंचती हो। अब यदि साइबर बुलिंग की बात की जाए तो यह एक ऐसी बुलिंग या उत्पीड़न है, जिसे इलेक्ट्रॉनिक या संचार माध्यमों जैसे कम्प्यूटर, मोबाइल फोन, लेपटॉप आदि पर टेक्स्ट मैसेज, फोन कॉल्स, ईमेल, इंस्टेन्ट मैसेन्जर, सोशल मीडिया प्लेटफॉर्म या चेट-रूम के माध्यम से अंजाम दिया जाता है। इसमें फेसबुक जैसी सोशल नेटवर्किंग साइट पर अशोभनीय कमेंट करना, इंटरनेट पर धमकियां देना, किसी का इस

स्तर तक मजाक बनाना कि वह तंग और व्यथित हो जाये, इंटरनेट पर दूसरों के सामने किसी को शर्मिंदा करना आदि जैसे कृत्य आम तौर पर देखने को मिलते हैं। सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008) की धारा-66(ई) एवं धारा-67 तथा भा.द.सं. की धारा-354(डी) के तहत साइबर बुलिंग के मामलों में अपराध की गंभीरता के अनुसार दण्डात्मक कार्रवाई के प्रावधान विद्यमान हैं।

9. **ऑनलाईन अश्लीलता फैलाना-** साइबर जगत में अश्लीलता की यदि बात की जाए तो यहां किसी भी तरह का अश्लील वीडियो बनाना और उसे इलेक्ट्रॉनिक माध्यमों से अपलोड करना, प्रसारित करना या साझा करना दण्डनीय अपराध की श्रेणी में आता है। सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008) की धारा-67(ए) और भा.द.सं. की धारा 292, 293, 294, 500, 506 एवं 509 के अंतर्गत ऑनलाईन अश्लीलता फैलाना दण्डनीय अपराध है।

10. **बाल-यौन-शोषण-सामग्री (CSAM-Child Saxual Abuse Material) का प्रकाशन व पारेषण-** बाल यौन शोषण सामग्री का तात्पर्य उस सामग्री से है, जिसमें किसी बच्चे, जिसके साथ दुव्यवहार किया गया है अथवा जिसका यौन शोषण किया गया है, का किसी भी रूप में यौनाचार संबंधी चित्र/वीडियो समाहित हो। ऐसी किसी भी सामग्री का प्रकाशन या पारेषण एक दण्डनीय अपराध है। यही नहीं बच्चों से ऑनलाइन रिश्ता रखना, बच्चों की अश्लीलता से भरी किसी वेबसाइट को ब्राउज करना भी दंडनीय अपराध है। सूचना प्रौद्योगिकी अधिनियम, 2000(यथा-संशोधित 2008) की धारा-67(बी) और भा.द.सं. की धारा 292, 293, 294, 500, 506 एवं 509 के अंतर्गत ऑनलाईन अश्लीलता फैलाना दण्डनीय अपराध है।

11. **निजता का अतिक्रमण (Violation of Privacy)-** किसी व्यक्ति की निजता का अतिक्रमण करते हुए, साशय या जानबूझ कर, उसकी सहमति के बिना, उसके गुप्तांगों के चित्र खींचना और उन्हें प्रकाशित व प्रसारित करना सूचना प्रौद्योगिकी अधिनियम 2000 की धारा-66 के तहत दण्डनीय अपराध है।

12. **साइबर स्क्वाटिंग (Cyber Squatting)-** अंग्रेजी शब्द Squat, जिससे Squatting शब्द बना है, का शाब्दिक अर्थ है किसी जगह पर अवैध रुप से रहना। इस शाब्दिक अर्थ से हमें साइबर स्क्वाटिंग की अवधारणा को सरल रूप में समझने में बड़ी मदद मिलती है, क्योंकि साइबर स्क्वाटिंग का अभिप्राय इससे काफी मिलता-जुलता है। सीधे अर्थों में साइबर जगत में किसी प्रयोगकर्ता के मनवांछित स्थान(डोमेन) पर किसी अपराधी द्वारा गैरकानूनी रूप से कब्जा जमा लेना ही स्क्वाटिंग कहलाता है। इसे और ज्यादा विस्तार से समझने के लिए हमें पहले डोमेन नेम (Domain Name) की अवधारणा को समझना होगा। दरअसल डोमेन नेम किसी वेबसाइट का नाम और पता है, जिसके माध्यम से कोई प्रयोगकर्ता उस तक पहुंचता है। इंटरनेट पर कम्प्यूटरों की पहचान डोमेन नेम से ही होती है। डोमेन नेम में अक्षरों और संख्याओं का समावेश होता है और इनके साथ इनके डोमेन नेम एक्सटेंशन जैसे -.com, .net भी जुड़े रहते हैं। प्रयोग से पहले डोमेन नेम को रजिस्टर करना होता है। हर डोमेन नेम अपने आप में अद्वितीय होता है। किन्हीं भी दो वेबसाईटों का एक ही डोमेन नेम कभी नहीं हो सकता। उदाहरण के तौर पर यदि कोई व्यक्ति www.abcin.com टाइप करता है तो वह उसी डोमेन नेम की वेबसाइट पर जाएगा न कि किसी ओर वेबसाइट पर। डोमेन नेम को हर वर्ष नवीनीकृत करवाना होता है और यह कार्य बहुत तत्परता से करना होता है क्योंकि यदि ऐसा नहीं किया जाता तो साइबर स्क्वाटिंग

करने वाले इस पर अपना कब्जा जमा सकते हैं और इसके लिए मोटी रकम की मांग कर सकते हैं। साइबर स्क्वाटिंग में किसी प्रतिष्ठित कम्पनी या ब्रांड के नाम से इंटरनेट डोमेन्स को रजिस्टर कर लिया जाता है, ताकि इसे बाद में उन कम्पनियों को बेचा जा सके। उदाहरण के लिए सितम्बर 2015 में गूगल के एक भूतपूर्व कर्मचारी सन्मय वेद ने जब यह देखा कि Google.com नामक डोमेन विक्रय के लिए उपलब्ध है तो उसने इस मात्र 12 डॉलर्स में खरीद लिया और बाद में गूगल ने इसे खरीदने के लिए वेद को 6066 डॉलर्स का भुगतान किया।[7] वस्तुत: भारत में डोमेन नेम संरक्षण के लिए अभी तक कोई कानून नहीं बनाया गया है और ऐसे ज्यादातर मामले ट्रेडमार्क एक्ट-1999 के तहत निपटाये जाते हैं।

13. **साइबर स्टॉकिंग (Cyber Stalking)-** Stalking का शाब्दिक अर्थ है , पीछा करना। साइबर स्टॉकिंग में कोई व्यक्ति या व्यक्तियों का समूह किसी दूसरे व्यक्ति या व्यक्तियों के समूह का इंटरनेट के जरिए पीछा करता है और उसे कई तरह से नुकसान पहुंचाने और प्रताड़ित करने की चेष्टा करता है। इसमें इंटरनेट के जरिए किसी की गतिविधियों पर नज़र रखना, उस पर झूठे आरोप लगाना, उसे धमकी देना, उसकी पहचान चुरा लेना, उसके डेटा या उपकरण के साथ छेड़छाड़ करना और नुकसान पहुंचाना, अपशब्द कहना, यौन उत्पीड़न देना या छेड़छाड़ करना आदि शामिल है। इन हथकंडों का इस्तेमाल करते हुए इंटरनेट के जरिए किसी को नुकसान पहुंचाना ही 'साइबर स्टॉकिंग' कहलाता है। ऐसे अपराधों के लिए इंटरनेट के साथ-साथ मोबाइल फोन का इस्तेमाल भी 'स्टॉकिंग' की श्रेणी में आता है। साइबर स्टॉकिंग को भारतीय दंड संहिता की धारा-354 सी एवं 354-डी के तहत अपराध घोषित किया गया है।

7 https://blog.ipleaders.in/laws-tackling-cyber-squatters-cyber-squatting/

14. **साइबर आतंकवाद (Cyber Terrorism)-** देश की एकता, अखण्डता, सुरक्षा या संप्रभुता को ख़तरे में डालने के मकसद से कम्प्यूटरों एवं इंटरनेट के माध्यम से किया गया कोई भी प्रयास साइबर अपराधों की श्रेणी में आता है और सूचना-प्रौद्योगिकी अधिनियम-2000 की धारा 66(एफ) और अन्य आंतकवाद निरोधक कानूनों के तहत दण्डनीय अपराध है।

15. **अन्य अपराध जो साइबर अपराधों की श्रेणी में गिने जाते हैं-** उपरोक्त अपराधों के अतिरिक्त कुछ अन्य अपराध भी दण्डनीय साइबर अपराधों की श्रेणी में आते हैं, जैसे- संचार सेवाओं के माध्यम से किसी व्यक्ति को आक्रामक संदेश भेजना(आईटी एक्ट की धारा-66ए), चोरी किए गए किसी कम्प्यूटर या संचार उपकरण को बेईमानी से हासिल करना(आईटी एक्ट की धारा-66बी) ।

प्रकृतिवश साइबर अपराध कम्प्यूटर और सूचना-प्रौद्योगिकी से जुड़े हुए अपराध हैं। कम्प्यूटर व स्मार्ट फोन जैसे कई अत्याधुनिक उपकरण सूचना-प्रौद्योगिकी की सुविधाओं के साथ आज जन-जन के हाथों में मौजूद हैं। साइबर जगत में आपराधिक प्रवृत्ति से जनित इरादों को मूर्तरूप देने में जरा वक्त नहीं लगता है। आश्चर्य की बात ये है कि साइबर अपराधी भले ही कम्प्यूटर जगत एवं सूचना-प्रौद्योगिकी क्षेत्र में शिक्षित व प्रशिक्षित हो या न हो, लेकिन वे अपराध जगत में कदम रखने के बाद या आंतरिक आपराधिक प्रवृत्तियों से प्रेरित होने के बाद ऐसे जटिल व भयावह साइबर अपराधों को अंजाम दे देते हैं, जो आज के दौर में सुरक्षा एजेंसियों और पुलिस-व्यवस्था के लिए हर कदम एक नई चुनौती उत्पन्न करते हैं। इस बात से कदापि इंकार नहीं किया जा सकता है कम्प्यूटर एवं अन्य कम्प्यूटरीकृत उपकरणों के साथ सूचना-प्रौद्योगिकी से हमें मिलने वाली सुविधाएं व लाभ असीमित हैं और इसीलिए साइबर जगत में खतरों की संभावनाएं भी असीमित हैं।

वर्तमान परिवेश की यदि बात की जाए तो यहां कम्प्यूटर, मोबाइल फोन, स्मार्ट फोन तथा सूचना व संचार प्रौद्योगिकी का हाथ थाम कर अपराधी हर दिन एक नए अंदाज में अपने नापाक मनसूबों को अंजाम देते नजर आते हैं। यहां कुछ बिरले मामलों पर नजर डालना बहुत ही प्रासंगिक है। मिसाल के तौर पर इन पांच दृष्टांतों से यह साफ तौर पर पता चलता है कि साइबर अपराध किस तरह से नित्य-नया स्वरूप बदल रहे हैं-

दृष्टांत-1 : एक शख़्स ने अपनी ही पत्नी की निजी तस्वीरें सोशल मीडिया पर साझा कर दी!

हाल ही में दहेज प्रताड़ना से परेशान एक विवाहिता मायके क्या गई, उसके पति ने उसकी निजी तस्वीरों को वॉट्सऐप और फेसबुक पर अपलोड कर दिया। इन तस्वीरों पर आरोपी ने अशोभनीय टिप्पणियां भी कीं। इन तस्वीरों के सोशल मीडिया पर वायरल होने की जानकारी मिलने पर पीड़िता ने शिकायत दर्ज की।8 इस मामले से यह जाहिर होता है साइबर अपराधी आदतन अपराधी नहीं होते, बल्कि बदलती मानसिक प्रवृत्तियां भी उन्हें कई बार साइबर अपराधों की ओर धकेल देती हैं।

दृष्टांत-2 : दिल्ली के लक्ष्मी नगर से फर्जी अंतरराष्ट्रीय टेलीफोन एक्सचेंज का पर्दाफाश!

पुलिस ने एक ऐसे गिरोह का पर्दाफाश किया जो एक गेटवे बनाकर भारतीय टेलीफोन नंबरों पर अंतरराष्ट्रीय वॉइस कॉल ट्रांसफर कर रहा था। आरोपियों ने मुंबई में अपना फर्जी टेलीकॉल एक्सचेंज खोल रखा था। विदेश से आने वाली कॉल्स जब उनके पास आती थीं तो वे उन कॉल्स को नोएडा स्थित फर्जी एक्सचेंज पर ट्रांसफर कर देते थे। यहां से इन कॉल्स को जम्मू-कश्मीर के अलावा देश के कई राज्यों में ट्रांसफर किया जाता था। ऐसी काल्स को

8 https://www.livehindustan.com/ncr/story-husband-made-viral-obscene-photos-of-his-wife-on-social-media-3938273.html

कनेक्ट करने के लिए लिए यह गिरोह प्रत्येक मिनिट के लिए 10 पैसे वसूल करता था।[9]

दृष्टांत-3 : सिम कार्ड को 4जी/5जी पर अपग्रेड करने के बहाने बैंक खाते से रकम साफ!

पुलिस ने 'साइबर ठगों के गढ़' झारखण्ड के जामताड़ा और कर्नाटक से ऑनलाईन ठगी करने वाले गिरोह का पर्दाफाश किया। ये आरोपी टेलीकॉम कम्पनी के कर्मचारी बनकर लोगों को कॉल करते थे और उनकी सिम को 4G से 5G में अपग्रेड करने का झांसा देते थे। उसके बाद आरोपी लोगों को उनके सिम कार्ड नंबर से IMSI नंबर कस्टमर केयर नंबर पर भेजने को कहते थे। लोगों के सिम कार्ड को अपनी सिम पर एक्टिवेट करके वे फोन व लिंक किए गए बैंक अकांउट को हैक कर नेट बैंकिग के जरिए उनके खाते से पैसे निकाल लेते थे।[10]

दृष्टांत-4 : मेटरीमोनियल साइट पर लाखों की ठगी!

एक अनूठे प्रकरण में एक मेटरीमोनियल वेबसाइट के माध्यम से एक युवक का एक युवती से सम्पर्क हुआ। इस दौरान युवती ने बताया कि वह विदेश में रहती है और युवक एवं युवती के बीच वैवाहिक बातचीत हुई। कुछ समय बाद युवती ने युवक को विदेश से कुछ उपहार भेजने की बात कही और युवक प्रलोभन में आकर युवती की बातों में आता चला गया। युवक के पास कई बार विदेश से खुद को सरकारी अथवा पार्सल अधिकारी बता कर कॉल

9 https://www.livehindustan.com/ncr/story-man-arrested-fof-foreign-call-transferr-came-from-mumbai-to-delhi-to-meet-his-girlfriend-3876782.html

10 https://ndtv.in/crime-news/cyber-crime-grabbed-lakhs-of-rupees-in-the-name-of-upgrading-sim-eight-arrested-from-jamtara-and-karnataka-2302395

किए गए और उसे कहा गया कि उसे भेजा गया उपहार बहुत कीमती है, जिसके लिए उसे एक खाता खुलवा कर धनराशि जमा करवानी होगी। इस तरह से उस युवक के साथ लगभग 9.5 लाख की ऑनलाईन ठगी की गई। [11]

दृष्टांत-5 : कोविड-19 टीकाकरण के नाम पर साइबर ठगी!

सच तो ये है कि साइबर ठग या साइबर अपराधी अपनी करतूतों को अंजाम देने के लिए एक भी मौका नहीं छोड़ते। जहां एक ओर पूरा विश्व कोराना महामारी से जूझ रहा है, वहीं साइबर अपराधी कोविड-19 की रोकथाम के लिए चलाए जा रहे टीकाकरण अभियान को भी एक बड़ा अवसर मान कर खूब भुना रहे हैं। नोएडा में साइबर सेल को ऐसी कई शिकायतें मिली हैं, जिसमें साइबर ठग खुद को स्वास्थ्य विभाग का कर्मचारी बताकर लोगों से संपर्क करते हैं और कोविड-19 का टीका लगाने हेतु पंजीकरण कराने के नाम पर ई-मेल, आधार संख्या आदि की जानकारी मांगते हैं। साइबर ठग लोगों से कहते हैं कि पंजीकरण के लिए आपके पास ओटीपी आएगा, जैसे ही लोग उन्हें ओटीपी बताते हैं, उनके खाते से पैसा निकाल लिया जाता है।[12]

इन मामलों से स्पष्ट होता है कि हम भले ही साइबर अपराधों को सैद्धांतिक रूप से लाख बार परिभाषित व परिमार्जित करके देख लें, लेकिन हम आपराधिक प्रवृत्तियों के नित्य–नए इरादों की थाह नहीं पा सकते। हमारे सामाजिक-आर्थिक परिवेश में हो रहे अनवरत परिवर्तन जग-जाहिर हैं। वहीं कम्प्यूटर एवं सूचना व संचार प्रौद्योगिकी की उन्नति एवं विकास से जुड़ा हर पहलू जन-जन की पहुंच में है। एक तो साइबर अपराध के घटित होने से पहले साइबर अपराधियों की पहचान नामुमकिन है, दूसरे उन्हें अपने लक्ष्य

11 https://mp.punjabkesari.in/madhya-pradesh/news/young-man-cheated-on-matrimonial-sites-1206651

12 https://www.abplive.com/states/up-uk/noida-cyber-fraud-is-being-done-in-the-name-of-corona-vaccine-police-issued-alert-1704552

को प्राप्त करने के लिए जरूरी जानकारी बहुत आसानी से मिल जाती है और तीसरे सूचना व संचार प्रौद्योगिकी से जुड़े संसाधनों के प्रयोग को सीमित नहीं किया जा सकता। इन हालातों में आपराधिक प्रवृत्ति के व्यक्तियों द्वारा साइबर अपराधों को अंजाम देना बहुत आसान हो जाता है। ऐसे माहौल में खुरापाती आपराधिक मनोवृत्तियों के चलते नित्य-नए किस्म के साइबर अपराधों से जूझना वाकई पुलिस के लिए एक बड़ी चुनौती है। भारत जैसे विकासशील देश में यदि साइबर अपराधों से निपटने के लिए अपनाई जा रही न्यायिक-प्रक्रिया पर नजर डालें तो स्थिति यहां भी बहुत ही निराशाजनक प्रतीत होती है। मसलन- केंद्र सरकार द्वारा संसद में दी गई जानकारी के अनुसार वर्ष 2018 में देश में साइबर अपराध के 27,248 मामले सामने आए थे, वहीं वर्ष 2019 में इनकी संख्या तेजी से बढ़ कर 44,546 तक जा पहुंची। इन साइबर अपराध के मामलों में 2018 में 13,569 लोगों को गिरफ्तार किया गया था, जिनमें से केवल 495 मामलों में अरोपियों पर दोष सिद्ध हुआ । जबकि वर्ष 2019 में 15,212 लोगों को गिरफ्तार किया गया था, जिनमें से केवल 366 मामलों में ही दोष सिद्ध हो सका था। साइबर अपराधों में पकड़े गए कुल व्यक्तियों में 2018 में केवल 601 लोगों को और 2019 में केवल 485 लोगों को सजा सुनाई गई ।[13]

निश्चित रुप से वर्तमान परिवेश में साइबर अपराधियों के हौसले बुलंद होते जा रहे हैं और वे अपनी पूरी क्षमता के साथ साइबर अपराधों को रोज नए-नए तरीकों से अंजाम दे रहे हैं। चाहें फिर वह बैंक खाते में केवाईसी अपडेट करने संबंधी कॉल हो, फर्जी फेसबुक आईडी बना कर मैसेंजर के जरिये लोगों से उधार मांग कर धन की उगाही हो, ईएमआई में छूट का वादा करके की जाने वाली ठगी हो, पीएम केयर फण्ड के लिए नकली आईडी/यूपीआई बना कर

13 https://www.amarujala.com/technology/tech-diary/cyber-frauds-are-increasing-but-due-to-weak-it-act-cyber-criminals-are-escaping-easily

धन की वसूली हो, प्रोमो-कोड/रिवॉर्ड प्वाँइट के नाम पर दिया जाने वाला झांसा हो, ऑनलाईन खरीद के नाम पर की जाने वाली धोखाधड़ी हो, सोशल नेटवर्क साइटों के माध्यम से फैलाई जा रही अश्लीलता हो, व्यक्तिगत डाटा की चोरी हो, साइबर अपराधी अपने हर दाव के लिए एक नया पैंतरा आजमाते हैं, जिसे समझने के लिए पुलिस बलों एवं सुरक्षा एजेंसियों को अपराधियों की भांती ही शातिराना अंदाज में सोचना होगा और फिर उन्हें रोकने के लिए सबसे पहले व्यापक रुप से जन-जागरूकता फैलानी होगी, ताकि साइबर अपराधों को उनके उदगम पर ही रोका जा सके।

अध्याय 3

साइबर अपराधों के अखिल भारतीय आंकड़ों का क्षेत्रवार गहन विश्लेषण

विज्ञान, प्रौद्योगिकी और साइबर अपराध

मानव सभ्यता के विकास में सबसे बड़ा योगदान विज्ञान का ही रहा है। कहा जाता है कि आवश्यकता ही अविष्कार की जननी है। मानव ने अपनी उत्पत्ति से आधुनिकता के इस दौर तक आते-आते हर बार अपनी आवश्यकताओं की पूर्ति के लिए नित्य नई खोज की है। उसने सबसे पहले अग्नि और फिर पहिए का अविष्कार किया। इसके बाद तो जैसे उसकी प्रगति में ही पहिए लग गए और मानव एक के बाद एक अविष्कार पर अविष्कार करता चला गया। आज गहरे पाताल से लेकर अंनत अंतरिक्ष तक विज्ञान ही विज्ञान है। विज्ञान के अविष्कारों के बदौलत ही आज हम सूचना और संचार प्रौद्योगिकी की क्रांति के इस युग के साक्षी बन सके हैं। विज्ञान और प्रौद्योगिकी को अनेकों बार एक ही अर्थ में समझा जाता है। इन्हें एक दूसरे का पर्यायवाची भी माना जाता है। परंतु वास्तविक रुप में विज्ञान और प्रौद्योगिकी सैद्धांतिक दृष्टिकोण से बहुत अलग हैं। विज्ञान स्वयं के लिए ज्ञानार्जन करता है और प्रौद्योगिकी विज्ञान की सहायता लेकर ऐसी वस्तुएं और साधन मुहैया कराती है, जिनसे मानव की समस्याओं का समाधान होता है या जो उसके जीवन स्तर को पहले से बेहतर बनाते हैं। दूसरे शब्दों में किन्हीं खास उद्देश्यों के लिए विज्ञान के सिद्धांतों का उपयोग प्रौद्योगिकी का कार्यक्षेत्र होता है। अर्थात यदि विज्ञान किसी वस्तु या पदार्थ की खोज करता है, उसके उदभव के सिद्धांत का पता लगाता है तो प्रोद्यौगिकी इसके आगे चल कर उस वस्तु, पदार्थ या सिद्धांत के सदुपयोग की योजना व पद्धति बनाती है। सच कहें

तो प्रौद्योगिकी विज्ञान के उपयोग की नई-नई तरकीबों, तकनीकों और नई प्रक्रियाओं का विस्तृत कार्यक्षेत्र है, जिनसे मानव जीवन की उन्नति, प्रगति तथा सहूलियतों के लिए संसाधन जुटाए जाते हैं।

विज्ञान ने अपने अनगिनत अविष्कारों में मानव को दूर रहकर आपसी सम्पर्क का वरदान दिया है। टेलीग्राफ, टेलीफोन, पेज़र, मोबाईल फोन, स्मार्ट फोन, कम्प्यूटर, लेपटॉप, इंटरनेट, वर्ल्ड वाईड वेब जैसे चमत्कृत कर देने वाले संसाधनों ने सारी दुनिया को मानव की मुट्ठी में समेट कर रख दिया है। यह युग सूचना एवं संचार प्रौद्योगिकी का युग कहा जाता है। आज सारी दुनिया में कम्प्यूटरीकरण, इंटरनेट सेवाओं, दृश्य-श्रव्य प्रचार माध्यमों, डिजिटल सुविधाओं, इन्सटेन्ट ग्राहक सेवा पद्धतियों और स्वचलित मशीनों का मानो जाल जैसा बिछा हुआ है। ये वो दौर है जब हम अपने मोबाईल फोन की स्क्रीन पर कुछ विकल्प चुन कर टिकट बुकिंग, बैंकिग, खरीद-फिरोख़्त, चिकित्सा सुविधा, यात्रा-सुविधा और मनोरंजन सुविधाओं का लाभ पलक झपते ही उठा सकते हैं। नई प्रौद्योगिकी के आगमन से हमारे लिए सुविधाओं और सहूलियतों का अंबार लग गया है और सुविधाएं भी ऐसी जो हर पल हर समय हमारे साथ चलती हैं, लेकिन इस युग में पूरे विश्व में सामाजिक-आर्थिक परिवेश में कुछ ऐसे विपरीत परिवर्तन आएं हैं, जिन्हें नज़रअंदाज करना पूरी मानव जाति को काफी मंहगा पड़ रहा है। प्रौद्योगिकी से बदलते परिवेश का असर सीधे तौर पर मानव के मन-मस्तिष्क पर पड़ रहा है। प्रौद्योगिकी से घिरे इस युग में मनुष्य का मनुष्य से सरोकार ख़त्म होता जा रहा है, जो मानव सभ्यता के लिए बेहद हानिकारक है। दुनिया भर में अपराधों का बढ़ता ग्राफ यही दर्शाता है कि प्रौद्योगिकी के इस युग में मानव के मन-मस्तिष्क में बेफिक्री बढ़ती जा रही है और वह बहुत हद तक प्रौद्योगिकी पर निर्भर रहने लगा है। इस जमाने में एक और सबसे ख़तरनाक मानवीय अवगुण विकसित हो रहा है और वह है उतावलापन। विज्ञान एवं प्रौद्योगिकी ने मानव को हर वस्तु इतनी तेज़ी से सुलभ करवाई है कि वह अब

बेसब्र हो चला है। सबको सब कुछ तुरंत चाहिए और इस दौर में देरी का सवाल ही नहीं उठता, क्योंकि सूचना व संचार प्रौद्योगिकी ने यह सब संभव कर दिखाया है।

अब सवाल यह उठता है कि जब सब कुछ अपनी मुट्ठी में है तो इंसान की चाहत तुरंत पूरी क्यों न हो, फिर चाहें ये चाहत अच्छी हो या बुरी, पाप हो या पुण्य, सही हो या गलत, कर्म हो या अपराध। प्रौद्योगिकी ने सबको उतावला बना दिया है और जब बात अपराधिक प्रवृत्तियों की हो तो उन्हें तो जैसे खुले आसमान में उड़ने को पंख मिल गए हैं। यूं तो समाज में अपराधिक प्रवृत्तियां इसके उदभव से ही विद्यमान कही जाती हैं, क्योंकि मानव मस्तिष्क से संचालित होता है और मस्तिष्क का समय-समय पर सकारात्मक व नकारात्मक होना एक स्वाभाविक प्रवृत्ति है। दुराचार या अपराध मस्तिष्क की नकारात्मक प्रवृत्तियों का परिणाम है। जैसे-जैसे समाज बढ़ता रहा अपराधों की किस्में और संख्या भी बढ़ती रहीं है। सच तो ये है कि अपराधिक प्रवृत्तियां समाज के बाहर से नहीं आती, बल्कि समाज में विद्यमान विकृत-मानसिकताओं के चलते समाज के भीतर ही जन्म लेती और पनपती हैं। समय के साथ बदलते परिवेश में जैसे-जैसे मानव समाज उन्नति करता गया, आपराधिक प्रवृत्तियां भी उन्नत होती चली गईं और कानून-व्यवस्था के सामने चुनौती बन कर उभरने लगीं। तिस पर नई प्रौद्योगिकी का प्रभाव समूचे विश्व और समाज पर छाया हुआ है और अपराध जगत भी इससे अछूता नहीं है। बल्कि अपराध जगत ने तो अपने नापाक इरादों को कामयाब बनाने के लिए नई प्रौद्योगिकी का सबसे जल्दी और सबसे ज्यादा सहारा लिया है। प्रौद्योगिकी का हाथ धाम कर पारम्परिक किस्म के कुछ अपराधों ने अब नया रूप धारण कर लिया है। सूचना और संचार प्रौद्योगिकी ने विश्व भर में आपराधिक जगत को और उसके तानेबाने को और ज्यादा मज़बूत बनाया है। बीते वर्षों में भारत में पैर पसारते आतंकवाद, अलगाववाद, उग्रवाद और नक्सलवाद को ही ले लीजिए, सूचना और संचार प्रौद्योगिकी ने इन्हें अपनी

गतिविधियों के विस्तार में खासी मदद प्रदान की है। आज चोरी लूट, डकैती, अपहरण, हत्या इत्यादि जैसे पारम्परिक अपराधों में मोबाईल फोन और सोशल मीडिया का प्रयोग तो एक आम बात हो गई है। इसके अलावा हवाला, नशीले पदार्थों की तस्करी, मानव तस्करी, मानव अंगों की तस्करी, हथियारों की तस्करी जैसे अपराधों में भी सूचना एवं संचार प्रौद्योगिकी का बखूबी इस्तेमाल किए जा रहा है और ऐसे गिरोह अब पहले से ज्यादा आसानी और कुशलता से अपना काम कर रहे हैं। हालांकि यह भी सत्य है कि जिस सूचना और संचार प्रौद्योगिकी का इस्तेमाल अपराधों को अंजाम देने में किया जाता है, वही इलेक्ट्रॉनिक संसाधन अपराधियों की धरपकड़ में पुलिस तथा सुरक्षा एजेंसियों को बड़ी सफलताएं दिलाते हैं, क्योंकि सूचना एवं संचार प्रौद्योगिकी की सहायता से अपराधियों के खिलाफ सारे सुराग मिल जाते हैं और उन्हें पकड़ना आसान हो जाता है। फिर भी यह दावे के साथ कहा जा सकता है कि सूचना एवं संचार प्रौद्योगिकी ने सारी दुनिया में अपराध जगत को नई ताकत दी है।

अब यदि विज्ञान और प्रौद्योगिकी के साथ साइबर अपराधों पर एक नज़र डालें तो हम पाते हैं कि नए जमाने में साइबर अपराध पुलिस तथा सुरक्षा एजेंसियों के लिए एक नई चुनौती बन कर उभरे हैं। कहा जाता है कि किसी कार्य को करने से पहले यदि उससे जुड़ी सारी जानकारियां हाथ लग जाएं तो फिर एक योजना बना कर उस कार्य को पूर्ण करना बहुत आसान हो जाता है और सफलता भी लगभग तय हो जाती है। अपराधियों ने आधुनिक सूचना और संचार प्रौद्योगिकी का पूरा लाभ उठाना शुरु कर दिया है और वे इसके प्रयोग से किसी व्यक्ति या स्थान के बारे में दबे-छिपे काफी जानकारियां हासिल कर लेते हैं और फिर अपना एक नेटवर्क तैयार कर अपराधों को संगठित रुप से अंजाम देते हैं। इसका सबसे सहज उदाहरण है बैंकों के क्रेडिट एवं डेबिट कार्डों से होने वाली धोखाधड़ी। आए दिन हम सुनते हैं कि किसी व्यक्ति के पास अमूक बैंक से एक फोन आया, उसने पूछे जाने

पर अपना व्यक्तिगत विवरण, कार्ड नम्बर, सीवीवी कोड, पासवर्ड या पिन संख्या बता दिया और कुछ ही मिनटों में उसके बैंक खाते से धन गायब हो गया। ये घटनाएं बहुत ही आम हैं, लेकिन सच्चाई ये है कि इस प्रकार की धोखाधड़ी संगठित अपराधों की श्रेणी में आती है, जिसे कई जगहों पर अपराधियों के बड़े-बड़े गिरोह सूचना व संचार प्रौद्योगिकी का लाभ उठा कर अंजाम देते आ रहे हैं।

गुमनामी और झूठी पहचान (Anonymity and Fake Identity) साइबर अपराधों की सबसे बड़ी खासियत है। सबसे बड़ी विडम्बना ये है कि साइबर अपराधों को न केवल देश के भीतरी हिस्सों में बल्कि सरहदों के आरपार एक देश से दूसरे देश यानि अंतरराष्ट्रीय स्तर पर भी अंजाम दिया जा रहा है। यहां सबसे बड़ी दुविधा यही है कि हम साइबर अपराधी की पहचान और उसके स्थान का प्रथम-दृष्टया कोई पता नहीं लगा पाते और फिर नुकसान को देखकर इतने हतप्रभ हो जाते हैं कि काफी समय तक इस सदमे से खुद को बाहर नहीं निकाल पाते। उदाहरण के लिए यदि साइबर अपराध फोन पर हुई कोई वित्तीय धोखाधड़ी की घटना है तो इसका शिकार व्यक्ति बहुत देर तक तो स्वयं ही उस संदिग्ध अपराधी के मोबाइल या फोन नम्बर पर कॉल करके उस पर झुंझलाने की कोशिश करता रहता है। नतीजा ये होता है कि इस देरी में अपराधी कानून के हाथों से और दूर निकल जाता है या समय मिलने पर और ज्यादा नुकसान पहुंचा देता है और फिर यदि कभी उससे बात हो भी गई तो दोनों तरफ से झड़प, धमकी और गाली-गलौच के अलावा कुछ और हो ही नहीं पाता।

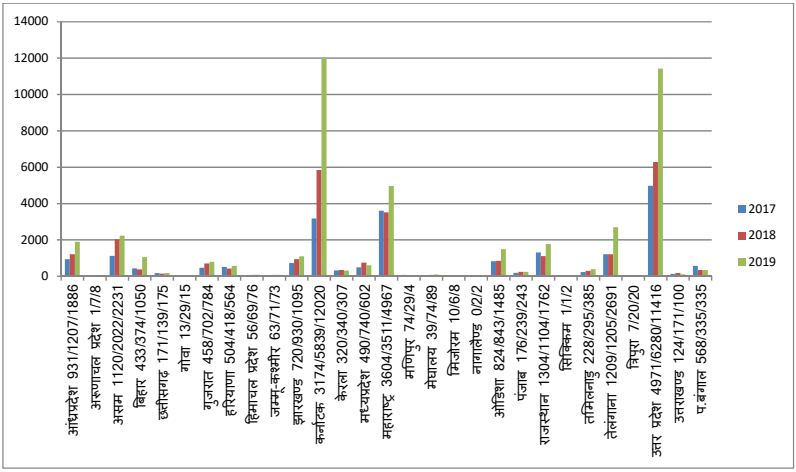
अंततया साइबर अपराधी अपने शिकार को नुकसान पहुंचा कर ऐसे अंतरध्यान हो जाता है जैसे वो कहीं था ही नहीं। न उसका नाम पता चलता है और न पता-ठिकाना। आज पुलिस के पास ऐसी धोखाधड़ी के कई मामले दर्ज हैं। कुछ मामलों में अन्वेषण जारी हैं तो कुछ को कोई सुराग न मिलने के

कारण बंद कर दिया गया है। सरकार की अनेक वेबसाईटें, विज्ञापन और सुरक्षा संगठन बार-बार नागरिकों से आह्वान करते हैं कि वे सूचना और संचार प्रौद्योगिकी के इस दौर में पूरी सतर्कता बरतें और अपने व्यक्तिगत ब्यौरे किसी से साझा न करें, फिर भी ऐसे आम, छोटे मगर संगठित साइबर अपराधों में कमी नज़र नहीं आ रही है और आए दिन लोग एक नहीं तो दूसरे माध्यम से इसका शिकार हो रहे हैं, जैसे- बैंकों की फर्जी टेलीफोन काल्स, टूर पैकेज के ऑफर, ऑनलाईन खरीद-फिरोख्त आदि।

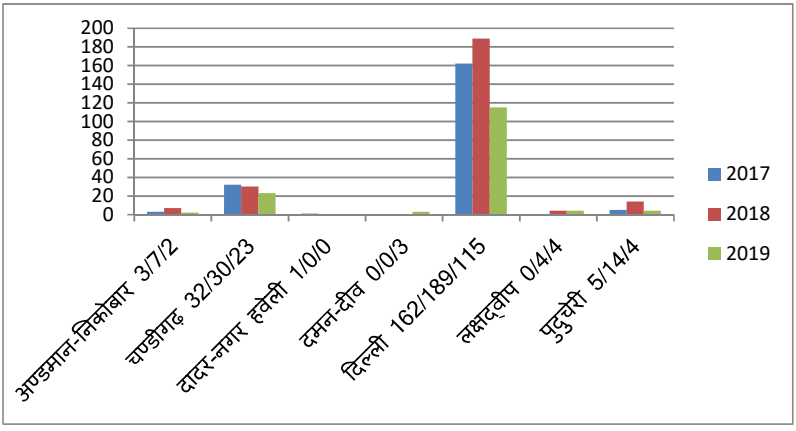
ये तो हुई बात सामान्य साईबर अपराधों की, लेकिन इससे भी कहीं ज्यादा गंभीर किस्म के साइबर अपराध हैं, जो भारत के विभिन्न हिस्सों में आम तौर पर घटित होते हैं, जैसे- सोशल मीडिया प्लेटफॉर्म पर साइबर मानहानी(Cyber Defamation), साइबर अश्लीलता और अश्लील साहित्य, चित्र व वीडियो का प्रदर्शन (Cyber Obscenity and Pornography), साइबर सेंधमारी(Cyber Stalking), हैकिंग(Hacking), निजता का उल्लंघन(Privacy Infringement), इंटरनेट पर धोखाधड़ी (Internet Fraud), वायरस के द्वारा कम्प्यूटर सिस्टम को अनधिकृत रूप से नुकसान पहुंचाना (Unauthorized disruption of Computer Systems through Virus) और किसी के कॉपीराईट का अनधिकृत रूप से इस्तेमाल (Using a Person's copyright) आदि। इनके अलावा भी दुनिया के साथ साथ भारत में सामाजिक और आर्थिक जगत में कई प्रकार के साइबर अपराध घटित होते हैं। इस संदर्भ में भारत के राष्ट्रीय अपराध रिकॉर्ड ब्यूरो द्वारा जारी "क्राइम इन इंडिया-2019" के भाग दो में उल्लिखित अद्यतन आंकड़ों का अवलोकन प्रमाणिक अध्ययन के लिए बहुत ही प्रासंगिक है। इस रिपोर्ट में हमें तत्कालीन 29 राज्यों और 7 केन्द्र शासित प्रदेशों के वर्ष 2017 से 2019 तक के आंकड़ें मिलते हैं[1], जिनका एक ग्राफ यहां प्रदर्शित है-

1 https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf

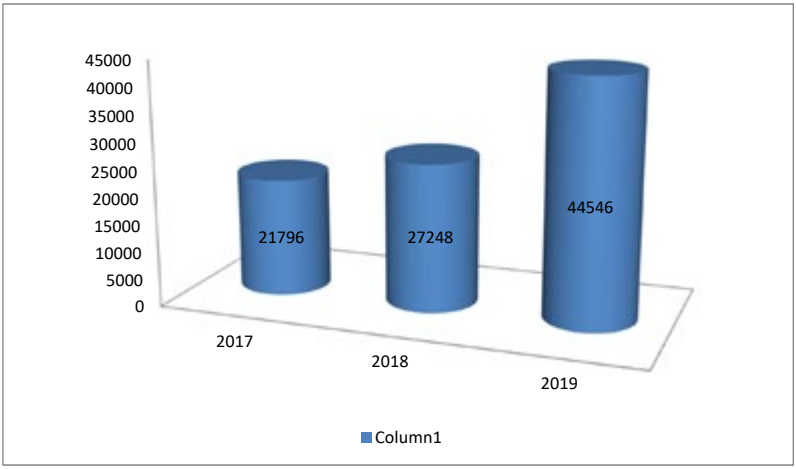
(क) वर्ष 2017, 2018 एवं 2019 में भारत के 29 राज्यों में साइबर अपराधों की स्थिति



(ख) वर्ष 2017, 2018 एवं 2019 में भारत के 7 केन्द्र शासित प्रदेशों में साइबर अपराधों की स्थिति



(ग) अखिल भारतीय स्तर पर वर्ष 2017, 2018 एवं 201 में साइबर अपराधों की स्थिति



भारत में सभी राज्यों और केन्द्र शासित प्रदेशों को मिला कर वर्ष 2017 में 21796, वर्ष 2018 में 27,248 और वर्ष 2019 में 44,546 साइबर अपराध घटित हुए। इन विस्तृत आंकड़ों के क्षणिक विश्लेषण से ही हमें ज्ञात होता है कि साइबर अपराध भारत में किस तेज़ी से बढ़ रहे हैं। राज्यों में क्रमश: कर्नाटक, उत्तर प्रदेश एवं महाराष्ट्र में सर्वाधिक साइबर अपराध घटित हो रहे हैं। वर्ष 2019 में कर्नाटक में 12,020, उत्तर प्रदेश में 11,416 और महाराष्ट्र में 4,967 साइबर अपराध पंजीबद्ध किए गए। वहीं केन्द्र शासित प्रदेशों की यदि बात की जाए तो यहां दिल्ली में वर्ष 2019 के दौरान 115 साइबर अपराध पंजीबद्ध किए गए।

वर्ष 2018 और 2019 के राष्ट्रीय अपराध रिकॉर्ड ब्यूरो के आंकड़ों के तुलनात्मक अध्ययन से पता चलता है कि इस दौरान पुलिस द्वारा देश भर में पंजीकृत अपराधों में सीधे 63.5% प्रतिशत की वृद्धि हुई है, जो पुलिस और सुरक्षा एजेंसियों के लिए वाकई चिंता का विषय है। अपराध की दर

(Crime Rate) राष्ट्रीय अपराध रिकॉर्ड ब्यूरो का एक अहम मानदण्ड है। सांख्यिकीय विश्लेषणों को और ज्यादा प्रभावी बनाने के लिए अपराध की दर प्रति लाख जनसंख्या के आधार पर निकाली जाती है, जिसका सूत्र है- कुल पंजीबद्ध अपराध/जनसंख्या (लाख में) = अपराध की दर। अब यदि राष्ट्रीय अपराध रिकॉर्ड ब्यूरो के आंकड़ों पर नज़र डालें तो वर्ष 2018 में अपराध की दर 2.0% थी जो वर्ष 2019 में बढ़कर 3.3% हो गई। वर्ष 2019 में पंजीबद्ध किए गए 44,546 मामलों में से 60.4% मामले यानी 26,891 अपराध धोखाधड़ी के मकसद से अंजाम दिए गए थे, जबकि 5.1% यानी 2,266 प्रकरण यौन उत्पीड़न के थे और 4.2% मामले यानी 1,874 मामले अपराधों की वजह से लोगों को मानहानि पहुंचाने वाले थे।[2]

वहीं यदि विशेष तौर पर सूचना प्रौद्योगिकी अधिनियम की धाराओं के अंतर्गत दर्ज अपराधों की बात की जाए तो वर्ष 2019 में स्रोत दस्तावेजों को नुकसान पहुंचाने(Tempering of Source Doucuments) के 173 मामले, कम्प्यूटर संबंधी अपराध(धारा-66) में रेनसमवेयर के 1,023 मामले एवं अन्य कम्प्यूटर अपराधों के 3,444 मामले, चोरी के कम्प्यूटर संसाधन या संचार उपकरणों को बेईमानी से प्राप्त करने (धारा-66 बी) के 558 मामले, *पहचान की चोरी(धारा-66 सी) के 12,255 मामले, कम्प्यूटर संसाधनों के जरिये ठगी(धारा-66 डी) के 5,520 मामले,* निजता के विरुद्ध अपराध(धारा-66 ई) के 812 मामले, साइबर आतंकवाद(धारा-66 एफ) के 12 मामले, अश्लीलता/यौन शोषण के इलेक्ट्रानिक स्वरुप के प्रदर्शन/ प्रकाशन (धारा-67 ए) के 4,187 मामले सामने आए।[3]

इसी प्रकार वर्ष 2019 में भारतीय दंड संहिता, 1960 की विभिन्न धाराओं के अंतर्गत पंजीबद्ध किए गए कुल 13,730 साइबर अपराधों में से ऑनलाइन

2 https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%201.pdf
3 https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf

माध्यम से आत्महत्या के लिए उकसाने(धारा-305/306) के 8 मामले, *महिलाओं एवं बच्चों के विरुद्ध साइबर स्टॉकिंग/बुलिंग (धारा-354 डी) के 777 मामले,* डाटा चोरी(धारा-379 एवं 381) के 285 मामले सामने आए। वहीं *ऑनलाईन धोखाधड़ी(धारा-420 के साथ पठित धारा-465, 468 एवं 471) में क्रेडिट/डेबिट कार्ड धोखाधड़ी के 367 मामले, एटीएम धोखाधड़ी के 2,067 मामले, ऑनलाईन बैंकिंग धोखाधड़ी के 2,093 मामले, ओटीपी धोखाधड़ी के 549 मामले और अन्य ऑनलाईन धोखाधड़ी के 1,157 मामले पंजीबद्ध किए गए।* वर्ष 2019 के दौरान भारतीय दंड संहिता की धारा-420 के अंतर्गत ऑनलाइन ठगी के कुल 3393 मामले दर्ज किए गए। इतना ही नहीं इस वर्ष के दौरान जालसाजी (धारा-465, 468 एवं 471) के 512 मामले, साइबर मानहानि/मोर्फिंग (स्त्री अशिष्ट रूपण (प्रतिषेध) अधिनियम, 1986 के साथ पठित भा.द.सं. की धारा-469) के 19 मामले, नकली प्रोफाइल बनाने के 87 मामले, साइबर ब्लैकमेलिंग/धमकी (धारा-धारा-506,503 एवं 384) के 372 मामले, सोशल मीडिया पर झूठी खबर फैलाने(धारा-505) के 190 मामले और भारतीय दंड संहिता की अन्य धाराओं के तहत साइबर अपराधों के 1,849 मामले दर्ज किए गए।[4]

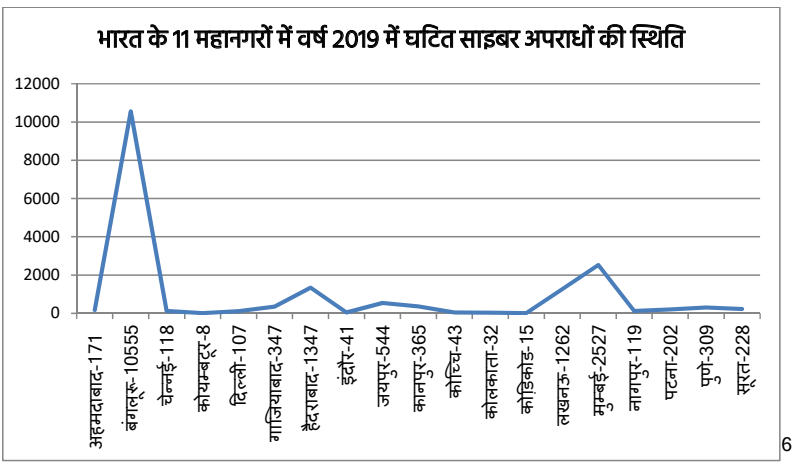
वर्ष 2019 में अन्य विशेष एवं स्थानीय कानूनों(एसएलएल) के साथ पठित सूचना प्रौद्योगिकी अधिनियम के प्रावधानों के अंतर्गत जो अपराध पंजीबद्ध किए गए, उनमें ऑनलाइन गेम्बलिंग के 22 मामले, ऑनलाइन लॉटरी के 9 मामले, कॉपीराइट अधिनियम, 1957 के अंतर्गत 34 मामले दर्ज किए गए।[5]

इन आंकड़ों से स्पष्ट होता है कि भारत में साइबर अपराध दिन-ब-दिन बढ़ते जा रहे हैं। यहां यह भी जरूरी है कि इन अपराधों के पीछे अपराधियों की मंशा और इरादों पर भी गौर किया जाए। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो की

4 https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf
5 https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf

वर्ष 2019 की कथित वार्षिक रिपोर्ट इस बारे में एक बहुत स्पष्ट तस्वीर पेश करती है। इस रिपोर्ट के मुताबिक वर्ष 2019 में घटित साइबर अपराध के मामलों में से 1,207 अपराध बदले की भावना से और 581 अपराध क्रोध की भावना से अंजाम दिए गए। वहीं 26,891 अपराध धोखाधड़ी के लिए, 1,842 अपराध जबरन वसूली के लिए, 1,874 मामले किसी की बेइज्जती करने के लिए, 1,385 अपराध शरारत के मकसद से, 2,266 अपराध यौन शोषण के लिए, 316 अपराध राजनैतिक मकसद से, 199 अपराध आतंकवादी मनसूबों से अंजाम दिए गए।

यदि हम भारत के 11 प्रमुख महानगरों में वर्ष 2019 में घटित साइबर अपराधों की ओर नजर डालें तो स्थिति कुछ इस प्रकार सामने आती है-



[6]

स्पष्ट रुप से सबसे अधिक साइबर अपराध बंगलूरू, मुम्बई, लखनऊ और हैदराबाद में घटित हो रहे हैं, हालांकि साइबर अपराधों को किस शहर, प्रदेश या देश की सीमाओं से जोड़ कर नहीं देखा जा सकता, क्योंकि सूचना-प्रौद्योगिकी की सर्वव्यापकता के चलते ये अपराध अक्सर दूर रह कर ही अंजाम दिए जाते हैं। आंकड़े ये भी बताते हैं कि सूचना प्रौद्योगिकी अधिनियम

6 https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf

के अंतर्गत पंजीबद्ध किए गए 50,518 मामलों में से 7,968 मामले और भारतीय दंड संहिता एवं अन्य विशेष स्थानीय कानूनों के अंतर्गत पंजीबद्ध किए गए 76,669 मामलों में से 11,517 मामले ऐसे भी थे जो सच्चे तो थे मगर उनमें पर्याप्त साक्ष्य मौजूद नहीं मिले या कोई सुराग ही नहीं मिल सका था।[7]

इंटरनेट के प्रयोग की दृष्टि से भारत विश्व में दूसरे स्थान पर है। जहां एक ओर वर्ल्ड वाइड वेब से परस्पर संपर्क को नए आयाम मिल रहे हैं वहीं आज का डिजिटल समाज नित्य नए खतरों की चुनौतियां भी झेल रहा है। सच कहें तो साइबर अपराधों की कोई सीमा नहीं है और ये उतनी ही तेजी से बढ़ते जा रहे है, जितनी तेजी से प्रौद्योगिकी का विकास हो रहा है। हर वर्ष दर्ज किए जाने वाले साइबर अपराधों के मामले में निरंतर बढ़ोत्तरी होती जा रही है। इनमें छोटी-छोटी ऑनलाईन धोखाधड़ियों से लेकर, लॉटरी के जरिये लूट और यौन उत्पीड़न के मामलों तक सब कुछ शामिल है। इस दौरान बैकिंग और वित्तीय क्षेत्र साइबर अपराधों से सबसे ज्यादा प्रभावित रहा है। विगत वर्ष विश्वव्यापी कोराना महामारी के चलते ज्यादातर सेवाएं ऑनलाईन हो गईं और इसके साथ ही साइबर अपराधों की संभावनाएं भी बढ़ती चली गईं। हालांकि निजी एवं सार्वजनिक क्षेत्रों ने साइबर अपराधों का दंश सबसे ज्यादा झेला है, किन्तु सरकारी महकमे भी इनसे होने वाले नुकसान ने अछूते नहीं रहे हैं।

कोविड-19 वैश्विक महामारी ने भी समूचे विश्व में साइबर अपराधियों को पनपने और फलने-फूलने का खूब अवसर प्रदान किया है। इस दौरान हुए लम्बे लॉकडॉउन में ज्यादातर जनसंख्या घर पर रह कर ही अपने कार्य का ऑनलाइन निपटान करने में जुटी थी। इतना ही नहीं लोग दिन-रात अपने आपसी संपर्क और मनो-विनोद के लिए पूरी तरह से सूचना एवं संचार प्रौद्योगिकी पर निर्भर हो गए थे। बाजार और दुकानें बंद होने की वजह से

7 https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf

ज्यादातर खरीद-फिरोख्त भी ऑनलाइन एवं डिजिटल माध्यमों से हो रही थी। वहीं शिक्षण संस्थाएं भी अपनी सभी गतिविधियां ऑनलाइन माध्यमों से चला रही थी तथा यह क्रम अब तक जारी है। ऐसे में अपराधियों को जालसाजी और धोखाधड़ी से धन कमाने के अनुकूल अवसर प्राप्त हुए। वहीं यह भी देखा गया कि हैकर्स ने इन अवसरों का जम कर लाभ उठाया तथा जालसाजी करने वाली वेबसाइटों में तेजी से वृद्धि हुई। वहीं वैश्विक महामारी से उत्पन्न आर्थिक मुश्किलों के दौर में आतंक, नफरत और वैमनस्य फैलाने वाली ताकतों ने अपने समर्थकों की संख्या बढ़ाने और उन्हें कट्टर बनाने में कोई कोर-कसर नहीं छोड़ी। ऑनलाइन माध्यमों के जरिये नशीली दवाओं आदि की तस्करी को भी खूब बढ़ावा मिला। संयुक्त राष्ट्र की ओर से जारी रिपोर्ट के अनुसार इस दौरान जालसाजी करने वाली फिशिंग वेबसाइटों में 350 प्रतिशत की वृद्धि दर्ज की गई।[8]

भारत की वित्तीय आसूचना इकाई (एफआईयू-इंडिया) ने अपनी एक हालिया रिपोर्ट में यह उल्लेख किया है कि कोविड-19 महामारी के कारण फैली उथल-पुथल नए तरह के इलेक्ट्रॉनिक एवं साइबर अपराधों को जन्म दे सकती है। यह इकाई मुख्य रूप से धन शोधन और आतंकवाद के वित्तपोषण से संबंधित संदिग्ध वित्तीय लेनदेन के बारे सूचना एकत्रीकरण, विश्लेषण और प्रसार के लिये देश के वित्तीय क्षेत्र और कानूनी कार्यान्वयन एजेंसियों के बीच की एक कड़ी के रूप में काम करती है।[9] वित्तीय आसूचना इकाई का यह विश्लेषण उस समय पूरी तरह चरितार्थ होता नजर आया जब ये समाचार मिला कि साइबर ठग लोगों को फोन करके कोरोना वैक्सीन लगवाने के लिए रजिस्ट्रेशन का झांसा दे रहे हैं और फिर रजिस्ट्रेशन के नाम पर उनसे आधार कार्ड नंबर, बैंक खाता, एटीएम कार्ड तथा क्रेडिट/डेबिट

8 https://www.patrika.com/miscellenous-world/united-nations-report-growth-in-cyber-crimes-during-covid-19-6324541/

9 https://www.tv9hindi.com/india/corona-upheaval-new-financial-cyber-crimes-may-arise-fiq-report-predicts-589203.html

कार्ड का नम्बर मांग रहे हैं। ये ठग कुछ देर बाद अपने शिकार के मोबाइल पर एक ओटीपी नम्बर भिजवाते हैं और फिर इस ओटीपी नम्बर के माध्यम से लोगों के खाते से रकम निकाल लेते हैं।[10]

इस बारे में भारत सरकार, गृह मंत्रालय द्वारा साइबर-सुरक्षा एवं जागरूकता के लिए संचालित किया जा रहा ट्विटर हैंडल "साइबर-दोस्त" बेहद सफल व कारगर सिद्ध हो रहा है। इस ट्विटर हैंडल पर जन-सामान्य को नित्य-नया रूप लेते साइबर अपराधों से बचाने के लिए आए दिन चेतावनियां जारी की जाती हैं। इसके अलावा गृह मंत्रालय ने 30 अगस्त 2019 से साइबर अपराधों ऑनलाइन शिकायत के लिए "साइबर अपराध रिपोर्टिंग पोर्टल' भी उपलब्ध कराया है। यह पोर्टल साइबर अपराध की शिकायतों की ऑनलाइन रिपोर्ट करने के लिए पीड़ितों / शिकायतकर्ताओं को सुविधा प्रदान करने के लिए भारत सरकार की एक पहल है। यह पोर्टल केवल साइबर अपराधों से संबंधित शिकायतों, विशेष रूप से महिलाओं और बच्चों के खिलाफ साइबर अपराधों के लिए है। इस पोर्टल पर दर्ज की गई शिकायतों को कानून प्रवर्तन एजेंसियों / पुलिस द्वारा शिकायतों में उपलब्ध सूचना के आधार पर निपटाया जाता है।[11] इस पोर्टल पर नागरिकों के लिए बहुत सी ज्ञानवर्द्धक जानकारियां और साइबर सुरक्षा उपाय की युक्तियां भी उपलब्ध हैं। चूँकि आज के दौर में सामान्य वार्तालाप से लेकर बैंकिग लेनदेन, कार्यालय का कामकाज, व्यवसायिक व्यवहार, खरीद-फिरोख्त सभी ऑनलाइन एवं डिजिटल माध्यमों से हो रहा है, इसलिए इन सभी ऑनलाइन एवं डिजिटल प्लेटफॉर्मों पर साइबर अपराधियों की बढ़ती करतूतों से कदापि इंकार नहीं किया जा सकता। वस्तुत: जन-जागृति ही साइबर अपराधों की रोकथाम का सबसे कारगर तरीका है। यदि देश का नागरिक साइबर अपराधों से बचने

10 https://www.amarujala.com/uttar-pradesh/jhansi/don-t-let-the-greed-of-the-corona-vaccine-make-your-bank-account-clear

11 https://cybervolunteer.mha.gov.in/Hindi/Defaulthn.aspx

लिए हर क्षण सजग रहे और अपना हर व्यवहार एवं लेनदेन सुरक्षा उपायों के साथ सुनिश्चित करे तो निश्चित रूप से साइबर अपराधों में भारी कमी लाई जा सकती है।

अध्याय 4

भारत में साईबर अपराधों की बड़ी घटनाएं : एक विश्लेषण

साइबर अपराध आज दुनिया भर में गहन चिंता का विषय बनते जा रहे हैं। भारत के संदर्भ में यदि अंतरराष्ट्रीय परिपेक्ष्य में आंकड़े तलाशे जाएं तो जो तस्वीर दिखाई देती है उसमें भारत इंटरनेट जनित अपराधियों का दंश झेल रहे विश्व के 20 सबसे ज्यादा प्रभावित देशों में तीसरे स्थान पर रहा है। यह आंकलन संयुक्त राज्य अमेरिका के फैडरल ब्यूरो ऑफ इंवेस्टीगेशन के इंटरनेट अपराध शिकायत केन्द्र(आईसी-3) की रिपोर्ट पर आधारित है।[1] इस रिपोर्ट के मुताबिक वर्ष 2019 में संयुक्त राष्ट्र में 93,796, कनाडा में 3,721 और भारत में 2,901 लोग साइबर अपराधों से ग्रसित थे। आईसी-3 की रिपोर्ट के अनुसार साइबर अपराध का सबसे मुख्य जरिया ईमेल था, जबकि टेक्स्ट मैसेज एवं फर्जी वेबसाईटों के द्वारा, अर्थात फार्मिंग(Pharming) के माध्यम से भी अपराधों को अंजाम दिया जाता रहा है। रिपोर्ट के अनुसार संयुक्त राज्य अमेरिका में सबसे ज्यादा साइबर अपराध के मामले फिशिंग और इसी प्रकार के चाल-फरेबों, व्यक्तिगत डाटा की चोरी, रोमांस-धोखाधड़ी और स्पूफिंग(Spoofing) से संबंधित थे और कुछ ऐसे ही साइबर अपराध अक्सर भारत में भी घटित होते रहते हैं। हालांकि सूचना प्रौद्योगिकी के नित्य बदलते दौर में यह स्थिति बदलती ही रहती है

इसके अलावा एक अन्य वेबसाइट www.comparitech.com पर प्रकाशित एक प्रतिष्ठित तकनीकि लेखक, निजता अधिवक्ता और वीपीएन

1 https://www.newindianexpress.com/nation/2020/feb/23/india-stands-third-among-top-20-cyber-crime-victims-says-fbi-report-2107309.html

विशेषज्ञ पॉल बिशॉफ के द्वारा 24 मार्च 2021 को लिखे गए ब्लॉग (Which countries have the worst (and best) cyber security?) में दी गई सूचनाओं और आंकड़ों की मानें तो वर्ष 2020 में किए गए आंकलन के आधार पर साइबर सुरक्षा की दृष्टि से असुरक्षित पाए गए देशों में ताजिकिस्तान सबसे पहले स्थान पर है, यानि यह देश साइबर अपराधों से सबसे ज्यादा प्रभावित है। जबकि साइबर अपराधों की दृष्टि से डेनमार्क को सबसे सुरक्षित देश बताया गया है। इस सर्वेक्षण के निष्कर्षों को प्राप्त करने के लिए निम्नलिखित 15 मानदण्ड निर्धारित किए गए थे[2]-

- मालवेयर से संक्रमित मोबाइल फोन का प्रतिशत
- मोबाइल बैंकिंग ट्रोजन के हमले से ग्रसित प्रयोगकर्ताओं का प्रतिशत
- मोबाइल रेनसमवेयर ट्रोजन के हमले से ग्रसित प्रयोगकर्ताओं का प्रतिशत
- बैंकिंग मालवेयर (नॉन-मोबाइल) के हमले से ग्रसित प्रयोगकर्ताओं का प्रतिशत
- रेनसमवेयर ट्रोजन (नॉन-मोबाइल) के हमले से ग्रसित प्रयोगकर्ताओं का प्रतिशत
- कम-से-कम एक मालवेयर(वेब-आधारित) हमले से ग्रसित कम्प्यूटरों का प्रतिशत
- कम-से-कम एक लोकल मालवेयर हमले से ग्रसित कम्प्यूटरों का प्रतिशत
- वेब स्त्रोतों से हुए हमलों से ग्रसित मोबाइल प्रयोगकर्ताओं का प्रतिशत

2 https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

- इंटरनेट ऑफ थिंग्स(आई ओ टी)/ओरिजिनेटिंग कंट्री द्वारा टेलनेट हमलों का प्रतिशत
- क्रिप्टोमाइनर्स द्वारा हमलों का प्रतिशत
- इंटरनेट ऑफ थिंग्स(आई ओ टी)/ओरिजिनेटिंग कंट्री द्वारा एसएसएच-आधारित हमलों का प्रतिशत
- ओरिजिनेटिंग कंट्री द्वारा भेजे गए सभी ईमेल स्पेम का प्रतिशत
- मेलिशियस मेलिंग द्वारा निशाना बनाए गए देशों की हिस्सेदारी का प्रतिशत
- फिशिंग द्वारा हमले से ग्रसित कम्प्यूटरों का प्रतिशत और
- साइबर हमलों के लिए सबसे ज्यादा तैयार देश कौन-कौन से है?

इस सर्वेक्षण में कुल 70 देशों के आंकड़ों को शामिल किया गया। सर्वेक्षण के अनुसार जिस देश का औसत ओवर-ऑल स्कोर सबसे ज्यादा रहा उसे साइबर अपराधों की दृष्टि से सबसे असुरक्षित देश और जिस देश का औसत ओवर-ऑल स्कोर सबसे कम रहा उसे सबसे सुरक्षित देश माना गया। इस सूची में सबसे अधिक अंक (35.54) ताजिकिस्तान के थे। इसके बाद बांग्लादेश के 34.57, चीन के 33.90, वियतनाम के 32.60, अल्जीरिया के 32.28 और भारत के 30.72 अंक थे। शेष सभी देश इस तालिका सें कम अंकों के साथ अपेक्षाकृत अधिक सुरक्षित अवस्था में पाए गए। इस तरह से साइबर अपराधों की दृष्टि से सबसे असुरक्षित देशों की फेहरिस्त में भारत का नाम छठवें स्थान पर है। इसे विपरीत दिशा में सोचा जाए तो इस सर्वेक्षण के अनुसार भारत साइबर अपराधों की दृष्टि से सुरक्षित देशों की सूची में बहुत ही नीचले स्थान यानी 70वें पायदान पर नजर आता है, जो गहरी चिंता का विषय है।

इस प्रकार साइबर अपराधों की रोकथाम के क्षेत्र में अंतरराष्ट्रीय स्तर पर भारत का स्तर कदापि संतोषप्रद नहीं है और खास तौर उन पुलिस अधिकारियों के लिए तो बिल्कुल नहीं, जो आए दिन जनता एवं देश की बहुविध संस्थाओं की शिकायतों पर साइबर अपराधों का अन्वेषण करने में अपना सर्वस्व समर्पित करते हैं। भारतीय कानून व्यवस्था साइबर अपराधों का प्रभावी रूप से प्रतिकार करती है, लेकिन फिर भी विगत वर्षों में भारत में जो बड़े साइबर अपराध घटित हुए हैं उनका उल्लेख यहां लाज़मी मालूम होता है, ताकि स्थिति हर दृष्टिकोण से स्पष्ट हो सके।

बीसवीं शताब्दी ने विज्ञान और प्रौद्योगिकी का साथ पाकर सारी दुनिया को एक वैश्विक गांव जैसा स्वरूप प्रदान कर दिया है, जहां डिजिटल तकनीकों ने वैश्विक अर्थव्यवस्था, संस्कृतियों और जनसंख्या को बहुत ही करीब से आपस में जोड़ दिया है। भारत भी इसका अपवाद नहीं रहा है और वर्ष 2020 तक यहां इंटरनेट प्रयोगकर्ताओं की संख्या लगभग 70 करोड़ तक पहुंच गई है, जिसके 2025 तक लगभग 97.4 करोड़ तक पहुंचने की संभावना है।[3] इंटरनेट प्रयोगकर्ताओं की दृष्टि से भारत चीन के बाद विश्व में दूसरे स्थान पर है।[4] वर्ल्ड-वाईड-वेब ने हमें जहां बहुत बेहतर ढंग से सम्पर्क स्थापित करने में समर्थ बनाया है, वहीं इसने साइबर अपराधों जैसे अनेक ख़तरों को भी जन्म दिया है। साइबर अपराधों के लिए सरहदें अब कोई मायने नहीं रखतीं, क्योंकि साईबर अपराधी आम इन्टरनेट प्रयोगकर्ता की तरह ही घर बैठे देश की सीमाओं के बाहर पूरे विश्व में अपने नापाक इरादों को अंजाम देने पर आमादा रहते हैं।

वर्ष 2020 में भारत एशिया महाद्वीप का दूसरा ऐसा देश रहा है, जिस पर सबसे

3 https://www.statista.com/statistics/255146/number-of-internet-users-in-india/

4 https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users

ज्यादा साइबर हमले हुए हैं और विश्व भर में घटित हुए साइबर अपराधों का 7 प्रतिशत हिस्सा भारत में घटित हुआ है। इस संबंध में आईबीएम द्वारा किए गए विश्लेषण के अनुसार कोविड-19 महामारी से उत्पन्न सामाजिक-आर्थिक परिस्थितियों से साइबर अपराधियों को बहुत लाभ मिला है और इस दौरान उन्होंने अस्पतालों, चिकित्सा एजेंसियों और दवा निर्माताओं के साथ-साथ आपूर्ति कायम रखने वाले प्रतिष्ठानों तथा आम नागरिकों को बहुत नुकसान पहुंचाया है। इतना ही नहीं साइबर अपराधियों ने इस दौरान लोक-स्वास्थ्य संबंधी डाटा का भी भरसक दुरूपयोग किया है। साइबर अपराध की हर घटना हमें यही बताती है कि आज के साइबर जगत में कोई भी प्रयोगकर्ता सुरक्षित नहीं है, क्योंकि साइबर अपराधियों के छल-कपट में आकर उसके द्वारा की गई एक भी चूक बड़े नुकसान का कारण बन जाती है।

चूँकि साइबर जगत में प्रौद्योगिकी की उन्नति के साथ अपराधों की प्रकृति में निरंतर परिवर्तन आते रहते हैं, इसलिए यह प्रासंगिक प्रतीत होता है कि भारत में विगत 5 वर्षों में घटित बड़े साइबर हमलों/अपराधों का विस्तृत विश्लेषण किया जाए, ताकि हमें साइबर अपराधों की गंभीरता एवं उनकी प्रवृत्ति का सटीक अंदाजा लग सके-

वर्ष 2016 –

1. 32 लाख डेबिट कार्ड का डाटा चोरी-

अक्टूबर 2016 में भारतीय बैंकों के डाटा में साइबर अपराधियों द्वारा सेंध लगाने का एक बड़ा मामला उजागर हुआ। इस प्रकरण में अंदाजन लगभग 32 लाख डेबिट कार्डों का डाटा चुराए जाने का अनुमान था। इस हमले में एसबीआई, एचडीएफसी, आईसीआईसीआई, यस बैंक और एक्सिस बैंक जैसे बड़े बैंकिंग प्रतिष्ठान सबसे ज्यादा प्रभावित हुए थे। बैंकों के डाटा में सेंधमारी का कई महीनों तक पता ही नहीं

चल सका था। इस साइबर हमले का खुलासा उस समय हुआ जब कुछ बैंकों ने ग्राहकों के डेबिट कार्डों के चीन और संयुक्त राज्य से किए जा रहे इस्तेमाल पर आपत्ति उठाई, जबकि उनके वास्तविक ग्राहक भारत में मौजूद थे। इस घटना के बाद भारत के इतिहास में डेबिट कार्डों के नवीनीकरण की सबसे बड़ी मुहिम छिड़ गई थी। भारत के सबसे बड़े बैंक, भारतीय स्टेट बैंक ने उस समय लगभग 6 लाख डेबिड कार्ड नए सिरे से जारी किए थे। इस बारे में किए गए लेखा परीक्षण से यह तथ्य सामने आया था कि बैंकों के डाटा में यह सेंधमारी एक मालवेयर के जरिये अंजाम दी गई थी।[5]

2. नोटबंदी, डिजिटलीकरण और साइबर हमले-

द न्यू इंडियन एक्सप्रेस समाचार पत्र में प्रकाशित एक रिपोर्ट के अनुसार 28 नवम्बर 2016 तक भारत में साइबर हमलों के प्रतिदिन औसतन रुप से 2 लाख खतरे महसूस किए जा रहे थे। नोटबंदी के बाद इन खतरों की संख्या 5 लाख तक पहुंच गई और दिसम्बर माह के पहले सप्ताह तक साइबर हमलों की कोशिशों की संख्या 6 लाख प्रतिदिन तक जा पहुंची। हालांकि इनमें से ज्यादातर कोशिशों को किसी भी बड़े नुकसान से पहले ही नाकाम कर दिया गया। लेकिन 'लीजन(Legion) नामक हैकर्स समूह ने कुछ नामचीन हस्तियों के ट्विटर एकाउंट हेक करते हुए तहलका मचा दिया और यह भी दावा किया कि भारत का बैंकिंग नेटवर्क कमजोर होने के कारण हेकिंग की जद में था। लीजन का दावा था कि वह भारत के बैंकिंग क्षेत्र को घुटनों पर ला देगा और इस खतरे से मुकाबले के लिए भारत के सूचना-संचार ढांचे एवं वित्तीय नेटवर्क में चाक-चौबंद व्यवस्थाएं

5 https://en.wikipedia.org/wiki/2016_Indian_Banks_data_breach#:~:text=2016%20Indian%20Banks%20data%20breach%20was%20reported%20in%20October%202016,were%20among%20the%20worst%20hit.

सरकार की ओर से सुनिश्चित की गईं। अधिकारिक सूत्रों के हवाले से यह कहा गया कि 22 से 26 नवम्बर 2016 के बीच भारतीय नेटवर्कों पर चीन, पाकिस्तान, सिंगापुर, संयुक्त राज्य, रूस, रोमानिया, यूक्रेन, दुबई और स्वीडन में बैठे हैकर्स ने 3,35,000 हमले किए। स्त्रोतों ने यह भी बताया कि लीजन के अलावा भी कुछ अनजाने समूह जैसे- सकफ्लाय(Suckfly), लेज़रस(Lazarus), ऑडिनेफ(Odinaff), डांटी(Danti) थे जो भारतीय नेटवर्कों पर उस समय साइबर हमले कर रहे थे, जब नोटबंदी के बाद देशवासी डिजिटल लेनदेनों पर निर्भर हो गए थे। उस समय भारत को सबसे बड़ा खतरा लीजन से था, जो भारत के 40,000 सर्वरों तक पहुंचने का दावा कर रहा था और कई वेबसाइटों एवं वित्तीय सेवाओं को क्षति पहुंचा सकता था। उस समय एंडरॉइड एवं आईओएस प्लेटफॉर्म आधारित स्मार्ट फोन डिवाइज को भी साइबर हमलावरों द्वारा बड़ी संख्या में निशाना बनाया जा रहा था। एक साइबर सुरक्षा संस्था केस्परस्काय(Kaspersky) ने मोबाइल मालवेयर के हमलों से ग्रसित देशों की सूची में भारत को सातवें स्थान पर बताते हुए यह भी कहा था कि ZeuS जैसे मोबाइल बैंकिंग ट्रोजन प्रयोगकर्ता के खातों से पैसा निकालने के लिए प्रयोग किए जाने वाले सबसे आम मालवेयर में से एक थे।[6]

वर्ष 2017-

1. बड़ी संख्या में वेबसाइटों की हैकिंग-

अप्रैल' 2017 से जनवरी' 2018 के बीच 22,000 से अधिक वेबसाइटों को हैक किया गया। इंडियन कम्प्यूटर इमरजेन्सी रेस्पोन्स टीम (CERT-in) से प्राप्त जानकारी के अनुसार 493 वेबसाइट मालवेयर

6 https://www.newindianexpress.com/nation/2016/dec/19/80000-cyber-attacks-on-december-9-and-12-after-note-ban-1550803.html

के प्रसार से ग्रसित थीं, जिनमें 114 सरकारी वेबसाइटें भी शामिल थीं। इन हमलों का मकसद संबंधित नेटवर्कों द्वारा प्रदान की जा रही सेवाओं और उनके प्रयोगकर्ताओं से जुड़ी जानकारी जुटाना था।[7]

2. यूनियन बैंक पर साइबर हमला-

जुलाई 2017 में भारत के एक बड़े राष्ट्रीयकृत बैंक, यूनियन बैंक ऑफ इंडिया पर एक बड़ा साइबर हमला हुआ। इस हमले की शुरुआत उस समय हुई जब इस बैंक के एक कर्मचारी ने एक इमेल के साथ मिले अटैचमेंट को खोल लिया। इस ईमेल अटैचमेन्ट में एक मालवेयर कोड छिपा हुआ था, जिसके जरिये हैकर्स बैंक के सिस्टम तक पहुंच गए और बैंक का डाटा चुरा लिया। यह ईमेल अटैचमेंट सेंट्रल बैंक से आया हुआ दिखाई देता था। संबंधित कर्मचारी ने इस इमेल के ब्यौरों को नजरअंदाज करते हुए इस पर भरोसा कर लिया और उसका यही भरोसा एक बड़े मालवेयर हमले की वजह बन गया। इससे हैकर्स को बैंक के डाटा में सेंध लगाने का मौका मिल गया और उन्होंने 'सोसाइटी फॉर वर्ल्डवाइड इंटरबैंक फायनेन्शियल टेलीकम्यूनिकेशन(SWIFT) के लिए यूनियन बैंक के एक्सेस कोड को चुरा लिया। इन कोडों का इस्तेमाल करके हैकर्स ने यूनियन बैंक से 170 मिलियन डॉलर्स की रकम न्यूयॉर्क स्थित सिटीग्रुप इंक. (Citigroup Inc) में ट्रांसफर कर दी।[8]

3. वॉनाक्राय (WannaCry) रैनसमवेयर-

वॉनाक्राय रैनसमवेयर एक मैलवेयर टूल था, जिसका इस्तेमाल करते हुए मई 2017 में वैश्विक रैनसमवेयर हमले को अंजाम दिया गया था।

7 https://www.testbytes.net/blog/cyber-attacks-on-india/

8 https://www.testbytes.net/blog/cyber-attacks-on-india/#:~:text=Cyber%20attack%20on%20Union%20Bank,attachment%20had%20a%20malware%20code.

रैनसम अंग्रेजी शब्द है जिसका अर्थ है- फिरौती। इस साइबर हमले के बाद संक्रमित कम्प्यूटरों ने काम करना बंद कर दिया था और उन्हें फिर से चालू करने के लिए बिटकॉइन के रूप में 300-600 डॉलर तक की फिरौती मांगी गई। ब्रिटेन की नेशनल हेल्थ सर्विस भी इस हमले से प्रभावित हुई। साइबर सुरक्षा शोधकर्ताओं के अनुसार इस दौरान बिटकॉइन मांगे जाने के 36 हज़ार मामलों का पता चला। इस साइबर हमले में विश्व भर में लगभग 2 लाख 30 हजार कम्प्यूटर प्रभावित हुए थे और इनमें भारत के भी कई हजार कम्प्यूटरों को क्षति पहुंची।[9]

वर्ष 2018-

1. सिम कार्ड को 3जी से 4जी में अपग्रेड करने को लेकर हुई धोखाधड़ी-

निसंदेह साइबर अपराधी सूचना एवं संचार प्रौद्योगिकी की हर नई करवट पर ध्यान देते हैं और उसी हिसाब से अपने मनसूबों को अंजाम देते हैं। जिस समय भारत के मोबाइल उपभोक्ता अपने मोबाइल सिम कार्डों को 3जी से 4जी में तबदील करने की जद्दोजहद में लगे थे, उसी समय साइबर अपराधियों ने इस उन्नति को अपने नापाक इरादों की कामयाबी का जरिया बना लिया। इस दौरान साइबर ठगों ने लोगों को सिम स्वेप (3जी से 4जी अपग्रेड) को लेकर लाखों रुपए का चूना लगाया। देश भर में ऐसे कई मामले दर्ज किए गए। दरअसल ये साइबर ठग मोबाइल सेवा प्रदाता कम्पनियों के कर्मचारी बन कर ग्राहकों को फोन करते थे और उन्हें 3जी से 4जी सिम स्वेप के लिए राजी करते थे। फिर वे ग्राहकों से कहते थे कि उनके मोबाइल पर नए 4जी सिम का

9 https://www.prabhatkhabar.com/tech-and-auto/wannacry-ransomware-recently-cyber-attacked-india-and-global-crime-coronavirus-lockdown-online-transaction

20 डिजिट का नम्बर आएगा, जिसे उन्हें सेवा प्रदाता की हेल्पलाइन नम्बर पर भेजना होगा। जैसे ही उपभोक्ता ऐसा करता था उसकी 3जी सिम बंद हो जाती थी और 4जी सिम एक्टीवेट हो जाती थी, जो पहले से ही साइबर ठग के पास होती थी। पुलिस अधिकारियों का मानना था कि इस तरह की सिम-स्वेप धोखाधड़ी को अंजाम देने के लिए साइबर अपराधी ग्राहकों की 4जी सिम ऑनलाइन माध्यम से मंगवा लेते थे या ग्राहकों से जालसाजी करके प्राप्त किए गए दस्तावेज सेवा प्रदाता के केंद्रों पर दिखा कर वहां से ग्राहक के नाम की 4जी सिम प्राप्त कर लेते थे। जब 4जी सिम एक्टीवेट हो जाती थी तो ये साइबर ठग इसका इस्तेमाल उपभोक्ता के बैंक खाते का ओटीपी प्राप्त करने के लिए करते थे। जांच एजेंसियों का ये भी मानना था कि ये साइबर ठग बैंक के कर्मचारियों से पहले ग्राहकों के बैंक खातों एवं डेबिट कार्ड आदि के विवरण और सेल फोन नम्बर जान लेते थे और फिर इनमें से अधिकांश नम्बरों पर कॉल करके 3जी मोबाइल उपभोक्ताओं को अपने चंगुल में फंसा लेते थे।[10]

2. **वर्ष 2018 में पुणे के कॉसमॉस को-**आपरेटिव बैंक में साइबर सेंधमारी की एक बड़ी घटना हुई, जिसमें बैंक के 94 करोड़ 42 लाख रूप साइबर अपराधियों ने निकाल लिए। जांच के दौरान इस मामले के तार हाँगकाँग और उत्तर कोरिया से जुड़े पाए गए। इन साइबर अपराधियों ने बैंक के सर्वर को हैक कर लिया था और उसके बाद 29 अलग-अलग देशों से बैंक की रकम पर हाथ साफ कर दिखाया था। भारत के अनुरोध पर संयुक्त राष्ट्र की ओर से गठित जांच पैनल ने इस मामले में उत्तर कोरिया का हाथ होना बताया था। इस मामले में बैंक सुरक्षा प्रणाली भी सवालों के घेरे में आ गई थी। जांच के दौरान यह

10 https://www.deccanchronicle.com/nation/in-other-news/100618/sim-swap-fraud-back-in-new-form.html

भी पता चला कि इस साइबर सेंधमारी के आरोपी चैन्नई की एक अन्य बैंक से की गई 33 करोड़ की लूट में भी शामिल थे। जांच में यह तथ्य भी सामने आया कि कंगाली के दौर से बचने के लिए उत्तर कोरिया दूसरे देशों की बैंकों में हैकिंग को अंजाम दे रहा था।[11]

वर्ष 2019-

1. चीनी हैकर्स ने लगाई 131 करोड़ की चपत-

जनवरी 2019 में चीनी हैकर्स ने फिशिंग ईमेल का इस्तेमाल करते हुए इटली की एक कंपनी की भारतीय शाखा से 131 करोड़ रुपए उड़ा लिए। हैकर्स ने फिशिंग ईमेल भेज कर संवेदनशील जानकारियां, यूजरनेम, पासवर्ड आदि की जानकारी लेकर इस बड़े साइबर हमले को अंजाम दिया। रिपोर्ट के अनुसार चीन के एक हैकर्स समूह ने इटली की कंपनी Tecnimont S.p.A. की भारतीय इकाई से 1.86 करोड़ डॉलर यानी करीब 130 करोड़ रुपये उड़ा लिए थे। यह भारत में अब तक का सबसे बड़ा साइबर हमला था। इन हैकर्स ने कंपनी के स्थानीय प्रबंधकों को एक नई कंपनी खरीदने के लिए राजी कर लिया था और इसके लिए उनसे धन भी ले लिया था। इसके बाद हैकर्स ने इस कम्पनी की भारतीय इकाई Tecnimont प्राइवेट लिमिटेड को एक ईमेल भेजी और इस ईमेल के साथ ही एक बड़ी साइबर धोखाधड़ी का खेल शुरू हो गया। दरअसल हैकर्स द्वारा भेजा गया यह ईमेल Tecnimont S.p.A. के सीईओ पिएरोबर्टो फोलगिएरो के ईमेल अकाउंट से भेजा गया प्रतीत होता था। इसके बाद हैकर्स ने चीन में नई कंपनी के अधिग्रहण से संबंधित निजी जानकारी जुटाने के लिए एक कॉन्फ्रेंस कॉल की, जिसमें ग्रुप के सीईओ, स्विट्जरलैंड

11 https://www.patrika.com/mumbai-news/cosmos-bank-loot-fir-lodged-against-hong-kong-based-company-5953674/

के जाने-माने वकील और कंपनी के अन्य वरिष्ठ कर्मियों समेत कई लोग शामिल हुए। तत्पश्चात हैकर्स ने कंपनी की भारतीय इकाई के प्रमुख को इस बात पर राजी कर लिया कि कुछ समस्याओं के कारण नई कम्पनी के अधिग्रहण हेतु इटली से धन मंगाना संभव न होने के कारण भारतीय इकाई से धन मुहैया करा दिया जाए। तदनुसार कंपनी की भारतीय इकाई के प्रमुख ने एक सप्ताह के भीतर तीन बार में 56 लाख डॉलर, 94 लाख डॉलर और 36 लाख डॉलर तथाकथित हैकर्स को ट्रांसफर कर दिए। यह धन भारत से हांगकांग के कई बैंकों में भेजा गया। खास बात ये थी कि ये रकम बहुत जल्द ही उन खातों से निकाल ली गई और इसके बाद जब हैकर्स ने और अधिक धन की मांग की तो उनका पर्दाफाश हो गया।[12]

2. देश के उद्योगपति और संसद सदस्य हुए साइबर अपराधियों का शिकार-

दरअसल साइबर अपराधी किसी को भी नहीं छोड़ते। उनका मकसद सिर्फ यही होता है कि साइबर अपराधों को अंजाम देते हुए अधिक से अधिक नुकसान पहुंचाया जाए। अप्रैल 2019 के दौरान एक शातिर साइबर अपराधी ने प्रसिद्ध उद्योगपति अनिल अंबानी के पुत्र आकाश अंबानी के नाम से एक ट्विटर एकाउंट बना लिया और देखते ही देखते उसके साथ कई फॉलोवर्स जुड़ गए। वहीं इस फर्जी ट्विटर एकाउंट के जरिये शातिर साइबर ठग ने एक लड़की से 8 लाख रूपए की धोखाधड़ी भी कर डाली। एक ओर सनसनीखेज मामले में एक संसद सदस्य के वेतन खाते से बिना किसी अलर्ट मैसेज के लगभग 16 लाख रुप की राशि गायब होने की शिकायत दर्ज की गई। दरअसल

12 https://www.amarujala.com/channels/downloads?tm_source=text_share

उनके बैंक खाते को हैक करने के बाद दिसम्बर 2018 के बाद से कई अनधिकृत लेनदेनों को अंजाम दिया गया और 15 लाख 62 हजार रुपए की रकम निकाल ली गई।[13]

वर्ष 2020-

1. चीन के साइबर हमले से मुम्बई अंधकारमय-

12 अक्टूबर 2020 को मुम्बई में पॉवर ग्रिड के फेल होने के कारण बड़े पैमाने पर बिजली गुल रही। न्यूयॉर्क टाइम्स का दावा था कि यह घटना चीन के एक साइबर अटैक का परिणाम थी। जिस समय पूर्वी लद्दाख में नियंत्रण रेखा पर भारत और चीन के सैनिकों के बीच तनातनी चल रही थी, उसी समय एक मालवेयर के जरिये भारत की एक बहुत ही महत्वपूर्ण पॉवरग्रिड प्रणाली को निशाना बनाया। न्युयॉर्क टाइम्स की रिपोर्ट में कहा गया कि चीन से जुड़े एक ग्रुप RedEcho ने भारत के प्रमुख पावर ग्रिडों पर मालवेयर प्लांट किए थे। राज्य सरकार द्वारा इस बारे में की गई जांच के बाद न्यूयॉर्क टाइम्स की रिपोर्ट को सही बताते हुए यह स्पष्ट किया गया कि जांच में बिजली की मांग और पूर्ति के आधार पर लोड डिस्पैच को संतुलित करने वाली SCADA इकाई में चीन, ब्रिटेन और आठ अन्य जगहों से फायरवॉल ब्रेक कर ट्रोजन हॉर्स मालवेयर के प्रवेश का खुलासा हुआ था। रिपोर्ट के अनुसार इस दौरान 8 जीबी डाटा चोरी किया गया था।[14]

हालांकि मार्च 2021 में आई एक और रिपोर्ट के मुताबिक चीन के

13 https://www.aajtak.in/crime/cyber-crime/story/year-ender-2019-top-5-cyber-crime-cases-online-fraud-social-media-police-akash-ambani-994380-2019-12-23

14 https://www.aajtak.in/crime/cyber-crime/story/maharashtra-cyber-attack-mumbai-power-grid-energy-minister-nitin-raut-said-will-not-use-chinese-equipment-anymore-1216585-2021-03-04

हैकर्स ने तेलंगाना की बिजली सप्लाई को रोकने की भी कोशिश की, लेकिन इंडियन कम्प्यूटर इमरजेंसी रिस्पॉन्स टीम(CERT-in) के द्वारा भेजे गए एक अलर्ट आधार पर इस अटैक को विफल कर दिया गया।

2. बिग-बास्केट 'ग्रॉसरी ई-कॉमर्स प्लेटफॉर्म से 2 करोड़ प्रयोगकर्ताओं का निजी डाटा चोरी-

नवम्बर 2020 में अपने तरह के एक अनूठे साइबर हमले में बिग-बास्केट नामक 'ग्रॉसरी ई-कॉमर्स प्लेटफॉर्म' से लगभग 15 जीबी का डाटा चोरी कर लिया गया, जिसमें 2 करोड़ प्रयोगकर्ताओं की निजी जानकारियां शामिल थीं। इस चोरी का खुलासा साइबर इंटेलीजेंस कंपनी Cyble के रुटीन वेब मॉनीटरिंग के दौरान हुआ। इस कम्पनी के अनुसार हैकर्स ने इस डाटा को 40,000 डॉलर (लगभग 29.5 लाख रुपए) में बेचने के लिए डार्क वेबसाइट पर डाल दिया था। (डार्क वेबसाइट का तात्पर्य उन वेबसाइटों से है जो गूगल एवं बिंग जैसे सर्च इंजन के दायरे में नहीं आती हैं।) Cyble की रिपोर्ट के बताती है कि इस डाटा में प्रयोगकर्ताओं का नाम, ई-मेल, पासवर्ड, मोबाइल नंबर, पता, जन्मतिथि एवं स्थान आदि की जानकारी के साथ लॉग-इन का IP एड्रेस भी दिया गया था।[15]

कोराना संक्रमण काल में भारत साइबर अपराधों के मामले में एशिया में दूसरे स्थान पर-

वर्ष 2020 भारत में वैश्विक महामारी का महासंकट लेकर आया। महामारी का खतरा इतना भयावह था कि मार्च 2020 के अंत से देश को लम्बे समय तक लॉकडॉउन का सामना करना पड़ा। इस दौरान आवश्यक सेवाओं को

15 https://www.bhaskar.com/tech-auto/news/data-breach-at-bigbasket-personal-info-of-over-2-crore-users-up-on-dark-web-for-sale-127898200.html

छोड़ कर सभी सरकारी, सार्वजनिक और निजी क्षेत्र के प्रतिष्ठान बहुत ही सीमिति संख्या में कर्मचारियों के साथ काम करते रहे। अधिकांश प्रतिष्ठानों ने अपने कर्मचारियों को 'वर्क फ्रॉम होम' की नई संकल्पना पर काम करने के निर्देश दिए। लम्बी लॉकडॉउन अवधि के दौरान देश मानो थम सा गया था, लेकिन इस दौरान कम्प्यूटर, मोबाइल और इंटरनेट तथा सूचना एवं संचार प्रौद्योगिकी से जुड़ी अन्य सुविधाओं ने क्रांतिकारी परिवर्तन ला दिए और जीवन के लगभग सभी कार्यकलाप इन माध्यमों से चलने लगे। जहां एक ओर सरकारी व निजी प्रतिष्ठानों का कामकाज इन माध्यमों से चलता रहा, वहीं शिक्षा व्यवस्था भी ऑनलाईन माध्यमों पर निर्भर हो गई। घर बैठे लोग अपने मनोरंजन के लिए भी इन्हीं सुविधाओं पर पूरी तरह से निर्भर हो गए। वैश्विक महामारी के इस दौर ने तो मानो साइबर अपराधियों के फलने-फूलने के लिए असीमित अवसर खोल दिए। वाकई साइबर सुरक्षा की दृष्टि से भी यह वैश्विक महामारी एक अभिशाप सिद्ध हो रही है।

इंडियन कम्प्यूटर इमरजेन्सी रिस्पोन्स टी(CERT-in) के हवाले से लोकसभा को ये बताया गया कि वर्ष 2020 में अगस्त माह तक ही साइबर सुरक्षा से जुड़ी 6,96,938 घटनाएं घटित हो चुकी थीं। जबकि 2015 में केवल 49455, 2016 में 50362, 2017 में 53117, 2018 में 208456 और 2019 में 394499 घटनाएं घटित हुई थी।[16] साफ तौर पर कहा जा सकता है कि वर्ष 2020 में साइबर अपराधों की घटनाएं 2019 की घटनाओं के दोगुने से भी कहीं ज्यादा थीं। वहीं आईबीएम द्वारा किए गए आंकलन के अनुसार वर्ष 2020 में हुए साइबर हमलों की दृष्टि से भारत एशिया महाद्वीप में जापान के बाद दूसरे स्थान पर रहा।[17] इस दौरान भारत में वित्तीय और बीमा क्षेत्र में सबसे ज्यादा साइबर हमले हुए, हालांकि व्यवसायिक सेवाओं और अन्य

16 https://zeenews.india.com/hindi/india/7-lakh-cyber-attacks-in-the-country-in-last-8-months-central-government-report/752109

17 https://www.indiatv.in/paisa/business-india-report-second-highest-syber-attack-in-asia-pacific-in-2020-says-ibm-

क्षेत्रों पर भी इनका असर साफ तौर पर देखने को मिला। इन हमलों में 40 प्रतिशत हमले रेनसमवेयर के जरिये अंजाम दिए गए।

कोरानाकाल में भारत में बढ़ते साइबर हमलों के बारे में राष्ट्रीय साइबर सुरक्षा समन्वयक, ले.जनरल राजेश पंत ने कहा कि साइबर हमले दिन-ब-दिन बढ़ते ही जा रहे हैं और वर्ष 2020 में भारत हर दिन लगभग 375 साइबर हमलों का सामना करता रहा है।[18]

वर्तमान परिवेश साइबर अपराध के नित्य नए प्रकरण सामने आ रहे हैं। इस बारे में आम जनता के और सुरक्षा कर्मियों के लिए यह निसंदेह रुप से हितकर है कि वे प्रिंट और इलेक्ट्रॉनिक मीडिया में आ रही साइबर अपराधों और साइबर हमलों से जुड़ी खबरों पर ध्यानपूर्वक गौर करते रहें, ताकि वे सूचना व संचार प्रौद्योगिकी के विकासक्रम के साथ हर दिन नया रुप धारण करते साइबर अपराधों की गंभीरता को समझ सकें और उनसे हर क्षण सर्तक रह सकें। साइबर अपराधों के संदर्भ में भी यह युक्ति बेहद सार्थक सिद्ध होती है कि 'सावधानी ही बचाव है।'

18 https://inc42.com/buzz/india-hit-by-375-cyberattacks-daily-in-2020-says-pant/

अध्याय 5

भारत का सामाजिक-आर्थिक परिवेश और साइबर अपराध

साइबर अपराध किसी देश के सामाजिक-आर्थिक परिवेश से सीधा ताल्लुक रखते हैं। सूचना एवं संचार प्रौद्योगिकी से बदलते माहौल का असर आज मनुष्य के जीवन के हर पहलू पर बहुत ही आसानी से देखा जा सकता है। इस संबंध में आगे विश्लेषण के लिए सामाजिक और आर्थिक परिवेश को अलग-अलग पायदानों पर रखते हुए उनमें साइबर अपराधों के अस्तित्व एवं विस्तार पर व्यापक चर्चा की गई है।

सामाजिक परिवेश और साइबर अपराध-

भारत एक विशाल देश है, जिसमें विभिन्न धर्म-सम्प्रदाय और संस्कृति के लोग निवास करते हैं। यहां क्षेत्रीय और भाषायी विविधताएं भी प्रचुरता से पाई जाती हैं। इनके बावजूद भी यह देश विविधता में एकता की अनूठी मिसाल पेश करता है। भारत का सामाजिक परिवेश अपने समृद्ध इतिहास, महान परम्पराओं और गौरवशाली संस्कृति के लिए विश्व भर में जाना जाता है। अतीत में अनेकों विभूतियों ने भारत के सामाजिक परिवेश पर अपनी अमिट छाप छोड़ी है, जो मार्यादा, न्याय, सत्य, अहिंसा, सदाचार, परोपकार, प्रेम, सद्भावना और त्याग की प्रतिमूर्ति रहे हैं। साहस, पराक्रम और पुरुषार्थ सदैव भारतीय संस्कृति को अनूठी पहचान दिलाते रहे हैं। इतने के बाद भी विश्व की दूसरी सभ्यताओं की भांति भारतीय सभ्यता एवं समाज में बुराईयां तथा आपराधिक प्रवृत्तियां सिर उठाती रही हैं और भारतीय समाज अपनी पूरे सामर्थ्य के साथ इनका प्रतिकार करता आया है।

आधुनिक युग की यदि बात की जाए तो यह सूचना व संचार प्रौद्योगिकी का युग है। इस युग में चहुंओर फैले कम्प्यूटरीकरण, इंटरनेट सेवाओं, सर्वत्र सुलभ दृश्य-श्रव्य प्रचार माध्यमों, डिजिटलीकृत सुविधाओं, इन्सटेन्ट ग्राहक सेवा पद्धतियों और स्वचलित मशीनी प्रणालियों ने सब कुछ इतना आसान और त्वरित बना दिया है कि मनुष्य को पलक छपकते ही मनचाही जानकारी एवं सुविधा मुहैया हो जाती है। नई प्रौद्योगिकी के आने से सुविधाओं और सहुलियतों का जो अम्बार लगा है, वो तो सर्वविदित है, लेकिन सूचना व संचार प्रौद्योगिकी के इस युग में हमारे सामाजिक परिवेश में क्रांतिकारी परिवर्तन आए हैं, जिन्हें कदापि नज़रअंदाज नहीं किया जा सकता।

वस्तुत: इस युग में बुराईयों और आपराधिक प्रवृत्ति ने भी नए माहौल का फायदा उठाते हुए भयावह रूप धारण कर लिया है। दरअसल साइबर अपराध नए ज़माने के अपराध माने जाते हैं, जिनमें सूचना एवं संचार प्रौद्योगिकी का खुल कर इस्तेमाल होता है, लेकिन इन अपराधों की जमीन समाज के बीच ही तैयार होती है। जहां एक ओर अपराध का दंश झेलने वाले समाज के बीच से ही होते हैं, वहीं दूसरी अपराधी भी समाज के बीच से ही निकल कर आते हैं और यहीं आश्रय भी पाते हैं। हालांकि साइबर अपराधों की अवधारणा ऐसी है कि साइबर अपराधी समाज के बाहर दूर किसी ओर देश में बैठ कर भी अपनी करतूतों को अंजाम दे जाते हैं, फिर भी उन्हें अपने मकसद में कामयाब होने के लिए समर्थनीय परिस्थितियां इसी सामाजिक पृष्ठभूमि पर मिलती हैं। नए दौर में वो कौन-कौन से कारक हैं, जो समाज में अपराधों के लिए ऐसी जमीन तैयार करते हैं, जिस पर साइबर अपराधी जन्म लेते हैं और सूचना प्रौद्योगिकी का हाथ थाम कर आगे बढ़ते चले जाते हैं या जहां उन्हें अपने अपराध के लिए शिकार बड़ी आसानी से मिल जाते हैं? आईए इन कारकों पर ज़रा गौर फरमाएं-

1. सामाजिक सरोकार की कमी-

सूचना एवं संचार प्रौद्योगिकी से बदलते परिवेश का प्रभाव मानव जीवन के हर क्षेत्र में देखा जा सकता है और समाज इससे अछूता नहीं रह सकता। समाज मनुष्यों से बना है और बदलते परिवेश का असर सबसे पहले मनुष्य के मन-मस्तिष्क और व्यवहार पर ही पड़ता है। सोशल मीडिया ने जहां एक ओर मानवीय संवेदनाओं को कम्प्यूटरीकृत बना कर रख दिया है, वहीं मानव समाज में परस्पर सम्पर्क की संस्कृति और ललक में काफी गिरावट देखी गई है। हालांकि 2020 की शुरुआत से दुनिया पर मंडरा रहे कोविड-19 के खतरे ने दूरियां बनाए रखने को ही नई संस्कृति बना दिया है, लेकिन यदि वैश्विक महामारी के इस दौर के पहले और बाद के समय की बात की जाए तो यह आंकलन बिल्कुल सटीक बैठता है। जहां पहले आपसी संपर्क और संबंध भावनाओं से ओतप्रोत होते थे, वहीं अब ये सब एक डिजिटलाईज्ड औपचारिकता सा लगता है। सामाजिक उत्सवों और समारोहों का दायरा सिकुड़ता जा रहा है। समाज में एक दूसरे के प्रति सहनशीलता घटती जा रही है और सामाजिक मूल्यों तथा परस्पर व्यवहार-कुशलता में साफ तौर पर गिरावट देखी गई है। यही कारण है कि कुछेक ग्रामीण क्षेत्रों को छोड़ कर मुनष्य प्राय: स्वयं तक ही सीमित हो कर रह गया है और अब उसे अपने आसपास के लागों और घटनाओं से उतना सरोकार नहीं रहा है।

बड़े शहरों में अक्सर ऐसी घटनाएं देखी गई हैं कि किसी खतरे या हमले के समय पड़ोसी अपने आप में इतने मशगुल थे कि उन्हें अपने ही पड़ोस में घटित हो रही घटना या वारदात की आहट सुनाई नहीं दी या अगर उन्हें ऐसा आभास भी हुआ तो उन्होंने जानबूझ कर जरूरतमंद व्यक्ति की कोई सहायता नहीं की तथा बाद में पुलिस व अदालत

के सामने गवाही देने से भी कतराते रहे। यहां कहने को तो हम सब चौबीसों घंटे सीसीटीवी कैमरों की निगरानी में हैं, लेकिन वास्तव में पहले जितने सुरक्षित नहीं हैं, क्योंकि अब हमारे आसपास के माहौल में आपसी सरोकार और व्यवहार-कुशलता का अभाव है। मानव की मानव से यही दूरियां सामाजिक संगठन को कमजोर बना देती हैं और आपराधिक प्रवृत्ति पनपने के लिए अनुकूल माहौल मिल जाता है और जब बात साइबर अपराधों की हो तो इस प्रकार के सरोकारविहीन सामाजिक परिवेश में इन्हें अंजाम देना और भी आसान हो जाता है, क्योंकि एक तो इन अपराधों में सूचना व संचार प्रौद्योगिकी सदैव साथ रहती है, दूसरे अपराधी की पहचान भी कई मामलों में मुश्किल हो जाती है।

2. सूचना एवं संचार प्रौद्योगिकी से भावनाएं घटीं और उतावलापन बढ़ा है-

हम में से बहुत से लोग इस बात से इत्तेफाक रखते हैं कि पहले के ज़माने में लोगों की भावनाएं आपसी मेलजोल के चलते ही एक दूसरे से बहुत हद तक जुड़ी रहती थी। जब भी कोई किसी से महीनों बाद मिलता था या बिछड़ता था तो आंखें भर आती थीं। भावनाओं का उबाल ऐसा होता था कि मुंह से शब्द नहीं निकलते थे। लोगों का आपसी प्रेम व सरोकार इतना घनिष्ठ था कि चिट्ठियां कभी खुशी तो कभी गम के आंसुओं का कारण बन जाती थीं। तार के आते ही लोगों के दिलों की धड़कने बढ़ जाती थी और वे किसी अनिष्ट की चिंता से घबरा जाते थे। वहीं आज मोबाईल पर वीडियो कॉल करके एक दूसरे से रुबरु होने के अनेकानेक एप्लीकेशन्स उपलब्ध हैं। मोबाईल फोन पर बात करना इतना सस्ता और आसान हो गया कि कोई भी, कभी भी, किसी से भी बात कर लेता है। यानि सबको सबका पल-पल

का हाल मालूम होता रहता है। फिर भी यह अंचभित कर देने वाली बात है कि एक दूसरे से बात और प्रत्यक्ष सम्पर्क की ऐसी सुविधाएं होने के बाद भी हम बैचेन और असुरक्षित महसूस करते हैं तथा अब पहले से कहीं ज्यादा बेसब्र और उतावले हो चले हैं। यदि किसी से बात करनी हो और इत्तेफाकन नेटवर्क चला जाए, या मोबाइल फोन डिस्चार्ज हो जाए या फिर उसका फोन न लगे तो इससे उत्पन्न होने वाला उतावलापन और मानसिक तनाव चेहरे पर साफ नज़र आने लगता है। और ऐसा सब कुछ समाज या परिवार में मानव के आपसी रिश्तों के बीच ही नहीं हो रहा है, बल्कि यही हाल व्यवसाय, नौकरी और बाजार के लेनदेन में भी साफ दिखाई देता है। सूचना और संचार प्रौद्योगिकी ने लोगों में एक नई आदत या कहें फ़ितरत कायम की है और वो यह है कि सबको सब कुछ तुरंत या बिना किसी विलम्ब के चाहिए, जैसे कि मशीन से निकलने वाली इंस्टेन्ट कॉफी।

यदि यह सब आम आदमी के साथ घटित हुआ है तो आधुनिक समाज में विद्यमान आपराधिक प्रवृत्तियां भी इस उतावलेपन से अछूती नहीं रही हैं। पहले यह देखा जाता था कि कोई अपराधी किसी अपराध को अंजाम देने के लिए सही मौके की ताक में रहता था, जबकि आज के युग के साइबर अपराधी इतने सक्षम हैं कि वे मनचाहे अपराध को किसी न किसी तरीके से, कहीं भी और किसी भी स्थान से अंजाम दे सकते हैं। आख़िर क्यूं न हो, उन्हें भी तो सूचना व संचार प्रौद्योगिकी के इस युग में इंसटेन्ट नतीजे चाहिए।

ऐसे माहौल में समाज में बहुत जल्दी पैसा व नाम कमा कर आगे बढ़ने वाले की होड़ सी लगी है। ऐसे समय में वो मानसिक प्रवृत्तियां जो गलत रास्ते से पैसा कमाने से परहेज नहीं करतीं, दबे पांव अपराधों के गलियारों की ओर मुड़ जाती हैं। उन्हें अपराध जगत में सबसे आसान

डगर साइबर अपराधों की डगर लगती है, क्योंकि गुमनामी और झूठी पहचान इसके सबसे बड़े फायदे हैं तथा इन अपराधों को अंजाम देने के लिए मोबाईल फोन, कम्प्यूटर, लेपटॉप एवं इंटरनेट जैसी सुविधाएं चहुंओर आसानी से उपलब्ध हैं।

अब एक ओर तो नौजवानों में बढ़ता उतावलापन उन्हें बहुत जल्दी और बहुत कुछ पा लेने को प्रेरित करता है, वहीं सामाजिक सरोकार ख़त्म होने से समाज में कोई भी व्यक्ति दूसरे व्यक्ति के आचार-व्यवहार या काम-धंधे में दख़ल नहीं देता। बस ऐसे ही सूचना प्रौद्योगिकी के दौर में साइबर अपराध करने वालों को मनचाहे संसाधन और बेरोक-टोक काम करने का माहौल मिल जाता है और तो और किसी को यह भी पता नहीं चलता कि आख़िर वो आजीविका कमाने के लिए कर क्या रहा है, क्योंकि फोन, लेपटॉप, इंटरनेट का इस्तेमाल तो वह किसी नौकरी-पेशा इंसान की तरह ही कर रहा होता है, इसमें नई या अजीब सी दिखने वाली कोई बात नहीं होती, खास तौर पर तब तक जब तक कि साइबर अपराधी का पर्दाफाश न हो जाए। समाज के ऐसे अनुकूल माहौल में साइबर अपराधी खूब पनप रहे हैं, जहां उनके काम पर कोई अंकुश नहीं होता और अंकुश हो भी कैसे, क्योंकि जब तक किसी शिकायत पर अन्वेषण करते हुए पुलिस या कानून उस अपराधी तक पहुंचते हैं, वह न जाने कितने लोगों को चूना लगा चुका होता है।

3. परिवारों में संस्कारों की सीख अब उतनी पुख़्ता नहीं रही-

मनुष्य की पहली पाठशाला उसके परिवार को माना जाता है। परिवार में रह कर ही कोई बच्चा अपनी संस्कृति और परम्पराओं को सीखता है। आज के दौर में संयुक्त परिवार टूट कर एकल परिवारों में बदलते जा रहे हैं, यानि आम तौर पर बच्चे को केवल माता-पिता और कभी-

कभी उनमें से भी किसी एक की परवरिश में ही पलना-बढ़ना होता है। इसके पीछे सामाजिक और व्यवसायिक दोनों प्रकार के कारण हैं, लेकिन इस परिपाटी से जो हानि समाज को हो रही है उसका व्यापक असर नई पीढ़ियों पर साफ तौर पर दिखाई देने लगा है। अकेले माता-पिता और कभी-कभी उनमें से भी केवल किसी एक के साथ रह कर बच्चे इंसानियत के बुनियादी सबक सीख ही नहीं पाते। ऐसा इसीलिए होता है कि आज के युग में अव्वल तो माता-पिता अपनी व्यवस्तताओं से बच्चों के लिए समय नहीं निकाल पाते और घर लौटने पर जब बच्चों से मेल-मिलाप व वार्तालाप का समय होता है तो वह बचा-खुचा समय भी कभी उनके जरूरी कामों तो कभी सोशल मीडिया के मेल-मिलापों के कारण मोबाईल फोन या लेपटॉप की भेंट चढ़ जाता है। ऐसे में घर में बुजुर्गों का मौजूद न होना बच्चों के जीवन को मानसिक आधार पर वो क्षति पहुंचाता है, जिससे वे जीवन भर जूझते रहते हैं। संस्कारों की कमी इंसान में परिपक्वता नहीं आने देती और नई प्रौद्योगिकी से जन्मे इस उथल-पुथल के माहौल में इंसानी सब्र दूर-दूर तक दिखाई नहीं देता। ऐसे में नई पीढ़ियों को अच्छे बुरे की पहचान सिखाने और गलत रास्तों पर जाने से रोकने के लिए अव्वल तो कोई रहनुमा होता नहीं है और यदि कभी माता-पिता उन्हें रोकने का प्रयास भी करें तो बच्चे उनकी बात सुनने का राज़ी नहीं होते क्योंकि बचपन से ही माता-पिता का प्रभाव उन पर उतना कारगार नहीं होता। उच्च मध्यम वर्गीय एवं सम्पन्न् परिवारों के पढ़े-लिखे ऐसे ही बच्चे जो युवावस्था तक संस्कारों की कमी के चलते अपने भीतर एक जिम्मेदार नागरिक की मानसिकता विकसित नहीं कर पाते, ज़रा सा गलत साथ या संगत मिलने पर साइबर अपराधों की सहज लगने वाली डगर पर चल निकलते हैं और समाज को अपने चातुर्य से लूटना शुरु कर देते हैं।

वहीं यदि निम्न मध्यम वर्गीय परिवारों या गरीब तबकों की बात की जाए तो वहां भी स्थिति एक नहीं तो दूसरी वजह से खराब और इससे मिलती-जुलती ही दिखाई देती है। इन तबकों में संस्कारों के अलावा शिक्षा का आभाव भी आग में घी के समान काम करता है। यहां भी जीविकोपार्जन की कठिनाईयों के चलते माता-पिता बच्चों की परवरिश पर पर्याप्त ध्यान नहीं दे पाते। वहीं बच्चे समाज में अपने से उच्च वर्गों की बराबरी करने की होड़ में सब कुछ बहुत जल्दी हासिल करने की कोशिशों में लग जाते हैं, और अत्यधिक उतावलापन उन्हें भी अपराधों या साइबर अपराधों की राह पर ढकेल देता है।

सूचना एवं संचार प्रौद्योगिकी की जन-जन तक पहुंच की पराकाष्ठा ये है कि यह न सिर्फ समाज के धनाड्य, सम्पन्न और मध्यम वर्गों तक आ चुकी है, बल्कि अशिक्षित और आर्थिक रूप से कमजोर वर्ग भी इससे अछूते नहीं हैं। अत्याधुनिक सुविधाओं का उपयोग और विलासिता की ललक विशेष तौर से कमजोर वर्ग के लोगों तथा बेरोजगार युवाओं को अपने सपने सच करने के लिए धैर्य खोकर किसी भी हद तक जाने पर विवश कर देती है और वे अपराध की डगर पर चल पड़ते हैं।

आर्थिक परिवेश या अर्थ-व्यवस्था और साइबर अपराध :

वो व्यवस्था जो आज विश्व के हर देश के विकास में केन्द्रीय भूमिका निभाती है, अर्थ-व्यवस्था ही है। अर्थ-व्यवस्था की उत्पत्ति और विकास मानव सभ्यता के विकासक्रम से जुड़ा हुआ है। जिस देश की अर्थ-व्यवस्था जितनी ज्यादा मजबूत होती है, सांस्कृतिक, सामाजिक, वैज्ञानिक और सामरिक दृष्टि से उसका स्थान उतना ही ऊंचा होता है। वस्तुत: अर्थ-व्यवस्था अनेक छोटी-छोटी प्रणालियों का एक समूह है, जिसमें नागरिकों के आपसी लेनदेन से लेकर, बाजार के सौदे, उद्योग-धंधे, व्यवसाय, व्यापार, बैंकिंग, कर-व्यवस्था, राजस्व का सदुपयोग, सरकारी लेनदेन, विदेशी विनिमय और आयात-निर्यात

तथा विदेशी-व्यापार तक सभी गतिविधियां शामिल होती हैं। अर्थ-व्यवस्था की मजबूती के लिए इन सभी गतिविधियों का पारदर्शी एवं नियमित होना परमावश्यक है। इसी आवश्यकता के मद्देनज़र समूचे विश्व में अर्थ-जगत के कार्यकलापों को नियंत्रित करने के लिए विभिन्न कानून बनाए गए हैं। अर्थव्यवस्था मानव-समाज का अभिन्न हिस्सा है और इसी लिए समाज की भांति अपराध जगत पर इसका भी समान रूप से प्रभाव पड़ता है। साइबर अपराधों की यदि बात की जाए तो ये अर्थव्यवस्था की खामियों से प्रेरित भी होते हैं और अर्थ-व्यवस्था पर दुष्प्रभाव भी डालते हैं। अर्थव्यवस्था के दृष्टिकोण से देखा जाए तो निम्नलिखित कारक बढ़ते साइबर अपराधों का आधार बनते नजर आते हैं-

1. कोई भी व्यक्ति जन्म-जात अपराधी नहीं होता-

वस्तुत: व्यक्ति की पूर्व व वर्तमान परिस्थितियां ही उसे अपराध की ओर ले जाती हैं। जब भी किसी क्षेत्र में आम आदमी अपराधिक् गतिविधियों में संलिप्त होता है तो समाज में विकृति आने लगती है। जब किसी व्यक्ति की मूलभूत आवश्यकताएं अर्थात रोटी कपड़ा और मकान, संघर्ष के बाद भी पूरी नहीं होतीं और उसमें संयम व धैर्य की कमी होती है तो वह अपराध की ओर उन्मुख होने लगता है। अपनी भूख मिटाने ले लिए वह अपराधियों से भी हाथ मिला सकता है और अपनी जरूरतों की पूर्ति के लिए वह अनुत्पादक कार्यों में जैसे तस्करी, गैर कानूनी व्यापार, चोरी डकैती, हेरा-फेरी इत्यादि में संलिप्त होकर अपराधी भी बन सकता है। सूचना एवं संचार प्रौद्योगिकी के इस दौर में अपराधी बनने के लिए उसे पुराने जमाने की तरह जोखिम उठाकर ज्यादा मशक्कत करने की जरूरत भी नहीं पड़ती और वह बिना किसी की मदद लिए आधुनिक परिवेश से प्रभावित होकर अकेले ही साइबर अपराधों को अंजाम देने निकल पड़ता है, जहां उसकी मदद करने

अपराधियों झुंड इकट्ठा रहता है।

2. आधुनिकता की होड़ : गांवों से पलायन के बाद शहरों में जीवनयापन की कठिनाईयां-

अक्सर देखा गया है कि अल्प-शिक्षित या अशिक्षित ग्रामीण युवा आधुनिकता की होड़ और रोजगार पाने की ललक में गांवों से शहरों की ओर पलायन कर जाते हैं। शहरों में अक्सर उन्हें मेहनत, मजदूरी या उद्योग धंधों में कामगारों का रोजगार जैसे-तैसे मिल पाता है और उन्हें अक्सर गंदी बस्तियों या झुग्गियों जैसे स्थानों पर ढ़ेरों परेशानियों के बीच जीवनयापन एवं परिवार का भरण-पोषण करना पड़ता है। ऐसे में शहरों की तेज रफ्तार जिंदगी और आधुनिक सुविधाओं की लालसा कभी-कभी उन्हें अपराध जगत की ओर धकेल देती है। खासतौर किशोरवय और नवयुवक बहुत जल्द धन कमाने की लालसा और गुमनामी के मकसद से साइबर अपराधों की राह पकड़ लेते हैं।

हालांकि यह भी देखा गया है कि साइबर अपराधी अब शहरों का रूख किए बिना गांवों से ही साइबर ठगी या फिशिंग जैसे अपराधों को अंजाम देने लगे हैं। झारखण्ड का जामताड़ा ऐसे साइबर अपराधियों का गढ़ रहा है। हाल ही में राजस्थान के मेवात क्षेत्र के 150 गांवों में 8000 साइबर ठगों के गोरखधंधे का पर्दाफाश एक अखबार ने अपनी रिपोर्ट में किया है। ये साइबर ठग रोजाना लगभग 2.4 करोड़ रूपए देश की जनता से लूट रहे हैं। ये साइबर ठग इतने शातिर हैं कि पांच मिनट में ही आधार कार्ड या पेन कार्ड की हू-ब-हू कॉपी तैयार कर देते हैं। इन ठगों ने झोपड़ियों में अपने कॉल सेंटर बना रखे हैं, ठीक उसी तर्ज पर जैसे जामताड़ा के साइबर ठग पेड़ पर चढ़ कर फर्जी फिशिंग कॉल किया करते थे। साइबर अपराधियों का राजस्थान में इतना बड़ा नया ठिकाना इस तरफ साफ इशारा कर रहा है कि पथ-

भ्रष्ट युवा भारत में कई जामताड़ा बना सकते हैं, जो पुलिस एवं सुरक्षा एजेंसियों के लिए निश्चित रुप से नई चुनौतियों का कारण बनेंगे।[1]

3. गरीबी, मंहगाई और बेरोज़गारी-

अपराध जगत की बात हो और इसमें गरीबी, मंहगाई तथा बेरोज़गारी का जिक्र न आए, तो बात पूरी ही नहीं होती। दरअसल, गरीबी, मंहगाई और बेराज़गारी अर्थ-व्यवस्था को किसी न किसी हद तक परिभाषित करते हैं। भारत की आजादी के बाद से ही गरीबी, मंहगाई और बेरोज़गारी लगभग हर सामाजिक व राजनैतिक आंदोलन के सबसे महत्वपूर्ण मुद्दों में शामिल रही हैं, लेकिन इनका उन्मूलन अब तक नहीं हो पाया है। बेशक ये तीनों अपराध जगत के फलने-फूलने में अहम व सक्रिय भूमिका निभाती हैं, लेकिन अपराधों की रोकथाम की दृष्टि से इनके उन्मूलन की दिशा में उठाए गए कदम अपर्याप्त ही नजर आते हैं। गरीबी और बेरोजगारी से त्रस्त लोग अक्सर अपनी जरूरतों की पूर्ति के लिए अपराध का रास्ता अपना लेते हैं और शिक्षित युवाओं की यदि बात की जाए तो उनके साइबर अपराध जगत में कदम रखने की संभावनाएं सबसे अधिक प्रतीत होती हैं।

4. समाज में आर्थिक विषमता-

आर्थिक विषमता का सीधा अर्थ आय की विषमता से है। वस्तुत: किसी भी समाज या अर्थव्यवस्था में लोगों की कमाई कभी भी एक समान नहीं हो सकती। सबको अपनी-अपनी मानसिक क्षमताओं, योग्यता, काबिलियत और हुनर के अनुसार ही धन की प्राप्ति होती है और यह परिपाटी प्राचीन मानव सभ्यता से ही चली आ रही है। लेकिन, वर्तमान समय में, खास तौर पर भारत जैसे विकासशील देश

1 Dainik Bhaskar, 11 April 2021. https://epaper.bhaskar.com/bhopal/120/11042021/mpcg/18/

में, आमदनी की विषमताएं अपने चरम तक आ पहुंची हैं, जिसके दुष्प्रभाव देश के विकास एवं समाज पर साफ तौर से दिखाई देने लगे हैं। सच कहें तो देश में आर्थिक विषमताओं के अनेकों कारण हैं, जो इस पुस्तक की विषय वस्तु से परे हैं, किन्तु यह निष्कर्ष कदापि नकारने योग्य नहीं है कि आर्थिक विषमताएं अपराधों का बड़ा कारण बनती हैं और साइबर अपराधों को इनसे निसंदेह प्रोत्साहन मिलता है।

उपरोक्त तथ्यों से स्पष्ट है कि साइबर अपराध देश की सामाजिक-आर्थिक पृष्ठभूमि पर ही उगते, पनपते और फलते-फूलते हैं। वहीं साइबर जगत में अनेक अपराध देश के बाहर मौजूद अपराधियों द्वारा भी अंजाम दिए जाते हैं। साइबर अपराधों के अन्वेषण का सम्पूर्ण दायित्व देश की पुलिस-व्यवस्था एवं सुरक्षा एजेंसियों पर है। निसंदेह देश की समस्त जांच एजेंसियां अपराधों के अन्वेषण में समर्पित होकर कार्य करती हैं, लेकिन यदि साइबर अपराधों को उनके उदगम पर ही रोकना है तो निश्चित रूप से देश की जनता को साइबर अपराधों के प्रति पूरी तरह से जागरुक एवं शिक्षित बनाना होगा, ताकि वे सूचना एवं संचार प्रौद्योगिकी से लाभान्वित होते हुए वह साइबर अपराधियों की साजिशों का शिकार न बने। इस दिशा में न केवल पुलिस एवं सुरक्षा एजेंसियों बल्कि हर सरकारी, सार्वजनिक एवं निजी क्षेत्र के प्रतिष्ठानों को भी एक सुनियोजित कार्य-प्रणाली के तहत अपनी सहभागिता निभानी होगी, साइबर अपराधों को प्रोत्साहित करने वाली परिस्थितियों का समूल निराकरण करना होगा और जन-जन में **साइबर-समझ** विकसित करनी होगी, तभी बढ़ते साइबर अपराधों पर प्रभावी ढंग से अंकुश लगाया जा सकेगा।

अध्याय 6

भारत में साइबर अपराध संबंधी कानून

परिवर्तन सदैव अपने साथ नई चुनौतियां लेकर आते हैं। मानव सभ्यता के साथ-साथ न केवल समाज विकसित हुआ है, बल्कि समाज में विद्यमान अपराधों को भी पनपने और विकसित होने का भरपूर अवसर मिलता रहा है। प्रौद्योगिकी ने अपराधों के नए स्वरूप 'साइबर अपराधों' को जन्म दिया है, जो प्रत्येक देश की कानून-व्यवस्था के लिए बड़ी चुनौती साबित हो रहे हैं। ऐसे में पुलिस और सुरक्षा एजेंसियों के लिए न केवल साइबर अपराधियों की धरपकड़ और उन्हें कानून से सजा दिलाना अपने आप में एक बड़ी चुनौती है, बल्कि पुलिस और सुरक्षा एजेसिंयां ऐसे अभिनव प्रयासों में भी जुटी हैं, जिनसे साइबर अपराधों की रोकथाम उनके उदगम स्थान पर ही की जा सके।

इस अध्याय में उन नियम-कानूनों पर विस्तार से चर्चा की जाएंगी, जिनके तहत साइबर अपराधों पर कार्यवाही करने और दण्ड के प्रावधान हैं। भारत में साइबर अपराधों पर मुख्यतया निम्नलिखित अधिनियमों, नियमों/ संहिताओं के तहत कार्रवाई की जाती है-

- सूचना प्रौद्योगिकी अधिनियम,2000
  (The Information Technology Act 2000)
- सूचना प्रौद्योगिकी(संशोधन) अधिनियम, 2008
  (The Information Technology(Ammendment) Act 2008)
- सूचना प्रौद्योगिकी (भारतीय कम्प्यूटर आपातकाल प्रतिक्रिया दल

और कार्य एवं कर्तव्य निर्वहन के तौर तरीके) नियम 2013 (The Information Technology(Indian Computer Emergency Response Team and manner of performing function and duties) Rules 2013)

- भारतीय दण्ड संहिता, 1860 (The Indian Penal Code, 1860)
- भारतीय साक्ष्य अधिनियम, 1872 (The Indian Evidence Act, 1862)
- कॉपीराइट अधिनियम, 1957 (The Copyright Act, 1957)
- लैंगिक अपराधों से बालकों का संरक्षण अधिनियम, 2012 (Protection of Children from Sexual Offences (POCSO) Act, 2012.)
- सरकारी गोपनीयता अधिनियम, 1923 (THE OFFICIAL SECRETS ACT, 1923)
- कम्पनी अधिनियम, 1956 (The Companies Act, 1956)
- कम्पनी अधिनियम, 2013 (The Companies Act, 2013)
- भारतीय रिजर्व बैंक अधिनियम 1934 (The Reserve Bank of India Act, 1934)
- बैंकर्स बुक एविडेन्स एक्ट 1891 (Bankers' Book Evidence Act, 1891)

सामान्यत: हम यह कह सकते हैं कि साइबर अपराध ऐसे गैरकानूनी कृत्य हैं, जिनमें कम्प्यूटर का इस्तेमाल कभी एक हथियार के रूप में किया जाता है तो कभी किसी कम्पयूटर को निशाना बनाया जाता है। अर्थात दोनों ही तरफ

से ऐसे कृत्यों में कम्प्यूटर और सूचना व संचार प्रौद्योगिकी की भागीदारी बनी रहती है। साइबर अपराधों में पारम्परिक अपराधों की गतिविधियां, जैसे- चोरी, धोखाधड़ी, जालसाजी, मानहानि और उत्पात तो शामिल होते ही हैं, इनके अलावा सूचना व संचार प्रौद्योगिकी का दुरुपयोग करते हुए अंजाम दिए जाने वाले कई अन्य किस्म के अपराध भी शामिल होते हैं, जो अंतत: भारतीय दंड संहिता के प्रावधानों के अंतर्गत दण्डनीय करार दिए जाते हैं। वस्तुत: कम्प्यूटरों और सूचना व संचार प्रौद्योगिकी के दुरुपयोग ने कई प्रकार के नए अपराधों को जन्म दिया है, जिन के विरुद्ध सूचना प्रौद्योगिकी अधिनियम 2000 के प्रावधानों के अंतर्गत कारवाई की जाती है। वस्तुत: हम साइबर अपराधों को दो श्रेणियों में बांट सकते हैं-

1) ऐसे अपराध जिनमें किसी कम्प्यूटर/स्मार्ट फोन या डिवाइज को निशाना बनाया जाता है।
(हैकिंग/ वायरस या कम्प्यूटर वॉर्म का हमला/ डोस अटैक इत्यादि)

2) ऐसे अपराध जिनमें कम्प्यूटर को एक हथियार के रूप में इस्तेमाल किया जाता है।
(साइबर अपराध, बौद्धिक संपदा अधिकारों का हनन, डेबिट/क्रेडिट कार्ड की धोखाधड़ी/ इलेक्ट्रॉनिक फण्ड ट्रांसफर संबंधी धोखाधड़ी और अश्लीलता फैलाना आदि)

अब सवाल यह उठता है कि आख़िर भारत में साइबर कानूनों की आवश्यकता क्यों है? और उनका महत्व क्या है?

निसंदेह जब इंटरनेट का अविष्कार किया गया था तो इसके जनक रॉबर्ट ई.कॉन और विन्ट सर्फ ने शायद कभी यह सोचा भी नहीं था कि इंटरनेट एक ऐसी सर्वव्यापी क्रांति में तबदील हो जाएगा, जिसे आपराधिक गतिविधियों में भी इस्तेमाल किया जा सकेगा और इसके प्रयोग को नियंत्रित करने के

लिए नियम-कानून बनाने पड़ेंगे। निसंदेह आज साइबर जगत में अनेकों चिंताजनक बदलाव देखने को मिल रहे हैं। दरअसल इंटरनेट के इस्तेमाल में गुमनामी का फायदा मिलता है और इसके सहारा लेकर अपराधी दंड से डरे बिना अनेक प्रकार के अपराधों को अंजाम दे सकते है। यही तो वो कारण है कि कम्प्यूटर तथा सूचना व संचार प्रौद्योगिकी के प्रयोग की जानकारी रखने वाले शातिर दिमाग लोग इंटरनेट की इस खूबी का पूरा-पूरा फायदा उठा रहे हैं और साइबर जगत में धड़ल्ले से नित्य-नए अपराधों को अंजाम दे रहे हैं। ऐसे में निसंदेह भारत में सुस्पष्ट और परिमार्जित साइबर कानूनों की सख्त आवश्यकता महसूस की जाती रही है। रही बात इन साइबर कानूनों के महत्व की, तो यह इनकी जरूरत के आधार पर स्वयं ही सिद्ध है। फिर भी, उल्लेखनीय है कि साइबर कानून अपने आप में बहुत अधिक महत्व रखते हैं, क्योंकि ये इंटरनेट, वर्ल्ड-वाइड-वेब और साइबर जगत में घटित होने वाली लेनदेनों और गतिविधियों के हर पहलू से सीधा ताल्लुक रखते हैं। हालांकि किसी को भी पहली नजर में यह महसूस हो सकता है कि साइबर कानूनों का क्षेत्र पूरी तरह से तकनीकी क्षेत्र है और इनका साइबर जगत की ज्यादातर गतिविधियों पर कोई प्रभाव नहीं होगा। लेकिन सच यह है कि साइबर जगत में रोजाना नए-नए किस्म के अपराध घटित हो रहे हैं, जो निसंदेह कम्पयूटरीकृत व्यवस्थाओं और सूचना व संचार प्रौद्योगिकी से सीधा संबंध रखते हैं। अत: यदि साइबर कानून व्यापक एवं सारगर्भित रूप से तैयार किए जाते हैं तो इनसे साइबर जगत पर निसंदेह प्रभावी नियंत्रण कायम होगा। इसका एक सबसे बड़ा मूल कारण यह है कि मनुष्य का हर कृत्य या तो कानूनी है या गैरकानूनी और साइबर जगत में भी इस अवधारणा को कदापि नकारा नहीं जा सकता। उदाहरणार्थ किसी को आत्महत्या के लिए उकसाना एक दण्डनीय अपराध है। फिर चाहे वह व्यक्तिगत वार्तालाप के जरिये हो, फोन कॉल के जरिये हो या इंटरनेट के माध्यम से भेज गए इन्सटेन्ट मैसेज के जरिये, अपराध तो हर दृष्टि से अपराध है। इसीलिए सुस्पष्ट साइबर कानूनों

का आज के युग में जो महत्व है, वह शायद विद्यमान नियम-कानूनों से कहीं ज्यादा है, क्योंकि साइबर जगत में अपराधों की असीमित संभावनाए और किस्में साफ तौर पर नजर आती हैं, जिनका अंदाजा लगाना भी मुश्किल प्रतीत होता है। इसकी वजह यह है कि जैसे-जैसे कम्प्यूटर, इंटरनेट और सूचना व संचार प्रौद्योगिकी उन्नत हो रही है, साइबर जगत में अपराधों की संख्या, किस्में और गंभीरता बढ़ती ही जा रही है। अतएव वर्तमान परिवेश में साइबर कानून हर देश के लिए बहुत अधिक महत्वपूर्ण हैं।

कैसे हुई साइबर कानूनों की शुरूआत?

आज की दुनिया में सूचनाओं के इलेक्ट्रॉनिक तथा अन्य संचार माध्यमों से आदान-प्रदान के जरिये बड़ी संख्या में अन्तरराष्ट्रीय स्तर पर व्यापारिक लेनदेन किए जा रहे हैं, जिन्हें इलेक्ट्रॉनिक कॉमर्स या ई-कॉमर्स के नाम से जाना जाता है। यह सर्वविदित है कि कम्प्यूटर तथा सूचना व संचार प्रौद्योगिकी ने पारम्परिक पत्र-व्यवहार और लेखांकन की कागजी प्रकियाओं का एक त्वरित व उत्तम विकल्प प्रस्तुत किया था और साथ ही साथ सूचनाओं के संग्रहण की असीमित सुविधाएं भी उपलब्ध कराई थीं। इसके फलस्वरुप 'अंतरराष्ट्रीय व्यापार कानून पर गठित संयुक्त राष्ट्र आयोग (UNCITRAL)' ने वर्ष 1997 में 'ई-कॉमर्स पर आदर्श कानून (Model Law on Electronic Commerce-MLEC)' के जरिये यह अनिवार्य कर दिया था कि सभी सदस्य देशों द्वारा अंतरराष्ट्रीय स्तर पर स्वीकृत ऐसे नियम बनाए जाएं जो ई-कॉमर्स की संभावनाओं को बढ़ावा देने और वैधानिक गतिरोधों का उन्मूलन करने में कारगर हों। इस संकल्प ने अंतरराष्ट्रीय व्यापार में इलेक्ट्रॉनिक माध्यमों से सूचनाओं के आदान-प्रदान को कागजी-सम्प्रेषण के समकक्ष मान्यता प्रदान की और इस प्रकार कागज-रहित सम्प्रेषण को बढ़ावा दिया, साथ ही सभी देशों से इसे मानने की अपील की।

भारत में साइबर अपराध संबंधी कानून

सूचना प्रौद्योगिकी अधिनियम, 2000

भारत ने 17 अक्टूबर 2000 को सूचना प्रौद्योगिकी अधिनियम, 2000[1] लागू कर दिया, जिसके आमुख पर ही इस अधिनियम के उद्देश्यों का उल्लेख द्रष्टव्य है-

सूचना प्रौद्योगिकी अधिनियम, 2000

(2000 का अधिनियम संख्यांक 21)

[9 जून, 2000]

इलैक्ट्रानिक डाटा के आदान-प्रदान द्वारा और इलैक्ट्रानिक संसूचना के अन्य साधनों द्वारा, जिन्हें सामान्यतया "इलैक्ट्रानिक वाणिज्य" कहा जाता है और जिनमें संसूचना और सूचना के भंडारण के कागज-आधारित तरीकों के अनुकल्पों का उपयोग अंतर्वलित है, किए गए संव्यवहारों को विधिक मान्यता देने, सरकारी अभिकरणों में दस्तावेजों को इलैक्ट्रानिक रूप से फाइल करना सुकर बनाने और भारतीय दंड संहिता, भारतीय साक्ष्य अधिनियम, 1872, बैंककार बही साक्ष्य अधिनियम, 1891 और भारतीय रिजर्व बैंक अधिनियम, 1934 का और संशोधन करने तथा उससे संबंधित या उसके आनुषंगिक विषयों का उपबंध करने के लिए अधिनियम

सूचना प्रौद्योगिकी अधिनियम, 2000 को इलेक्ट्रोनिक लेन-देन को प्रोत्साहित करने, ई-कॉमर्स और ई-ट्रांजेक्शन के लिए कानूनी मान्यता प्रदान करने, ई-शासन को बढ़ावा देने, कम्प्यूटर आधारित अपराधों को रोकने तथा सुरक्षा संबंधी कार्य प्रणाली और प्रक्रियाएं सुनिश्चित करने के लिए अमल में लाया गया है। वस्तुत: इस अधिनियम के द्वारा भारत में सूचनाओं के इलेक्ट्रॉनिक आदान-प्रदान यानी ई-कॉमर्स को मान्यता प्रदान की गई, कागज-रहित सम्प्रेषण यानि ईमेल को विधिक मान्यता प्रदान की गई, सरकारी दफ्तरों में दस्तावेजों के इलेक्ट्रानिक स्वरुप को स्वीकार्य घोषित किया गया और भारतीय दंड संहिता, भारतीय साक्ष्य अधिनियम-1872, बैंककार बही साक्ष्य

1 https://legislative.gov.in/sites/default/files/H200021.pdf

अधिनियम-1891 और भारतीय रिजर्व बैंक अधिनियम-1934 में आवश्यक संशोधन किए गए। सूचना प्रौद्योगिकी अधिनियम न केवल इलेक्ट्रॉनिक डाटा इंटरचेंज और अन्य इलेक्ट्रॉनिक माध्यमों से किए लेनदेनों को न्यायिक वैधता और संरक्षण प्रदान करता है, बल्कि इसमें ऐसे प्रावधान भी समाहित हैं जो इलेक्ट्रॉनिक डाटा, सूचना अथवा रिकॉर्ड की सुरक्षा का प्रबंध करते हैं और कम्प्यूटर पद्धतियों के अनधिकृत व गैरकानूनी प्रयोग का निषेध करते हैं।

सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का अधिनियम संख्यांक 21) के लागू होने के बाद, 15 दिसंबर, 2006 को सूचना प्रौद्योगिकी (संशोधन) विधेयक-2006 लोकसभा में पेश किया गया और 23 दिसंबर, 2008 को संसद के दोनों सदनों ने इसे पारित कर दिया। इसके बाद 5 फरवरी, 2009 को सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 को राष्ट्रपति ने अपनी मंजूरी दे दी और इसे भारत के राजपत्र में अधिसूचित कर दिया गया। तदनुसार इस अधिनियम के अंतर्गत निम्नलिखित अपराधों के लिए दण्ड का प्रावधान रखा गया है-

1. कम्प्यूटर साधन कोड से छेड़छाड़ - धारा-65

2. संचार माध्यमों द्वारा आक्रामक संदेश भेजना – धारा-66 क
   (इस धारा को उच्चतम न्यायालय ने वर्ष 2015 में श्रेया सिंघल और अन्य की जनहित याचिका को स्वीकार करते हुए असंवैधानिक करार दिया और इसे निरस्त कर दिया।[2] हाल ही में उच्चतम न्यायालय ने 'पीपुल्स यूनियन फॉर सिविल लिबरटीज़(पीयूसीएल) द्वारा दायर एक याचिका पर विचार करते हुए इस बात पर आश्चर्य जताया कि 2015 में उक्त अधिनियम की धारा-66क को निरस्त कर दिए जाने

2 https://www.patrika.com/miscellenous-india/sc-to-deliver-verdict-on-66a-of-it-act-1012835/

के बावजूद भी, सुरक्षा एजेंसियों/पुलिस द्वारा इस धारा के अंतर्गत अपराध पंजीबद्ध किए जा रहे हैं, जिस उच्चतम न्यायालय ने गंभीरता से लिया है।[3]*)*

3. चुराए गए कम्प्यूटर संसाधन या संचार उपकरण को बइमानी से प्राप्त करना–धारा-66 ख

4. पहचान की चोरी -धारा 66 ग

5. कम्प्यूटर संसाधनों का इस्तेमाल करके किसी और के नाम से छल करना-धारा 66 घ

6. निजता का अतिक्रमण-धारा 66 ङ

7. साइबर आतंकवाद -धारा 66 च

8. अश्लील सामग्री का इलेक्ट्रॉनिक रुप में प्रकाशन या परेषण करना-धारा 67

9. कामुकता व्यक्त करने वाले कार्य आदि वाली सामग्री का इलेक्ट्रानिक रूप से प्रकाशन-धारा 67 क

10. कामुकता व्यक्त करने वाले कार्य आदि में बालकों को चित्रित करने वाली सामग्री का इलेक्ट्रानिक रूप से प्रकाशन या परेषण – धारा 67 ख

11. मध्यवर्ती संस्थाओं(Intermediaries)द्वारा सूचना का परिरक्षण और प्रतिधारण–धारा 67 ग

12. धारा 70 का उल्लंघन करते हुए किसी संरक्षित कम्प्यूटर प्रणाली तक पहुंच प्राप्त करना या पहुंच प्राप्त करने का प्रयास करना – धारा 70(3)

3 https://www.thehindu.com/news/national/shocked-that-section-66a-is-still-being-used-sc-seeks-centres-response/article25931913.

13. दुर्व्यपदेशन के लिए शास्ति(Penalty for Misrepresentation) -धारा 71

14. गोपनीयता एवं एकांतता/निजता भंग करने के लिए शास्ति – धारा 72

15. विधिपूर्ण संविदा भंग करते हुए सूचना का प्रकटन – धारा 72 क

16. डिजिटल सिग्नेचर संबंधी प्रावधान – धारा 73

17. कपटपूर्ण प्रयोजन के लिए प्रकाशन – धारा 74

18. अधिनियम का भारत से बाहर किए गए अपराधों और उल्लंघनों पर लागू होना–धारा 75

19. अधिहरण (Confiscation) – धारा 76

20. प्रतिकर शास्ति या अधिहरण का अन्य दंड में हस्तक्षेप न करना – धारा 77

21. अपराधों का शमन (Compounding of offences) – धारा 77 क

22. तीन वर्ष के कारावास वाले अपराधों का जमानती होना – धारा 77 ख (तीन वर्ष और उससे अधिक के कारावास से दंडनीय अपराध संज्ञेय होंगे, जबकि तीन वर्ष तक के कारावास से दंडनीय अपराध जमानती होंगे।)

23. अपराधों का अन्वेषण करने की शक्ति – धारा 78
(कोई ऐसा अधिकारी, जो निरीक्षक की पंक्ति से नीचे का न हो, इस अधिनियम के अधीन किसी अपराध का अन्वेषण कर सकेगा।)

भारतीय दंड संहिता, 1860-

साइबर अपराधों पर भारतीय दंड संहिता की निम्नलिखित धाराएं लागू होती हैं और इनके लिए दंड के प्रावधानों को सुदृढ़ बनाती हैं-

धारा-268 : लोक-बाधा या संकट उत्पन्न करना(पब्लिक न्यूसेन्स)।

धारा-292 : अश्लील पुस्तकों आदि का विक्रय।

धारा-293 : तरुण व्यक्तियों को अश्लील वस्तुओं का विक्रय।

धारा-294 : अश्लील कार्य और गीत।

धारा-378 एवं 379 : चोरी एवं चोरी के लिए दंड।

धारा-383 : जबरन वसूली।

धारा-405 : आपराधिक न्यासभंग।

धारा-406 : आपराधिक न्यासभंग के लिए दंड।

धारा-417 : छल के लिए दंड।

धारा-419 : प्रतिरूपण द्वारा छल के लिए दंड।

धारा-420 : छल और संपत्ति परिदत्त करने के लिए बेईमानी से उत्प्रेरित करना।

धारा-463 : कूटरचना।

धारा-465 : कूटरचना के लिए दंड।

धारा-499 : मानहानि।

धारा-500 : मानहानि के लिए दंड।

धारा-506 : आपराधिक अभित्रास के लिए दंड।

धारा-509 : शब्द, अंगविक्षेप या कार्य जो किसी स्त्री की लज्जा का अनादर करने के आशय से हो।

कॉपी राईट अधिनियम 1957

इस अधिनियम की निम्नलिखित धाराएं साइबर अपराधों के मामले में लागू होती है-

धारा-14 : प्रतिलिप्याधिकार (कॉपी राईट) का अर्थ।

धारा-63ख : कम्प्यूटर प्रोग्राम की अतिलंघनकारी प्रति के जानबूझ कर किए गए उपयोग का अपराध।

अन्य अधिनियम एवं नियम

साइबर अपराधों की प्रकृति के अनुसार इन पर कुछ अन्य अधिनियमों में दिए गए संगत प्रावधान भी लागू होते हैं, जिनकी एक उदाहरणात्मक सूची इस अध्याय के आरंभ में दी गई है। यहां यह भी उल्लेखनीय है कि यदि कुछ विशिष्ट प्रकार के अपराधों को कम्प्यूटर तथा सूचना एवं संचार प्रौद्योगिकी से जुड़े संसाधनों के माध्यम से अंजाम दिया जाता है तो उन मामलों में ऐसे अपराधों जड़े बुनियादी नियम-कानूनों के प्रावधान आकृष्ट होते हैं। उदाहरण के तौर पर यदि नशीले पदार्थों की तस्करी को साइबर माध्यमों से अंजाम दिया जाता है तो ऐसे प्रकरणों में 'स्वापक औषधि और मन:प्रभावी पदार्थ अधिनियम, 1985 (Narcotic Drugs And Psychotropic Substances Act, 1985 (NDPS Act)) के प्रावधान लागू होंगे। इसी प्रकार यदि हथियारों की तस्करी को साइबर माध्यमों से अंजाम दिया जाता है तो इन मामलों में आयुध अधिनियम, 1959 (Arms Act, 1959) के प्रावधान लागू होंगे।

वर्ष 2000 में सूचना प्रौद्योगिकी अधिनियम लागू करने के बाद भारत सरकार ने देश में साइबर अपराधों पर अंकुश लगाने के लिए निम्नलिखत नियम जारी किए हैं-

1. इस अधिनियम की धारा 79 में कुछ मामलों में मध्यवर्ती संस्थाओं को देनदारी से छूट के बारे में विस्तार से बताया गया है। धारा 79(2) (ग) में जिक्र किया गया है कि मध्यवर्ती संस्थाओं को अपने कर्तव्यों का पालन करते हुए उचित तत्परता बरतनी चाहिए और साथ ही केन्द्र सरकार द्वारा प्रस्तावित अन्य दिशा-निर्देशों का भी पालन करना चाहिए। तदनुसार सूचना प्रौद्योगिकी(मध्यवर्ती संस्थाओं के लिए दिशा-निर्देश) नियम 2011, माह-अप्रैल 2011 में अधिसूचित किए गए।

2. भारत में 2 जुलाई 2013 को 'राष्ट्रीय साइबर सुरक्षा नीति-2013' लागू की गई।

3. 16 जनवरी 2014 को सूचना प्रौद्योगिकी अधिनियम-2000 की धारा 70-क की उप धारा 3 के साथ पठित धारा 87 की उप धारा 2 के खण्ड (यग) के द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए 'सूचना प्रौद्योगिकी (राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र और कार्यों तथा दायित्वों के निर्वहन की रीति) नियम, 2013 लागू किए गए।[4] इन नियमों के अंतर्गत सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70 के प्रावधानों के अधीन 'राष्ट्र की महत्वपूर्ण सूचना अवसंरचना के संरक्षण के उद्देश्य से' एक नोडल एजेंसी के रुप में राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र की स्थापना की गई।

4. वर्ष 2018 के आते-आते अपराधियों और राष्ट्र विरोधी तत्वों ने सोशल मीडिया का दुरुपयोग करते हुए विधि-प्रवर्तन एजेंसियों के लिए नई चुनौतियां खड़ी कर दीं। इसमें आतंकवादियों की भर्ती के लिए प्रलोभन, अश्लील सामग्री का प्रसार, वैमनस्य फैलाना, हिंसा भड़काना, झूठी खबरें फैलाना आदि शामिल था। वॉट्सऐप और अन्य सोशल मीडिया साइटों के जरिये फैलाई गई अफवाहों और झूठी खबरों

4 https://www.meity.gov.in/writereaddata/files/gazette_11-01-2014.pdf

के कारण 2018 में भीड़ द्वारा घेरकर मारने की अनेक घटनाएं सामने आने लगीं थीं। ऐसे में वर्ष 2018 में संसद के मानसून सत्र में "सोशल मीडिया प्लेटफॉर्म के दुरुपयोग और झूठी खबरों के प्रसार" पर राज्य सभा में ध्यानाकर्षण प्रस्ताव लाने को मंजूरी दी गई। इलेक्ट्रोनिकी और सूचना प्रौद्योगिकी मंत्री ने 26 जुलाई, 2018 को इस बारे में विस्तार से जवाब दिया, जिसमें उन्होंने अन्य बातों के अलावा सदन को यह भी बताया कि सरकार कानूनी ढांचे को मजबूत करने और इस कानून के अंतर्गत सोशल मीडिया प्लेटफॉर्मों को जवाबदेह बनाने के लिए कृतसंकल्पित है। साथ ही मंत्रालय ने 2011 में अधिसूचित नियमों के स्थान पर सूचना प्रौद्योगिकी (मध्यवर्ती संस्थानों के लिए दिशा-निर्देश) नियम, 2018 का मसौदा तैयार कर लिया । इस समय विचार-विमर्श की प्रक्रिया चल रही है। विभिन्न मंत्रालयों के बीच और उसके बाद सोशल मीडिया प्लेटफॉर्म/फेसबुक, गूगल, ट्विटर, याहू, वॉट्सऐप और मध्यवर्ती संस्थानों का प्रतिनिधित्व करने वाली अन्य एसोसिएशनों जैसे आईएएमएआई, सीओएआई और आईएसपीएआई जैसे संदेश देने वाले प्लेटफॉर्मों सहित अन्य साझेदारों के साथ विचार-विमर्श की प्रक्रिया की शुरुआत की गई। इसके बाद मंत्रालय ने लोगों की राय लेने के लिए नियमों का मसौदा तैयार किया और उस पर टिप्पणियां मांगी गईं।[5] अतंत: इस दिशा में ठोस कदम उठाते हुए 5 फरवरी 2021 को सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत सूचना प्रौद्योगिकी (मध्यवर्ती संस्थानों के लिए दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021 अधिसूचित कर दिए गए।[6]

5 https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1557240
6 https://pib.gov.in/PressReleasePage.aspx?PRID=1702320

भारत में साइबर सुरक्षा के प्रबंध-

भारत सरकार ने साइबर सुरक्षा से जुड़ी समस्याओं के समाधान हेतु अनेक कानूनी, तकनीकी और संस्थागत कदम उठाए हैं। वस्तुत: भारत में साइबर अपराधों के लिए न केवल नियम-कानून मौजूद हैं, बल्कि भारत सरकार ने देश को साइबर हमलों और अपराधों से सुरक्षा प्रदान करने के लिए विभिन्न संस्थाएं भी गठित की हैं और साइबर मामलों की शिकायतों और जांच के लिए आवश्यक व्यवस्थाएं भी सुनिश्चित की हैं।

संस्था	गठन का उद्देश्य	गठन का वर्ष
भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (Indian Computer Emergency Response Team) CERT-In	• इसका गठन साइबर घटनाओं के बारे में सूचना एकत्र करने, विश्लेषण करने और प्रसार करने, साइबर सुरक्षा घटनाओं के बारे में पूर्वानुमान लगाने और चेतावनियां देने, साइबर सुरक्षा घटनाओं से निपटने के लिए आपात उपाय करने, साइबर घटना प्रत्युत्तर कार्यकलापों का समन्वय करने, सूचना सुरक्षा प्रक्रियाओं, पद्धतियों, रोकथाम, प्रत्युत्तर और साइबर घटनाओं की रिपोर्टिंग से संबंधित दिशानिर्देश देने, परामर्शी निदेश, देने और सुभेद्यता नोट तथा श्वेत पत्र जारी करने के उद्देश्य से किया गया है।	2004

राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र (National Critical Information Infrastructure Protection Centre-NCIIPC)	इस केन्द्र की स्थापना हवाई नियंत्रण, नाभिकीय तथा अंतरिक्ष संबंधी महत्वपूर्ण रणनीतिक क्षेत्रों में साइबर सुरक्षा संबंधी खतरों से निपटने के उद्देश्य से की गई है, जो राष्ट्रीय तकनीकी अनुसंधान संगठन (NTRO) के अंतर्गत कार्य करता है।	2014
राष्ट्रीय साइबर समन्वय केन्द्र (NCCC)[7]	यह केन्द्र आसन्न और संभावित साइबर सुरक्षा खतरों के प्रति जागरूकता उत्पन्न करता है और संबंधित संस्थाओं/सुरक्षा एजेंसियों को समय रहते खतरों की रोकथाम की त्वरित कार्रवाई हेतु सचेत करते हुए आवश्यक सूचनाएं मुहैया कराता है।	2015
साइबर स्वच्छता केन्द्र (Cyber Swachhta Kendra)[8]	यह इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय द्वारा उपलब्ध कराई गई एक वेबसाइट है, जिसे राष्ट्रीय साइबर सुरक्षा नीति के लक्ष्यों के अनुरूप तैयार किया गया है। यह वेबसाइट यूजर्स को इन्फर्मेशन और टूल्स मुहैया करवाती है ताकि वे अपने कम्प्यूटर सिस्टम और डिवाइसों को सुरक्षित रख सकें। इस वेबसाइट का संचालन CERT-In द्वारा ही किया जा रहा है।	2017

7 https://www.bankinfosecurity.asia/india-opens-cyber-coordination-centre-a-8100

8 https://navbharattimes.indiatimes.com/tech/gadgets-news/cyber-swacchta-kendra-botnet-cleaning-and-malware-analysis-centre-free-bot-removal-tools/articleshow/57267600.cms

साइबर एवं सूचना सुरक्षा (C&IS) प्रभाग[9]	यह प्रभाग साइबर सुरक्षा, साइबर अपराध, राष्ट्रीय सूचना सुरक्षा नीति एवं दिशानिर्देश (एनआईएसपीजी) और एनआईएसपीजी, नैटग्रिड आदि के कार्यान्वयन से संबंधित मामले देखता है।	2017
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (National Cyber Crime Reporting Portal : www.cybercrime.gov.in)[10]	भारत सरकार के गृह मंत्रालय की यह एक नागरिक-केंद्रित पहल है, जो इस पोर्टल के माध्यम से नागरिकों को साइबर अपराधों की शिकायत ऑनलाईन दर्ज करने की सुविधा उपलब्ध कराती है। यह पोर्टल खास तौर पर महिलाओं और बच्चों के विरुद्ध होने वाले साइबर अपराधों और बाल पोर्नोग्राफी, बाल यौन शोषण सामग्री, रेप/गैंग रेप से संबंधित ऑनलाइन सामग्री आदि से जुड़े अपराधों को अविलम्ब दर्ज करने हेतु उपलब्ध कराया गया है।	2019
रक्षा साइबर एजेंसी (Defence Cyber Agency-DCA)	साइबर जगत में संभावित खतरों से निपटने के लिए एकीकृत रक्षा स्टाफ (आईडीएस) के तहत यह विशेष साइबर एजेंसी गठित की गई है।	2019

9 https://www.mha.gov.in/hi/division_of_mha

10 https://pib.gov.in/PressReleasePage.aspx?PRID=1599068

भारतीय साइबर अपराध समन्वय केन्द्र (Indian Cyber Crime Coordination Centre- I4C)[11]	भारतीय साइबर अपराध समन्वय केन्द्र की योजना व्यापक और समन्वित तरीके से सभी प्रकार के साइबर अपराधों से निपटने के लिए है। इस योजना के सात घटक हैं- नेशनल साइबर क्राइम थ्रेट एनालिटिक्स यूनिट, नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल, नेशनल साइबर क्राइम ट्रेनिंग सेंटर, साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट, नेशनल साइबर क्राइम रिसर्च एंड इनोवेशन सेंटर, नेशनल साइबर क्राइम फॉरेंसिक लेबोरेट्री ईको सिस्टम और प्लेटफॉर्म फॉर ज्वाइंट साइबर क्राइम इन्वेस्टिगेशन टीम। गृह मंत्रालय की पहल पर 15 राज्यों और केन्द्र शासित प्रदेशों ने अपने यहां क्षेत्रीय अपराध समन्वय केन्द्र स्थापित करने की सहमति दी है।	2020
साइबर-दोस्त Twitter Handle - "@ CyberDost"[12]	लोगों को साइबर या ऑनलाइन ठगी से बचाने के लिए गृह मंत्रालय ने ट्विटर पर साइबर दोस्त नामक हैंडल शुरु किया है।	2020

निष्कर्ष रूप में हम कह सकते हैं कि भारत सरकार ने देश में मंडराते साइबर खतरों का मुकाबला करने में वैधानिक, तकनीकी और संस्थागत प्रयासों में कोई कसर नहीं छोड़ी है और इस दिशा में निरंतर अभिनव प्रयास किए जा रहे हैं, फिर भी यदि साइबर अपराधों को उनके उदगम पर ही रोकना है तो इन सभी व्यवस्थाओं और कानूनी प्रावधानों तथा साइबर अपराध के ख़तरों के प्रति जन-जन को जागरुक बनाना परमावश्यक है।

11 https://pib.gov.in/PressReleasePage.aspx?PRID=1599068

12 https://www.amarujala.com/india-news/home-ministry-started-cyber-dost-twitter-handle-to-create-awareness-about-cyber-crime-in-covid19

अध्याय 7

विश्व के चुनिंदा देशों में साइबर अपराध और उनके उन्मूलन की व्यवस्थाएं

सूचना और संचार प्रौद्योगिकी समूचे विश्व में व्यापक रूप से विद्यमान है। भारत जैसे विकासशील देश में गांव-गांव तक हर प्रकार की कनेक्टिविटी सुलभ है। इसीलिए यह कहना अतिश्योक्ति नहीं होगा कि आज विश्व का कोई राष्ट्र, महानगर, नगर और गांव साइबर अपराधों की ज़द से बाहर नहीं रहा हैं। साइबर अपराधी नई प्रौद्योगिकी का सहारा लेकर विश्व के किसी भी कोने में बड़े से बड़े साइबर अपराधों या साइबर हमलों को अंजाम देने की योजना बना सकते हैं और थोड़ी बहुत जद्दोजहद के बाद इसे मूर्त रूप भी दे सकते हैं। इक्कीसवीं शताब्दी में साइबर- जासूसी, साइबर-आतंकवाद और साइबर-युद्ध जैसे खतरों ने दुनिया के सामने नई मुश्किलें पैदा कर दी हैं। जैसे-जैसे इंटरनेट प्रयोगकर्ताओं की संख्या बढ़ती जा रही है वैसे-वैसे दुनिया भर में साइबर अपराधों का ग्राफ भी बढ़ता जा रहा है। आज साइबर हमलों से विश्व का कोई भी देश अछूता नहीं है। ये इंटरनेट ऑफ थिंग्स, क्लाउड कम्प्यूटिंग, आर्टिफिशियल इंटेलीजेंस और अत्याधुनिक सूचना व संचार प्रौद्योगिकी का जमाना है और हर देश में इस समय एक मजूबत व समन्वित साइबर सुरक्षा प्रणाली का होना बहुत जरूरी है।

पिछले कुछ वर्षों में पूरे विश्व में साइबर हमले तेज हुए हैं। जानकारों के अनुसार दुनिया भर की लगभग 70 प्रतिशत वेबसाईटें हैकिंग का शिकार हैं। 'दी इकॉनामिक टाईम्स' में दिसम्बर 2020 में प्रकाशित एक रिपोर्ट[1] के

1 https://economictimes.indiatimes.com/news/company/corporate-trends/massive-cyberattacks-that-shook-the-world-in-2020/articleshow/79937731.cms?from=mdr

अनुसार वर्ष 2020 बड़े साइबर हमलों से अटा पड़ा था। कोराना महामारी से जूझ रहे विश्व में जब लोग अपने इंटरनेट डिवाइजों पर पूरी तरह से निर्भर हो गए थे, साइबर अपराधी अपने मनसूबों को अंजाम देकर लाभ कमाने की होड़ में जुटे हुए थे और उन्हें इसके लिए खूब मौके भी मिल रहे थे। इस दौरान रेनसमवेयर के द्वारा काफी साइबर हमलों को अंजाम दिया गया, कई लोगों का डाटा चोरी कर लिया गया। वहीं कुछ देशों द्वारा प्रायोजित साइबर हमलों को भी बखूबी अंजाम दिया गया। वर्ष के अंत में एक सबसे बड़ा साइबर हमला उस समय उजागर हुआ जब साइबर सुरक्षा से जुड़ी एक कम्पनी FireEye ने दिसम्बर की शुरूआत में यह बताया कि कि कम्पनी खुद ही हैकर्स के हमले का शिकार बन गई। ये हैकर्स कम्पनी के ऐसे टूल्स तक जा पहुंचे थे, जिन्हें कम्पनी के द्वारा अपने ग्राहकों की सुरक्षा-जांच के लिए प्रयोग किया जाता था। इस साइबर हमले के दायरे की जांच-पड़ताल करते हुए यह ज्ञात हुआ कि यह हमला एक कम्पनी या संगठन को निशाना बना कर किया गया कोई साधारण साइबर हमला नहीं था। 'वॉल स्ट्रीट जर्नल' में प्रकाशित रिपोर्ट के अनुसार संदिग्ध रूसी हैकर्स ने एक आई.टी. मैनेजमेंट कम्पनी SolarWinds द्वारा बेचे गए 'ओरियन' साफ्टवेयर में एक मालवेयर स्थापित कर दिया था और इस मालवेयर के जरिये हैकर्स ने संयुक्त राज्य की कई सरकारी एजेंसियों का संवेदनशील डाटा हथिया लिया था। मेलिशियस कोड युक्त इस साफ्टवेयर को 24 बड़ी कम्पनियों ने भी स्थापित किया था, जिसमें Cisco, VMware और Nvidia जैसी प्रतिष्ठित कम्पनियां भी शामिल थीं। माइक्रोसाफ्ट के प्रेसिडेन्ट ब्रैड स्मिथ ने कहा था कि यह साइबर हमला संयुक्त राज्य एवं उसकी सरकार तथा अन्य महत्वपूर्ण संस्थाओं व कुछ सुरक्षा फर्मों को निशाना बना कर किया गया था। इस हमले से पहले भी होटल समूह 'मेरिएट इंटरनेशनल' ने यह कहते हुए सनसनी फैला दी थी कि हैकर्स ने उनके दो कर्मचारियों के लॉग-इन विवरणों का इस्तेमाल करके 52 लाख ग्राहकों की निजी जानकारियां हथिया लीं। वहीं इस साल

के मध्य में सोशल मीडिया प्लेटफॉम ट्विटर ने अपने ऊपर हुए एक "को-ऑर्डिनेटेड सोशल इंजीनियरिंग हमले" की बात से सबको हैरान कर दिया। इस हमले में क्रिप्टोकरेंसी घोटाले के मकसद से कई सुप्रसिद्ध हस्तियों के ट्विटर खाते हैक किए जाने की खबर थी, जिनमें उस समय संयुक्त राज्य के राष्ट्रपति पद के उम्मीदवार जो बाइडेन, बराक ओबामा, एलन मस्क, बिल गेट्स, जेफ बेजोस, एप्पल और उबर के ट्विटर खातों के नाम शामिल बताए गए थे। वहीं अगस्त–सितम्बर में न्यूज़ीलैण्ड के स्टॉक एक्सचेंज पर कई बार साइबर हमले हुए, जिनके चलते एक्सचेंज को लेनदेन बंद करना पड़ा। नवम्बर में माइक्रोसाफ्ट ने यह खुलासा किया कि कोविड-19 के टीके और उपचार की खोज में लगी 7 प्रमुख कम्पनियों, जिनमें भारत की कम्पनियां भी शामिल थीं, को भी साइबर हमलों का निशाना बनाया गया था। कनाडा, फ्रांस, भारत, दक्षिण कोरिया और संयुक्त राज्य की इन दवा कम्पनियों और टीका-अनुसंधान कम्पनियों को रूस द्वारा प्रयोजित Strontium नामक एक्टर और उत्तरी कोरिया द्वारा प्रायोजित Zinc एवं Cerium नामक एक्टरों ने निशाना बनाया था।

उपरोक्त विश्लेषण से स्पष्ट है कि विश्व भर में साइबर हमलों और साइबर अपराधों का दायरा सूचना-प्रौद्योगिकी के विकास के साथ बढ़ता जा रहा है। विश्व के सभी देश साइबर सुरक्षा पर हर वर्ष एक बड़ी रकम खर्च करते हैं, क्योंकि उन्हें हर मोर्चे पर अपने देश की आर्थिक, सामाजिक, वैज्ञानिक और रणनीतिक व्यवस्थाओं को चारों तरफ से तेज होते साइबर हमलों से बचाना है। वैश्विक साइबर सुरक्षा सूचकांक (Global Cyber Security Index) एक विश्वसनीय सूचकांक है जो वैश्विक साइबर सुरक्षा की ओर विभिन्न देशों की प्रतिबद्धता को दर्शाता है तथा साइबर सुरक्षा के महत्व एवं विभिन्न आयामों के प्रति जागरूकता फैलाता है। चूँकि साइबर सुरक्षा का क्षेत्र बहुत ही व्यापक है और इसमें बहुत से उद्योग एवं विभिन्न कार्यक्षेत्र समाहित होते हैं, अत: इस सूचकांक के निर्धारण में प्रत्येक देश की विकासशीलता

अथवा योगदान को निम्नलिखित पांच मानदण्डों के आधार पर आंका जाता है- (1) विधिक मानदण्ड (2) तकनीकी या प्रौद्योगिकी संबंधी मानदण्ड (3) संगठनात्मक मानदण्ड (4) क्षमता विकास (5) समन्वय और इन सबको मिलाकर निकाला जाने वाला औसतन स्कोर।[2].इस सूचकांक का निर्धारण अंतरराष्ट्रीय दूरसंचार संघ (International Telecommunication Union) करता है, जिसका मुख्यालय जिनेवा, स्विटजरलैण्ड में स्थित है। पिछला वैश्विक साइबर सुरक्षा सूचकांक वर्ष 2018 के लिए जारी किया गया था। इसके बाद का सूचकांक वर्ष 2021 की द्वितीय तिमाही में जारी किए जाने की संभावना है।[3] वर्ष 2018 के वैश्विक साइबर सुरक्षा सूचकांक के संबंध में जारी रिपोर्ट[4] के अनुसार भारत को उच्चस्तरीय प्रतिबद्धता वाले देशों में शामिल किया गया है। फिर भी इस रिपोर्ट के पृष्ठ संख्या 62 पर दी गई विश्वस्तरीय रैंकिंग में भारत 0.719 अंकों के साथ 47 वें स्थान पर है। वस्तुत: इस सूची में यूनाईटेड किंगडम 0.931 अंकों के साथ पहले स्थान पर, संयुक्त राज्य अमेरिका 0.926 अंकों के साथ दूसरे स्थान पर और फ्रांस 0.918 अंकों के साथ तीसरे स्थान पर है। वहीं भारत के पड़ोसी देशों में चीन 0.828 अंकों के साथ 27वें स्थान पर, बांग्लादेश 0.525 अंकों के साथ 78वें स्थान पर और पाकिस्तान 0.407 अंकों के साथ 94वें स्थान पर है।

इस संबंध में किए गए एक अन्य विश्लेषण में चार अलग-अलग विश्वस्तरीय संस्थाओं द्वारा प्रस्तुत आंकड़ों का तुलनात्मक अध्ययन किया गया। इन संस्थाओं में अंतरराष्ट्रीय दूरसंचार संघ (ITU) के साथ Analytics Insights, CyberDB, Comparitech के आंकलनों को शामिल किया गया, जिसमें

2 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

3 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

4 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

निम्नलिखित देशों को साइबर सुरक्षा के प्रति सबसे ज्यादा प्रतिबद्ध बताया गया[5]-

आईटीयू	एनालीटिकल इन्साइट्स	साइबर डीबी	कॉम्पेरिटेक
यूनाईटेड किंगडम	यूएसए	यूएसए	जापान
यूएसए	रूस	इजराइल	फ्रांस
फ्रांस	इजरायल	रूस	कनाडा
लिथुआनिया	चीन	कनाडा	डेनमार्क
एस्टोनिया	स्पेन	यूनाईटेड किंगडम	यूएसए

अब साइबर सुरक्षा को लेकर सबसे ज्यादा प्रतिबद्धता की यदि बात की जाए तो इन चारों सूचियों में यूएसए का नाम अनिवार्य रूप से शामिल किया गया है और क्यों न हो, इस सर्वेक्षण के अनुसार विश्व के 58 प्रतिशत डिजिटल सुरक्षा संगठन संयुक्त राज्य अमेरिका में स्थित हैं। इस रिपोर्ट में विभिन्न देशों द्वारा साइबर सुरक्षा के क्षेत्र में अर्जित उपलब्धियों का भी उल्लेख किया गया है-

- यूनाइटेड किंगडम ने अपने एक्टिव साइबर डिफेंस प्रोग्राम के जरिये हजारों साइबर हमलों को रोका है।
- लिथुआनिया ने राष्ट्रीय साइबर सुरक्षा केन्द्र की स्थापना की है।
- स्पेन ने सार्वजनिक और निजी क्षेत्रों के बीच में समन्वय स्थापित करने और साईबर सुरक्षा को सुदृढ़ बनाने के लिए राष्ट्रीय साइबर सुरक्षा परिषद का गठन किया है।

5 https://cipher.com/blog/which-country-is-1-in-cybersecurity/

- चीन ने 2017 में साइबर सुरक्षा नियम लागू किए हैं, ताकि साइबर सुरक्षा के साथ राष्ट्रीय सुरक्षा को सुदृढ़ बनाया जा सके।
- एस्टोनिया यूरोप का वह देश है जिसने इतने पुख्ता साइबर सुरक्षा इंतेजाम किए हैं कि आज वहां इंटरनेट नि:शुल्क होने के बाद भी साइबर अपराध घटित नहीं होते।[6]
- स्वीडन में मालवेयर संक्रमण की दर विश्व में सबसे कम है।
- जापान में मोबाईल मालवेयर संक्रमण की दर सबसे कम यानी 1.34% है।
- विश्व के 300 देशों में कम्प्यूटर आपात प्रतिक्रिया दल (CERT) स्थापित किए गए हैं, भारत में इस दल का नाम CERT-In है।

वैसे तो विश्व के सभी देशों ने सूचना एवं संचार प्रौद्योगिकी के इस युग में साइबर सुरक्षा के लिए अपने-अपने स्तर पर व्यवस्थाएं की हैं, लेकिन वैश्विक साइबर सुरक्षा सूचकांक से यह स्पष्ट रूप से पता चलता है कि कौन सा देश साइबर सुरक्षा के क्षेत्र में कितना प्रतिबद्ध है। वस्तुत: विश्व में साइबर सुरक्षा को लेकर सर्वाधिक प्रतिबद्ध देशों की स्थिति गहन विश्लेषण के बाद कुछ इस प्रकार सामने आती है[7] :-

1) संयुक्त राज्य अमेरिका एक ऐसा देश रहा है जिसने साल दर साल बड़ी संख्या में साइबर हमलों का सामना किया है। यही कारण है कि 58 प्रतिशत साइबर सुरक्षा कम्पनियां इसी देश में स्थित हैं और हर प्रकार के साइबर हमलों से बचने के उपाय खोजती रहती हैं।

6 https://hindi.news18.com/photogallery/knowledge/european-nation-estonia-is-a-model-for-free-and-open-internet-access-mrj-3220394.html

7 https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/

2) इजराइल दूसरा ऐसा देश है जहां सबसे ज्यादा साइबर सुरक्षा कम्पनियां हैं और इनकी संख्या बढ़ती जा रही है।

3) रूस पर इसके राजनीतिक दुश्मन भले ही बार-बार साइबर-जासूसी और साइबर-हमलों के आरोप लगाते हों, लेकिन रूस ने अपने देश में साइबर-जासूसी और साइबर सुरक्षा खतरों से बचने के लिए पुख्ता इंतेजाम किए हैं। यूनाईटेड स्टेट्स काँग्रेस के एक सार्वजनिक नीति अनुसंधान संस्थान 'काँग्रेशनल रिसर्च सर्विस' ने अपनी 4 जनवरी 2021 की रिपोर्ट में उल्लेख किया है कि रूस ने नई किस्म की साइबर इकाईयां बनाई हैं ताकि वह इन इकाईयों की विशिष्ट साइबर क्षमताओं के साथ विश्व भर में दुष्प्रचार, अन्य किस्म का प्रचार, जासूसी और साइबर हमलों को अंजाम दे सके।[8] इस रिपोर्ट में रूस के पिछले साइबर अभियानों का भी हवाला दिया गया है।

4) कनाडा की संघीय सरकार के बारे में कहा जाता है कि वह साइबर सुरक्षा पर हर वर्ष 1 अरब की धनराशि खर्च करती है, जो निसंदेह इस बात का प्रमाण है कि कनाडा साइबर अपराधों की रोकथाम के लिए काफी कुछ कर रहा है।

5) यूनाइटेड किंगडम एक 'साइबर सुरक्षा मानक' अपना कर आसन्न साइबर सुरक्षा खतरों से जूझने के लिए प्रतिबद्ध है। यहां एक राष्ट्रीय साइबर सुरक्षा केन्द्र (National Cyber Security Centre) की स्थापना वर्ष 2016 में की गई थी, जिसका मकसद यूनाईटेड किंगडम को रहने और ऑनलाईन काम करने के लिए सबसे सुरक्षित देश बनाना है।

8 https://crsreports.congress.gov/product/pdf/IF/IF11718

6) मलेशिया भी सिंगापुर की तरह साइबर सुरक्षा की दृष्टि से बहुत सुदृढ है और वर्ष 2017 के वैश्विक साइबर सुरक्षा सूचकांक के अनुसार इसका विश्व में तीसरा स्थान था।

7) चीन ने वर्ष 2017 में एक नया साइबर सुरक्षा कानून लागू किया है। इस कानून का मूल उद्देश्य चीन में साइबर सुरक्षा और राष्ट्रीय सुरक्षा को सुदृढ़ बनाना है। हालांकि चीन में रह रहे विदेशी व्यवसासियों या उनसे जुड़े लोगों में इस संस्था को लेकर सरगर्मियां अक्सर बनी रहती हैं।

8) फ्रांस ने 16 अक्टूबर 2015 को 'द फ्रेंच नेशनल डिजिटल सिक्योरिटी स्ट्रेटेजी' को अंगीकार किया है।[9] वहीं यह भी कहा जाता है कि फ्रांस साइबर सुरक्षा के क्षेत्र में यूनाइटेड किंगडम, चीन, रूस और यूएसए के साथ सहभागिता बनाने को लालायित रहता है।[10]

9) स्वीडन में मालवेयर संक्रमण के सबसे कम (यानी के दुनिया के 19.88 प्रतिशत) मामले पाए गए और यह देश साइबर आतंकवाद से लड़ने और अपनी साइबर सुरक्षा को मजबूत करने के लिए निरंतर प्रयत्नशील रहता है।

10) एस्टोनिया को खास तौर पर इसकी ई-गवरनेन्स सेवाओं के लिए जाना जाता है। वर्ष 2007 में हुए बड़े साइबर हमलों से जूझते हुए इस देश ने साइबर युद्ध का डटकर मुकाबला करने की सीख ली है, जो वाकई अनुकरणीय है।

साइबर सुरक्षा के प्रति कृतसंकल्पित इन देशों की तैयारियों से साफ जाहिर होता है कि ये देश न केवल साइबर अपराधों, बल्कि साइबर-जासूसी,

9 https://www.ssi.gouv.fr/en/cybersecurity-in-france/

10 https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/

साइबर-हमलों, साइबर-आतंकवाद और साइबर-युद्ध के प्रति भी सजग हैं। जैसा कि पूर्व के अध्यायों में उल्लेख किया गया है भारत में भी साइबर सुरक्षा के कानून और उपायों की अपर्याप्तता नहीं है, किन्तु यहां साइबर अपराधों की साल-दर-साल बढ़ती या यूं कहें दुगनी, तुगनी होती संख्या साफ दिखाई देती है। कहना न होगा कि रोज दर्ज किए जाने वाले नए साइबर अपराधों की संख्या में कमी अन्वेषण की प्रक्रिया को तेज करने से नहीं बल्कि पुलिस एवं सुरक्षा एजेंसियों के साथ जनता को जागरुक होने से आएगी। साइबर अपराध यदि एक बार घटित हो जाता है तो अन्वेषण ही आखिरी विकल्प बचता है, जो वाकई में अपनी तकनीकि प्रवृत्ति के कारण इतना आसान नहीं होता, जितना कि सामान्य अपराधों का अन्वेषण। भारत को यदि वैश्विक साइबर सुरक्षा सूचकांक की फेहरिस्त में सम्मानजनक स्थान दिलाना है तो पुलिस एवं सुरक्षा एजेंसियों को साइबर अपराधों के प्रखर अन्वेषण के साथ-साथ जनता को जागरुक बनाने के प्रति और ज्यादा प्रतिबद्ध होना होगा।

अध्याय 8

भारत में साइबर अपराध के मामलों का पंजीकरण और अन्वेषण

साइबर अपराधों का आंकड़ा हर साल एक नई ऊंचाई को छूने लगा है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो द्वारा जारी विगत 3 वर्षों के आंकड़ों में यह वृद्धि साफ तौर पर दिखाई देती है। हैरानी की बात तो यह है कि साइबर अपराधों की न केवल संख्या में इजाफा हो रहा है, बल्कि इनके नित्य-नए स्वरूप और तौर-तरीके भी सामने आ रहे हैं।

ऐसी स्थिति में निश्चित रूप से उन परिस्थितियों और कारकों पर गहराई से विचार करना आवश्यक हो जाता है जो समाज में आपराधिक प्रवृत्तियों को जन्म देते हैं। निसंदेह कोई भी इंसान जन्मजात अपराधी नहीं होता। आपराधिक प्रवृत्तियां इंसान के भीतर पनपती जरूर हैं, लेकिन उनके बीज आसपास के कलुषित वातावरण की पृष्ठभूमि पर ही अंकुरित होते हैं। वातावरण का मनोवृत्तियों पर सीधा असर पड़ता है। यह भी एक सत्य है कि मनुष्य की मनोवृत्तियां भी आयु और वातावरण के साथ बदलती रहती हैं। किसी मनुष्य के अपराधी बनने के कारणों पर यदि विचार किया जाए तो इसके अनेकानेक कारण हो सकते हैं, जो निसंदेह देश, काल और वातावरण पर निर्भर करते हैं। उदाहरण के लिए ऐसी कई कहानियां हमने फिल्मों में देखी व सुनी हैं कि गांव का एक सीधा-सादा युवक शहर आकर अपने लिए रोजी-रोटी, कपड़ा और मकान तलाशते-तलाशते अपराध की डगर पर चल पड़ा और एक शातिर व कुख्यात अपराधी बन गया। कभी अपराध मजबूरी में होते हैं, कभी बदले की भावना से, कभी धन और विलासिता के लालच से, कभी समाज व राजनीति में अपना लोहा मनवाने के लिए, कभी किसी

की संगत में आकर तो कभी शौकिया। अब अपराध-शास्त्र की यदि बात की जाए तो इसमें सैद्धांतिक रूप से अपराधों के कई कारण गिनाए जाते हैं जैसे- सामाजिक, आर्थिक और मनोवैज्ञानिक इत्यादि।

जहां तक साइबर अपराधों का प्रश्न है, इनके पीछे भी सामान्य अपराधों की भांति ही कुछ न कुछ कारण होते हैं। लेकिन अंतर सिर्फ इतना है कि साइबर अपराधों की दुनिया में अपराध का कारण उत्पन्न होते और फिर अपराध को अंजाम देते देर नहीं लगती। यहां भी अपराध कभी लाचारी में, कभी मजबूरी में, कभी जल्दी अमीर बनने के लालच में, कभी अपने समाज व राजनीति में अपना लोहा मनवाने के लिए, कभी दूसरों की संगत में आकर तो कभी शौकिया और मौज-मजे के लिए अंजाम दिए जाते हैं। जिस तरह से हम यह कह सकते हैं कि साइबर अपराध या तो व्यक्ति के विरुद्ध होते है, या संपत्ति के विरुद्ध अथवा सरकार के विरुद्ध, ठीक उसी तरह से साइबर अपराधों को अंजाम देने वाले अपराधियों की प्रवृत्तियों को निम्न 5 किस्मों में बांटा जा सकता है-

1. ऐसे साइबर अपराधी जो शौकिया ही हैकिंग जैसे अपराध करते हैं।
2. ऐसे साइबर अपराधी जो हैकिंग जैसे अपराधों के जरिये राजनीतिक या अन्य गलियारों में नाम कमाना चाहते है।

3. ऐसे साइबर अपराधी जो विकृत मनोवृत्तियों के चलते साइबर अपराधों को अंजाम देते हैं।

4. ऐसे साइबर अपराधी जो धन कमाने के लिए साइबर अपराध करते हैं या किसी आर्थिक अपराध गिरोह से जुड़ कर संगठित साइबर अपराधों का हिस्सा बन जाते हैं।

5. ऐसे साइबर अपराधी जो बदले की किसी भावना से साइबर अपराधों को अंजाम देते हैं।

बहरहाल, एक बात और भी है कि साइबर जगत में अनजाने ही किसी अपराध का हो जाना बहुत ही आम बात है और इसकी अनगिनत संभावनाएं रहती हैं, क्योंकि कम्प्यूटर संसाधनों, मोबाइल/स्मार्ट फोन तथा सूचना व संचार प्रौद्योगिकी के प्रयोगकर्ता इनकी तकनीकी बारीकियों और कानूनी पहलुओं से भली-भांति परिचित नहीं रहते हैं।

अधीरता मानव स्वभाव की एक सहज वृत्ति है और कमोबेश हर इंसान में पाई जाती है। कम्प्यूटर, मोबाइल, स्मार्ट-फोन और सूचना व संचार प्रौद्योगिकी के इस युग से पहले निसंदेह मानव सभ्यता में आपराधिक प्रवृत्तियां अपेक्षाकृत कम पाई जाती थीं। इसका एक कारण यह भी था कि इंसान अपने मन में छिपी कई विकृत मनोवृत्तियों के उजागर होने से डरता था और ऐसे में संयमित व्यवहार उसकी आदत बन जाता था। उदाहरण के तौर पर यदि किसी के पास कोई वस्तु या धन नहीं होता था तो लाख बार मन ही मन सोच कर भी वह इस डर से चोरी नहीं कर पाता था कि समाज उसके बारे में क्या सोचेगा, उसका अपमान हो जाएगा और उसे सजा हो जाएगी। वहीं आज के दौर में स्थिति एक दम बदल चुकी है। अब चोरी की उस मनोवृत्ति को किसी के सामने प्रकट करने की जरूरत नहीं है। बस अपना मोबाइल उठा कर फिशिंग जैसे किसी अपराध को चुपचाप अंजाम देना है, धन हड़पना है

और फिर लापता हो जाना है। यही है साइबर अपराध की दुनिया का सच, जहां विकृत मनोवृत्तियां, अधीरता और उतावलापन बहुत तेजी से अपराध में बदल जाता है और फिर अपराधी नदारद हो जाता है। ये तो हुई बात साइबर धोखाधड़ी की अन्य तरह के साइबर अपराधों में भी स्थितियां कुछ ऐसी ही है और इन्हीं परिस्थितियों एवं मनोवृत्तियों के चलते अनेक प्रकार के साइबर अपराधों को अंजाम दिया जा रहा है। इस पुस्तक के अध्याय-2 में हमने साइबर अपराधों के प्रकार और प्रौद्योगिकी के साथ बदलती प्रकृति के बारे में पढ़ा, जिसमें एक सैद्धांतिक दृष्टिकोण अपनाया गया था। वस्तुत: आज इतनी तरह के साइबर अपराधों को अंजाम दिया जा रहा है, जिनके बारे आम आदमी सोच भी नहीं सकता। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो और गृह मंत्रालय के सूत्रों के अनुसार भारत में किस प्रकार के साइबर अपराध आम तौर पर घटित होते हैं उनका विवरण इस प्रकार है:-

1) साइबर अश्लीलता और बाल यौन शोषण सामग्री का प्रसार (Cyber Pornography/Child Sexually Abusive Material-CSAM)

सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 67, 67(क) और 67(ख) के अनुसार क्रमश: अश्लील सामग्री का इलेक्ट्रानिक रूप से प्रकाशन व पारेषण, कामुकता वयक्त करने वाले कार्य आदि की सामग्री के इलेक्ट्रॉनिक रूप से प्रकाशन और कामुकता व्यक्त करने वाले कार्य आदि में बालकों को चित्रित करने वाली सामग्री को इलेक्ट्रॉनिक रूप से प्रकाशित व पारेषित करना दण्डनीय अपराध है। इस धारा के प्रयोजनों के लिए "बालक" से ऐसा व्यक्ति अभिप्रेत है, जिसने अट्ठारह वर्ष की आयु पूरी न की हो।

☞ राष्ट्रीय अपराध रिकॉर्ड ब्यूरो की रिपोर्ट के अनुसार वर्ष 2019 में साइबर अश्लीलता के प्रसार के कुल 1158 मामले दर्ज किए गए, जिनमें से सर्वाधिक 341 मामले ओड़िशा में और 178 मामले उत्तर प्रदेश में दर्ज किए गए। वहीं बाल यौन शोषण सामग्री प्रसार से संबंधित कुल 102 मामले दर्ज किए गए, जिनमें से सर्वाधिक 27 मामले केरल में और 25 मामले उत्तर प्रदेश में दर्ज किए गए।[1]

2) साइबर दुर्व्यवहार/बदमाशी (Cyber bullying)

किसी व्यक्ति को इंटरनेट से जुड़े कम्प्यूटर या मोबाइल फोन के जरिये परेशान करना, भयभीत करना या डराना-धमकाना साइबर बुलिंग कहलाता है। इसके अंतर्गत किसी व्यक्ति को असभ्य, घटिया और तकलीफदेह संदेश भेजना, सोशल साइट्स पर असभ्य टिप्पणियां करना, किसी को चित्र या वीडियो जैसी सामग्री भेज कर जानबूझ कर तंग करना या डराना और सोशल नेटवर्किंग साइट के चैटरूम व मैसेंजर

1 https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf

आदि का प्रयोग करके लोगों का परेशान करना या डराना-धमकाना आदि शामिल होता है। साइबर बुलिंग अक्सर मित्र, रिश्तेदार या सोशल नेटवर्किंग साइट से जुड़े लोगों अथवा ऑनलाईन गेम्स खेलने वालों

द्वारा की जाती है। भा.द.स. की धारा 354(डी) के साथ पठित सूचना प्रौद्योगिकी अधिनियम की संगत धाराओं के अधीन दण्डनीय अपराध है।

3) साइबर स्टॉकिंग (Cyber Stalking)

ऑनलाइन माध्यम से की गयी छेड़खानी को साइबर स्टॉकिंग कहा जाता है। जब ऑनलाइन माध्यम का प्रयोग करके किसी को परेशान करने के लिए जब ईमेल या मैसेज भेजा जाता है तो वह साइबर स्टॉकिंग कहलाता है। यह भा.द.सं. की धारा 354(सी) एवं (डी) और सूचना प्रौद्योगिकी अधिनियम 2000 के संगत प्रावधानों के अंतर्गत दण्डनीय अपराध है।

☞ राष्ट्रीय अपराध रिकॉर्ड ब्यूरो की रिपोर्ट के अनुसार वर्ष 2019 में साइबर बुलिंग/स्टॉलकिंग के कुल 836 मामले दर्ज किए गए, जिनमें सबसे ज्यादा 455 मामले महाराष्ट्र और 65 मामले हरियाणा में दर्ज किए गए।

4) साइबर ग्रूमिंग(Cyber Grooming)

साइबर ग्रूमिंग इंटरनेट पर बढ़ता एक ऐसा खतरा है, जिसमें अपराधी कोई फर्जी एकाउंट बना कर बच्चों जैसा ही व्यवहार करके उनसे ऑनलाईन सम्पर्क बढ़ाते है और इस तरह बच्चों से भावनात्मक रुप से जुड़ जाते है। इसके बाद वे उनका विश्वास जीत कर उनके यौन शोषण की कोशिश करते हैं। सोशल नेटवर्किंग साइट्स बच्चों और किशोरों को बहुत आकर्षित करती हैं और वे उस पर अपनी तस्वीर या वीडियो आदि अपलोड करते रहते हैं और आने वाले लाईक्स से बहुत खुश होते हैं। ऐसे में साइबर ग्रूमर बच्चों या किशोरों की भावनाओं से खेलते हुए उनकी तारीफ करके या कोई प्रलोभन देकर उनकी अश्लील तस्वीरें एवं वीडियो आदि हासिल करने का प्रयास करते हैं। इसे ही साइबर ग्रूमिंग कहा जाता है, सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा-67(बी) के तहत एक दण्डनीय अपराध है।

☞ हालांकि राष्ट्रीय अपराध रिकॉर्ड ब्यूरो की वर्ष 2019 की वार्षिक रिपोर्ट में साइबर ग्रूमिंग के मामलों को अलग से नहीं दर्शाया गया है और कदाचित बच्चों की यौन शोषण सामग्री के प्रदर्शन संबंधी मामलों में समावेशित रखा गया है। भारत सरकार के गृह मंत्रालय ने बच्चों और किशोरों को ऐसे साइबर अपराधों के प्रति जागरूक बनाने के लिए 38 पन्नों की एक पुस्तिका जारी की है जो सभी प्रदेशों द्वारा जिलों की सरकारी वेबसाइटों पर उपलब्ध कराई गई है। इस पुस्तिका में बच्चों और किशोरों को साइबर अपराधों से बचाने के लिए बहुमुल्य जानकारियां प्रस्तुत की गई हैं।[2]

5) ऑनलाईन सेक्सटॉरशन (Online Sextortion)

इंटरनेट पर अश्लील साईट्स की भरमार है और उन्हें देखने वाले भी कम नहीं हैं। साइबर अपराधी ऐसे ही अश्लील साईट्स देखने वाले लोगों की ब्राउसिंग हिस्ट्री को हथिया लेते हैं और फिर उन लोगों को ब्लैकमेल करते हैं। इसे ही ऑनलाईन सेक्सटॉरशन कहा जाता है।

2 https://www.vimarsh.mp.gov.in/files/CyberSafetyHindi.pdf

☞ एक रिपोर्ट[3] के अनुसार दिल्ली पुलिस ने हाल ही में ऐसे 12 मामले पंजीबद्ध किए हैं, जिनकी तफ्तीश जारी है। इससे पहले जम्मू-कश्मीर में भी सेक्सटॉरशन के मामले सामने आए थे और वर्ष 2018 में वह भारत का पहला राज्य बन गया था, जिसने सेक्सटॉरशन को एक दण्डनीय अपराध करार दिया था। [4]

6) ऑनलाईन नौकरियों संबंधी धोखाधड़ी (Online Job Fraud)

भारत में बेरोजगारी की समस्या निरंतर बनी हुई है। माह मार्च 2021 के आंकड़ों की मानें तो भारत में बेरोजगारी की दर 6.5 फीसदी है,जो शहरों में 7.1 फीसदी और गांवों में 66.2 फीसदी है। भारत के दस राज्य- हरियाणा, राजस्थान, गोवा, हिमाचल प्रदेश, जम्मू-कश्मीर, झारखंड, बिहार, त्रिपुरा, दिल्ली और पंजाब में तो बेरोजगारी की दर

3 https://navbharattimes.indiatimes.com/metro/delhi/crime/now-new-kind-of-crime-in-cyber-world-called-sextortion/articleshow/80149159.cms

4 https://www.aajtak.in/trending/photo/jammu-kashmir-law-offence-of-sextortion-banning-sexual-exploitation-of-woman-tkha-591000-2018-12-15-5

ज्यादा है।[5] ऐसे में नौकरी की तलाश में युवा इंटरनेट सुविधाओं की मदद लेते हैं और यहां नौकरी का झांसा देकर उन्हें लूटने वाले ठगों का तांता लगा हुआ है। इनमें से ज्यादातर

जालसाज ऑनलाइन जॉब पोर्टल के माध्यम से अपना शिकार खोजते हैं।सबसे पहले वे जॉब रिक्रूटमेंट साइट से नौकरी तलाशने वालों की प्रोफाइल निकालते हैं। इनमें से जो उनके झांसे में आ जाते हैं, उनमें से सभी को ये जालसाज एक साथ ईमेल भेजते हैं,ताकि किसी को शक न हो। ये जालसाज खुद को जॉब कन्सल्टेंट के रूप में पेश करते हैं।

दिखावे के लिए अपनी फर्जी वेबसाइट और एक अस्थायी दफ्तर भी बना लेते हैं। इसके बाद नौकरी तलाश रहे बेरोजगारों से जॉब रजिस्ट्रेशन के नाम पर मोटी रकम फीस के रूप में वसूल कर लेते हैं। इन अभयर्थियों का ऑनलाईन या टेलीफोन द्वारा इंटरव्यू भी लिया जाता है और फिर फर्जी कॉल लैटर भी भेज दिया जाता है। नौकरी के नाम पर ये जालसाज ज्यादातर छोटे शहरों के युवा एवं साधारण कॉलेज व संस्थानों के स्नातक छात्र, जिनकी अंग्रेजी व हिंदी ज्यादा अच्छी नहीं होती तथा उन्हें 5 साल से कम का कार्यानुभव होता है को अपना निशाना बनाते हैं।

7) इन्टरनेट पर लालच देकर धोखाधड़ी या फिशिंग(Phishing)

फिशिंग इंटरनेट पर की जाने वाली चोरी का एक सामान्य रूप है। फिशिंग में अपराधी किसी व्यक्ति को ईमेल या एस.एम.एस. भेज कर या उसे फोन करके छल कपट से उसकी व्यक्तिगत जानकारियां जैसे नाम, बैंक खाता संख्या, नेट बैंकिंग पासवर्ड, डेबिट/क्रेडिट कार्ड संख्या, उसका पिन, सीवीवी नम्बर और व्यक्तिगत पहचान विवरण

5 https://www.abplive.com/news/india/unemployment-is-the-biggest-challenge-for-india-read-full-story-1823298

जैसे आधार कार्ड एवं पेन कार्ड का नम्बर आदि जान लेते हैं और फिर उसके खाते से पैसे निकाल लेते हैं, खरीद-फिरोख्त कर लेते हैं या अपने बिलों का भुगतान कर देते हैं। ईमेल से की जाने फिशिंग में प्रयोगकर्ता को किसी बैंक या प्रतिष्ठित संस्था के नाम से फर्जी ईमल भेज कर किसी अन्य फर्जी वेबसाइट पर ले जाया जाता है, जहां उसके विवरण चुरा लिए जाते हैं। फोन करके की जाने वाली फिशिंग/धोखाधड़ी को वॉइस फिशिंग और एस.एम.एस. के जरिये की जाने वाली फिशिंग को स्मिशिंग कहते हैं। बहरहाल, फिशिंग किसी भी तरह की हो, वह एक दण्डनीय अपराध है, जिसके बारे में सूचना प्रौद्योगिकी अधिनियम, 2000 (यथा-संशोधित 2008) की धारा 66(डी) और भा.द.सं. की धारा—419, 463, 465 एवं 468 में दण्डात्मक प्रावधान उल्लिखित हैं।

डेबिट/क्रेडिट कार्ड क्लोनिंग

एटीम या डेबिट एवं कार्डों ने हमारी जिंदगी को बेहद आसान बना दिया है, लेकिन इसके साथ ही ठगों को धन लूटने के नए अवसर हाथ लग गए हैं। कोविड-19 महामारी और इस दौरान हुए डिजिटल लेनदेनों में बढ़ोत्तरी के चलते ऑनलाईन या साइबर ठगी के मामले तेजी से बढ रहे हैं। आजकल साइबर ठगों ने कार्ड कलोनिंग के जरिये लोगों की गाढ़ी कमाई उनके खातों से उड़ाने का नया गोरखधंधा चालू कर दिया है। दरअसल हर डेबिट/क्रेडिट कार्ड में एक मैग्नेटिक स्ट्रिप होती है जिसमें ग्राहक के खाते से जुड़ी सभी जानकारी सुरक्षित रहती है। जालसाज 'स्कीमर' नामक डिवाइस का इस्तेमाल कार्ड क्लोनिंग के लिए करते हैं। इस डिवाइस को एक कार्ड स्वैपिंग मशीन में फिट कर दिया जाता है और कार्ड स्वाइप होने पर यह कार्ड की जानकारी को कॉपी कर लेता है। कॉपी किया गया डाटा एक इंटरनल मेमरी यूनिट में स्टोर हो जाता है। इसके बाद इस डाटा को एक ब्लैंक कार्ड में कॉपी कर दिया जाता है और इन्हीं कार्डों का इस्तेमाल कर ग्राहक के खाते से रकम उड़ा ली जाती है। इतना ही नहीं एटीएम के की-पैड में एक ओवरले डिवाइज लगा कर ग्राहक की पिन हथिया ली जाती है और इसके बाद जालसाज इन जानकारियों के जरिए ऑनलाइन लेनदेन कर धोखाधड़ी को अंजाम देते हैं।

एटीएम मशीन में स्कीमर दो जगहों पर लगाए जा सकते हैं-

1) पिन की-पेड पर

2) कार्ड इंसर्ट स्लॉट पर


सामान्य स्लॉट


स्कीमर


स्कीमर लगा स्लॉट

सावधानी ही बचाव है-

- एटीएम से रकम निकालने से पहले जांच लें कि उसमें कोई स्कीमर तो नहीं लगा है।
- स्वैपिंग मशीन को हाथ से टोटल कर जांच लें कि कहीं स्कीमर तो फिट नहीं किया गया है। स्कीमर की डिजाइन ऐसी होती है कि वह मशीन का हिस्सा लगे। यदि इसमें कुछ अजीब महसूस हो तो सावधान हो जाएं।
- की-पैड का एक कोना दबा कर देखें, यदि वहां पैड स्कीमर होगा तो उसका दूसरा सिरा ऊपर उठ जाएगा।
- यह बहुत जरूरी है कि आप समय-समय पर अपने डेबिट कार्ड का पिन बदलते रहें।

8) डेबिट/क्रेडिट कार्ड से धोखाधड़ी (Debit/Credit Card Fraud)

भारत में डेबिट/क्रेडिट कार्ड धोखाधड़ी से जुड़े मामले लगभग रोज की घटना है। इस प्रकार की धोखाधड़ी को साइबर अपराधियों द्वारा कई तरीकों से अंजाम दिया जाता है। इसमें वॉइस फिशिंग और कार्ड

क्लोनिंग जैसे नुस्खे भी उनके लिए बहुत कारगर सिद्ध होते हैं।

9. साइबर स्क्वाटिंग (Cyber Squatting)

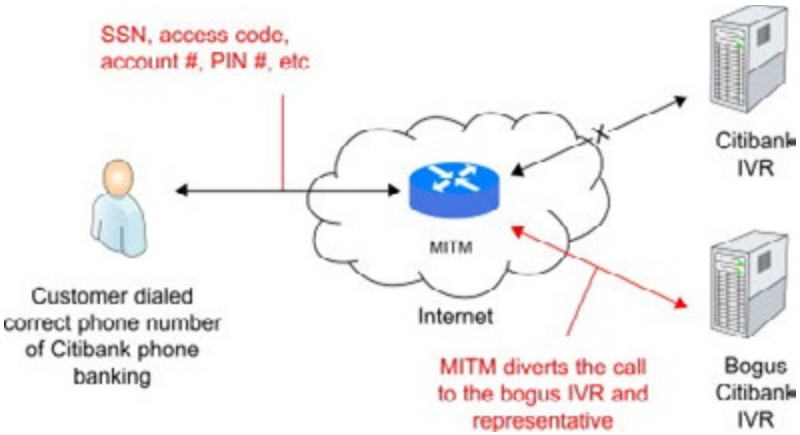
अंग्रेजी शब्द Squat, जिससे Squatting शब्द बना है, का शाब्दिक अर्थ होता है किसी जगह पर अवैध रूप से रहना। इस शाब्दिक अर्थ से हमें साइबर स्क्वाटिंग की अवधारणा को सरल रूप में समझने में बड़ी मदद मिलती है, क्योंकि साइबर स्क्वाटिंग का अभिप्राय इससे काफी मिलता-जुलता है। सीधे अर्थों में साइबर जगत में किसी प्रयोगकर्ता के मनवांछित स्थान(डोमेन) पर किसी अपराधी द्वारा गैरकानूनी रूप से कब्जा जमा लेना ही स्क्वाटिंग कहलाता है। इसे और ज्यादा विस्तार से समझने के लिए हमें पहले डोमेन नेम (Domain Name) की अवधारणा को समझना होगा। दरअसल डोमेन नेम किसी वेबसाइट का नाम और पता है, जिसके माध्यम से कोई प्रयोगकर्ता उस तक पहुंचता है। इंटरनेट पर कम्प्यूटरों की पहचान डोमेन नेम से ही होती है। डोमेन नेम में अक्षरों और संख्याओं का समावेश होता है और

इनके साथ इनके डोमेन नेम एक्सटेंशन जैसे -.com, .net भी जुड़े रहते हैं। प्रयोग से पहले डोमेन नेम को रजिस्टर करना होता है। हर डोमेन

नेम अपने आप में अद्वितीय होता है। किन्हीं भी दो वेबसाईटों का एक ही डोमेन नेम कभी नहीं हो सकता। उदाहरण के तौर पर यदि कोई व्यक्ति www.abcin.com टाइप करता है तो वह उसी डोमेन नेम की वेबसाइट पर जाएगा न कि किसी ओर वेबसाइट पर। डोमेन नेम को हर वर्ष नवीनीकृत करवाना होता है और यह कार्य बहुत तत्परता से करना होता है क्योंकि यदि ऐसा नहीं किया जाता तो साइबर स्क्वाटिंग करने वाले इस पर अपना कब्जा जमा सकते हैं और इसके लिए मोटी रकम की मांग कर सकते हैं। साइबर स्क्वाटिंग में किसी प्रतिष्ठित कम्पनी या ब्रांड के नाम से इंटरनेट डोमेन्स को रजिस्टर कर लिया जाता है, ताकि इसे बाद में उन कम्पनियों को बेचा जा सके। वस्तुत: भारत में अब तक डोमेन नेम संरक्षण के लिए अभी तक कोई कानून नहीं बनाया गया है और ऐसे ज्यादातर मामले ट्रेडमार्क एक्ट-1999 के तहत निपटाये जाते हैं।

10. फार्मिंग (Pharming)

फार्मिंग एक ऐसा अपराध है जिसमें हैकर्स इंटरनेट प्रयोगकर्ता को असली के स्थान पर किसी फर्जी वेबसाइट पर भेज देते हैं। यह नकली वेबसाइट इंटरनेट प्रयोगकर्ता की गोपनीय जानकारियां, जैसे- यूज़रनेम, पासवर्ड और डेबिट/क्रेडिट कार्ड का डाटा आत्मसात कर लेती है अथवा प्रयोगकर्ता के कम्प्यूटर पर कोई मालवेयर स्थापित कर देती है। फार्मिंग करने वाले अपराधी ज्यादातर वित्तीय क्षेत्र से जुड़ी वेबसाइट, जिनमें बैंक की वेबसाइटें, ऑनलाइन पेमेंट प्लेटफॉर्म या ई-कॉमर्स डेस्टीनेशन शामिल होते हैं, बना कर इंटरनेट पर लॉच कर देते हैं, जिनका खास मकसद प्रयोगकर्ताओं की जानकारी चुराना होता है, ताकि उसका गलत फायदों के लिए इस्तेमाल किया जा सके। फार्मिंग हमले इस लिए ज्यादा खतरनाक होते हैं, क्योंकि ये



प्रयोगकर्ता के साथ उसके कम्प्यूटर को भी नुकसान पहुंचाते हैं। इसका तकनीकी पक्ष ये है कि जब कभी किसी प्रयोगकर्ता को किसी वेबसाइट पर जाना होता है तो वह उसका यूआरएल दर्ज करता है। बस इसी यूआरएल को एक डीएनएस सर्वर द्वारा एक विशेष आई.पी. नम्बर से जोड़ दिया जाता है। डीएनएस सर्वर का अर्थ है, डोमेन नेम सिस्टम (Domain Name System) सर्वर, जिसे इंटरनेट की फोन-बुक भी कहा जा सकता है। इसे इस प्रकार समझा जा सकता है कि डीएनएस सर्वर एक फोन-बुक है और यूआरएल एक (वेबसाइट का) नाम तथा आई.पी. एड्रेस इसका फोन नम्बर है। अपराधी बड़ी आसानी से इस फोन-बुक रूपी डीएनएस सर्वर में नाम के आगे लिखें फोन नम्बर यानी आई.पी. नम्बर को अपनी चुनिंदा नकली वेबसाइट के आई.पी. नम्बर से बदल देते हैं। आज के दौर में फार्मिंग एक प्रचलित साइबर अपराध बन चुका है।

☞ चाहें फिशिंग हो, फार्मिंग हो, नौकरी के लिए ऑनलाइन धोखाधड़ी हो या फिर डेबिट/क्रेडिट कार्ड से जुड़ी धोखाधड़ी इन सभी के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 एवं भारतीय दंड संहिता की

विभिन्न धाराओं के साथ पठित संगत कानूनों में दण्ड का प्रावधान है। केन्द्रीय अपराध रिकॉर्ड ब्यूरो की वार्षिक रिपोर्ट के मुताबिक वर्ष 2019 के दौरान देश भर में कम्प्यूटर एवं इंटरनेट संसाधनों के माध्यम से की गई जालसाजी/ठगी/धोखाधड़ी के कुल 1,65,782 आर्थिक अपराध पंजीबद्ध किए गए, जो वाकई पुलिस एवं सुरक्षा एजेंसियों के लिए गहन चिंता का विषय हैं।

11. क्रिप्टोजेकिंग (Cryptojacking)

क्रिप्टोजेकिंग को समझने से पहले हमें क्रिप्टोकरेंसी और क्रिप्टोमाईनिंग को समझना होगा।

क्रिप्टोकरेंसी- हमने अब तक पैसों यानि करेंसी को कई रूपों में देखा है, जैसे भारत में रुपये, अमेरिका में डॉलर, ब्रिटेन में पॉण्ड, यूरोप में यूरो आदि। ये सभी मुद्राएं या करेंसी भौतिक रूप में यानि कागज के नोट व सिक्कों के रूप में होती हैं, जिन्हें हम हाथ से छू सकते हैं और अपनी जेब में रख सकते हैं। हम दुनिया में जहाँ कहीं भी जाते हैं, हमें वहीं की मुद्रा या करेंसी का इस्तेमाल करना होता है। लेकिन साइबर जगत में एक और ऐसी करेंसी है जो पूरी दुनिया के लिए एक है। डिजिटलाइजेशन के इस दौर में दुनिया भर में इंटरनेट के नेटवर्क पर चलने वाली यूनिवर्सल डिजिटल करेंसी ही क्रिप्टोकरेंसी कहलाती है, जिसे हम देख नहीं सकते हैं या छू नहीं सकते, किन्तु आज के समय में यही सबसे मूल्यवान करेंसी बन गई है। यह क्रिप्टोकरेंसी है बिटकॉइन। 2009 में जब बिटकॉइन लॉन्च हुई थी तो इसकी कीमत 0.060 रुपये थी। तब भारत में सोने की कीमत 14500 रुपये प्रति 10 ग्राम थी। आज एक बिटकॉइन की कीमत 48 लाख रुपये के पार पहुंच चुकी है जबकि सोना 46 हजार रुपये प्रति 10 ग्राम के आसपास मंडरा रहा है। दुनिया की पहली विकेन्द्रीकृत करेंसी बिटकॉइन की कीमत

इन 12 सालों में बहुत तेजी से बढ़ी है।[6] यह एक विश्वव्यापी क्रिप्टो करेंसी है जो डिजिटल भुगतान प्रणाली पर चलती है। ऐसा कहा जा सकता है कि यदि इंटरनेट किसी जगह का नाम होता तो क्रिप्टोकरेंसी यानी बिटकॉइन वहाँ की राष्ट्रीय करेंसी है। भारत में यह डिजिटल करेंसी पूरी तरह से गैरकानूनी है, अर्थात भारतीय सरकार द्वारा इसे मान्यता नहीं दी गई हैं।

- **क्रिप्टोमाइनिंग** – क्रिप्टोकरेंसी बिटकॉइन बनाने की प्रक्रिया को क्रिप्टोमाइनिंग कहा जाता है। यह एक प्रतिस्पर्धी और विकेन्द्रीयकृत प्रकिया है, जिसके तहत बिटकॉइन को जनरेट किया जाता है। बिटकॉइन प्रोटोकॉल के मुताबिक सीमित मात्रा में ही इनकी माइनिंग की जा सकती है। बिटकॉइन बनाने की प्रक्रिया एक प्रतिस्पर्धी व्यवसाय है। जैसे-जैसे माइनर्स की संख्या बढ़ती है बिटकॉइन से मुनाफा कमाना कठिन होता जाता है। किसी भी सरकार या पदाधिकारी के पास ऐसी कोई शक्ति नहीं होती कि वह बिटकॉइन

6 https://navbharattimes.indiatimes.com/business/commodity/one-bitcoin-is-now-more-precious-than-1-kg-gold/articleshow/82067079.cms?story=4

से मुनाफे को बढ़ाने के लिए सिस्टम को नियंत्रित कर सके। इसकी माइनिंग निर्धारित होती है। माइनिंग बुनियादी तौर पर ऐसी प्रक्रिया है जिसके माध्यम से किसी आभासी मुद्रा के लेन-देन को सत्यापित किया जाता है। कुल 21 मिलियन बिटकॉइन्स ही माइन किए जा सकते हैं और अब तक तकरीबन 16 मिलियन बिटकॉइन माइन किए जा चुके हैं।

- **क्रिप्टोजेकिंग -** क्रिप्टोजैकिंग' एक प्रकार का साइबर हमला है, जिसका इस्तेमाल हैकर्स क्रिप्टोकरेंसी की माइनिंग (Mining) करने के लिये करते हैं। क्रिप्टोजैकिंग में इंटरनेट सर्वर, निजी कंप्यूटर या फिर स्मार्टफोन में मैलवेयर इंस्टाल कर क्रिप्टोकरेंसी की माइनिंग की जाती है।

12. साइबर आतंकवाद (Cyber Terrorism)

आतंकवाद से हम सभी भली-भांति परिचित है क्योंकि पिछले कई दशकों से भारत इसका दंश झेलता आया है और देश के सुरक्षा बलों ने इसका हर मोर्चे पर डट कर मुकाबला किया। सबसे पहले पूर्वोत्तर, फिर पंजाब और फिर जम्मू-कश्मीर में अपने पैर पसारने वाली आतंकवाद की इस समस्या पर भारत सुरक्षा बलों की साहसिक कोशिशों के चलते नियंत्रण कर पाया है और कई स्थानों से आतंकवाद का समूल नाश हो चुका है। लेकिन आज भी देश के कुछ इलाकों में और कभी-कभी महत्वपूर्ण स्थानों पर आतंकवाद का भयावह चेहरा सामने आ जाता है। किन्तु साइबर आतंकवाद इस पारम्परिक आतंकवाद से बिल्कुल भिन्न है।

आज के युग में रोजमर्रा की कार्यप्रणाली में साइबर जगत का दायरा उत्तरोत्तर बढ़ता ही जा रहा है । सरकारों द्वारा प्रशासन, वित्त, शिक्षा,

व्यवसाय, नाभिकीय व परमाणु ऊर्जा, अंतरिक्ष अनुसंधान सहित सभी प्रमुख क्षेत्रों के विकास में कम्प्यूटर तथा सूचना व संचार प्रौद्योगिकी का बढ़-चढ़कर इस्तेमाल किया जा रहा हैं। इसके अलावा देश की बहुत सी व्यवस्थाएं आज कम्प्यूटर एवं सूचना प्रौद्योगिकी पर आश्रित हो गई हैं, जैसे- हवाई यातायात, रेलवे, बैंकिंग, चिकित्सा-व्यवस्था आदि। और तो और दुनिया के देशों के सैन्य-प्रतिष्ठानों और सुरक्षा बलों का काम-काज तथा प्रशासन भी कम्प्यूटर नेटवर्क के साथ जुड़ चुका है । अब जरा सोचें कि जब एक छोटे से वायरस, कम्प्यूटर वॉर्म या रेनसमवेयर के हमले से हमारे कम्प्यूटर या नेटवर्क की पूरी व्यवस्था चरमरा सकती है तो उन बड़ी-बड़ी कम्प्यूटर आधारित प्रणालियों का क्या होगा, जिन पर देश का पूरा दारोमदार निर्भर है। निसंदेह, कम्प्युटरीकरण और सूचना व संचार क्रांति के इस युग में आतंकवादी भी इसके प्रयोग में किसी से पीछे नहीं हैं। वे न केवल इन माध्यमों से अपने आंतकी मनसूबों का प्रचार-प्रसार करते हैं, बल्कि संशय, कौतुहल और अशांति फैलाने के लिए सोशल मीडिया का भी प्रयोग करते हैं और अपने साथियों की भर्ती के लिए भी इसका भरपूर लाभ लेते हैं। दरअसल, जब आतंकवादी विध्वंस फैलाने के लिए भौतिक हथियारों जैसे- बंदूक, गोला-बारूद या विस्फोटकों के स्थान पर साइबर जगत एवं उससे जुड़े संसाधनों का इस्तेमाल करने लगते हैं तो ऐसे आतंकवाद को ही साइबर आतंकवाद कहा जाता है।

साइबर आतंकवाद दुनिया भर में अनेकों बार अपना घिनौना चेहरा दिखा चुका है। इसका एक हालिया उदाहरण हमें उस समय देखने को मिला था, जब पूर्वी लद्दाख में सीमा पर जारी तनाव के बीच चीन ने साइबर अटैक कर देशभर में बिजली आपूर्ति ठप करने की साजिश रची थी। चीन चाहता था कि भारत डर जाए और सीमा पर ज्यादा आक्रामक रवैया न अपनाए। चीन ने अपने हैकर्स समूह रेड इको के

जरिए भारत के बिजली तंत्र पर मालवेयर शेडो पैड के जरिए यह हमला किया था। इस संबंध में हाल ही प्रकाशित एक रिपोर्ट के अनुसार विद्युत मंत्रालय ने बताया था कि इस हमले के बाद राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना सुरक्षा केंद्र (एनसीआईआईपीसी) ने 12 फरवरी 2021 को एक ईमेल के जरिए सूचित किया था कि चीन समर्थित हैकर्स समूह रेड इको ने भारत के क्षेत्रीय बिजली वितरण केंद्रों व राज्य वितरण केंद्रों के सिस्टम में मालवेयर वायरस भेजकर इसे ठप्प करने की साजिश रची थी। वहीं मुम्बई बिजली गुल काण्ड में भी चीन का ही हाथ था।[7]

साइबर आतंकवाद को सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 66 एफ में कुछ इस प्रकार परिभाषित/समावेशित किया गया है-

" (1) यदि कोई-

7 https://www.amarujala.com/india-news/chinas-cyber-attack-conspiracy-was-to-create-electricity-crises-in-entire-country-along-with-mumbai-cert-had-warned

(अ) भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को भंग करने या इसके निवासियों को आतंकित करने के लिए-

(क). किसी अधिकृत व्यक्ति को कंप्यूटर के इस्तेमाल से रोकता है या रोकने का कारण बनता है।

(ख) बिना अधिकार के या अपने अधिकार का अतिक्रमण कर जबरन किसी कंप्यूटर के इस्तेमाल की कोशिश करता है।

(ग) कंप्यूटर में वायरस जैसी कोई ऐसी चीज डालता है या डालने की कोशिश करता है, जिससे लोगों की जान को खतरा पैदा होने की आशंका हो या संपत्ति के नुक़सान का ख़तरा हो या जीवन के लिए आवश्यक सेवाओं में जानबूझ कर खलल डालने की कोशिश करता हो या धारा 70 के तहत संवेदनशील जानकारियों पर बुरा असर पड़ने की आशंका हो या-

(आ) अनाधिकार या अधिकारों का अतिक्रमण करते हुए जानबूझ कर किसी कंप्यूटर से ऐसी सूचनाएं हासिल करने में कामयाब होता है, जो देश की सुरक्षा या अन्य देशों के साथ उसके संबंधों के नज़रिए से संवेदनशील हैं या कोई भी गोपनीय सूचना इस इरादे के साथ हासिल करता है, जिससे भारत की सुरक्षा, एकता, अखंडता एवं संप्रभुता, अन्य देशों के साथ इसके संबंध, सार्वजनिक जीवन या नैतिकता पर बुरा असर पड़ता हो या ऐसा होने की आशंका हो, देश की अदालतों की अवमानना अथवा मानहानि होती हो या ऐसा होने की आशंका हो, किसी अपराध को बढ़ावा मिलता हो या इसकी आशंका हो, किसी विदेशी राष्ट्र अथवा व्यक्तियों के समूह अथवा किसी अन्य को ऐसी सूचना से फायदा पहुंचता हो, तो उसे साइबर आतंकवाद का आरोपी माना जा सकता है।

(2) यदि कोई व्यक्ति साइबर आतंकवाद फैलाता है या ऐसा करने की किसी साजिश में शामिल होता है तो उसे आजीवन कारावास की सजा सुनाई जा सकती है।"

☞ राष्ट्रीय अपराध रिकॉर्ड ब्यूरो के वार्षिक रिपोर्ट के अनुसार वर्ष 2019 के दौरान देश में साइबर आतंकवाद के कुल 12 मामले दर्ज किए गए। वस्तु: साइबर आतंकवाद को लेकर भारत की सभी सुरक्षा एजेंसियां और अन्य संबद्ध संगठन बहुत ही सजग व सर्तक है और समर्पित होकर कार्य कर रहे हैं।

समग्रतया यह स्पष्ट है कि भारत में कानूनी स्तर पर प्रत्येक प्रकार के साइबर अपराध को परिभाषित किया गया है और उसके लिए दण्ड का प्रावधान मौजूद है। हालांकि साइबर अपराधों के मामलों की संख्या में हर वर्ष तेज बढ़त दर्ज की जा रही है, किन्तु पुलिस और सुरक्षा एजेंसियां इन अपराधों के अन्वेषण के लिए प्रक्रियावत कार्रवाई भी सुनिश्चित कर रही हैं। सूचना व संचार क्रांति के इस दौर में साइबर अपराधों को रोकने के लिए सभी राज्यों में सक्रिय कम्यूनिटी पुलिसिंग की सख़्त आवश्यकता है। यानी साइबर अपराधों को रोकने के लिए पुलिस को न केवल अन्वेषण की गति बढ़ानी होगी, बल्कि समाज में अपनी गतिविधियां और ज्ञानवर्द्धक कार्यक्रमों के जरिये जागरूकता फैलाने के अभिनव प्रयास करने होंगे।

अध्याय 9

भारत में साइबर अपराध अन्वेषण में पुलिस की सफलताएं

मनुष्य एक सामाजिक प्राणी है और समाज संसार की वह व्यवस्था है, जिसमें सदाचार और दुराचार दोनों साथ-साथ पनपते हैं। कानून समाज की वह शक्ति है, जिसके बिना स्वस्थ्य व समृद्ध समाज के अस्तित्व की कल्पना संभव नहीं है। यानी, समाज यदि शरीर है तो कानून उसकी रोग-प्रतिरोधक-क्षमता(Immunity) है। कानून समाज को अपराधों और दूसरे नुकसानदेह ख़तरों से बचाने में सबसे महत्वपूर्ण भूमिका निभाता है। पुलिस कानून की संरक्षक है और अपराधों की जांच व अन्वेषण पुलिस के कार्यक्षेत्र से जुड़े वो सबसे अहम कर्तव्य हैं, जो सीधे तौर पर पुलिस के प्रभावशाली अस्तित्व पर असर डालते हैं। पुलिस यदि अपराधों की जांच और अन्वेषण के कार्य में पूरी तरह सक्षम व समर्थ हो और उसकी कार्यप्रणाली दक्षता से भरी हो तो न केवल अपराधियों पर कानून का शिकंजा कसता है, बल्कि उनके हौसले भी पस्त होते है और फिर निश्चित रुप से समाज में पुलिस की सकारात्मक एवं विश्वसनीय छवि कायम होती है।

सामाजिक व्यवस्था में न केवल सकारात्मक योगदान देने वाले तत्व शामिल होते हैं, बल्कि इसके भीतर ही इसे नुकसान पहुंचाने वाली ताकतें यानी असामाजिक तत्व एवं आपराधिक प्रवृत्तियां भी मौजूद होती हैं। अपराधों का मूल मनोवृत्तियों में छिपा होता है और मनोवृत्तियां सामाजिक, सांस्कृतिक, आर्थिक, राजनैतिक, शैक्षणिक, धार्मिक, भौतिक, प्राकृतिक एवं वैज्ञानिक प्रभावों से प्रेरित व ग्रसित हो सकती हैं। आधुनिक परिवेश में समाज के भीतर मानव, वस्तुएं और कार्यकलाप सभी कुछ कम्प्यूटर और सूचना व संचार

प्रौद्योगिकी से प्रभावित है, ऐसे में अपराधिक प्रवृत्तियां भला इन प्रभावों से कैसे अछूती रह सकती हैं। सभ्यता के विकास के साथ समाज उन्नत हुआ है और समाज के विकास के साथ ही इसमें पनपने वाले अपराधों ने भी आधुनिक परिवेश में नया और पहले से ज्यादा भयावह रूप धारण किया है। कम्प्यूटर और सूचना व संचार प्रौद्योगिकी का लाभ न केवल आम नागरिकों और विधि-प्रवर्तक एजेंसियों को मिला है, बल्कि अपराध जगत ने भी इसका जम कर लाभ उठाया है। यहां यह कहना भी अतिश्योक्ति नहीं होगा कि सूचना व संचार प्रौद्योगिकी का जितना लाभ समाज ने नहीं उठाया, उससे कहीं ज्यादा इसका दुरूपयोग अपराध जगत में देखने का मिला है। साइबर अपराध इन्हीं उन्नत होती आपराधिक प्रवृत्तियों का परिणाम हैं।

राष्ट्रीय अपराध रिकॉर्ड ब्यूरो के विगत तीन वर्ष (यानी वर्ष 2017,2018,2019) के आंकड़ों के अनुसार इन तीन वर्षों में उत्तर प्रदेश में सबसे ज्यादा अर्थात 22,667 साइबर अपराध दर्ज किए गए, जबकि कर्नाटक में 21,033 मामले और और महाराष्ट्र में 12,082 मामले दर्ज किए गए। अकेले वर्ष 2019 की यदि बात की जाए तो बंगलूरू में सबसे ज्यादा 10,555 साइबर अपराध, मुम्बई में 2,527 साइबर अपराध और हैदराबाद में 1,347 साइबर अपराध के मामले दर्ज किए गए। चिंताजनक बात यह है कि अन्य महानगरों और छोटे शहरों में भी साइबर अपराध के मामले घटने का नाम नहीं ले रहे। वर्ष 2019 में जयपुर में 544, कानपुर में 365, गाजियाबाद में 347, पूणे में 309 और पटना में 202 साइबर अपराध घटित हुए।

विगत वर्षों में विभिन्न पुलिस विभागों ने साइबर अपराध के मामलों में कुछ अनुकरणीय सफलाएं अर्जित की हैं, जो पुलिस कर्मियों को बढ़ते साइबर अपराध के मामलों से जूझने के लिए प्रेरणा और प्रोत्साहन प्रदान करती हैं। जिस गति से देश में साइबर अपराध बढ़ रहे हैं और लम्बित प्रकरणों की संख्या में बढ़ोत्तरी हो रही है, उसे देखते हुए पुलिस को मिली ऐसी

सफलताएं निसंदेह इस बात परिचायक हैं कि यदि साइबर अपराधी अपनी करतूतों से बाज़ नहीं आ रहे हैं, तो पुलिस भी उनका पीछा नहीं छोड़ रही है। यहां कुछ ऐसी ही अनुकरणीय मिसालों का जिक्र किया जा रहा है जो साइबर अपराधों के अन्वेषण की राह में मील का पत्थर बन कर उभरी हैं-

1) **बंगलूरु साइबर पुलिस थाने ने 15 दिनों में 400 साईबर अपराध के मामले निपटाए[1] :**

बंगलूरु देश का वह शहर है, जिसे वर्ष 2001 में देश का सबसे पहला साइबर पुलिस थाना स्थापित करने का श्रेय जाता है। जनवरी-फरवरी 2020 से पहले यहां लगभग 16,000 साइबर अपराध के मामले लम्बित थे। इस बीच बैंगलूरु पुलिस ने अपने 8 पुलिस जिलों के लिए एक-एक साइबर-इकोनॉमिक-नारकोटिक (सीईएन) स्टेशन की स्थापना की। ये सभी विशेष पुलिस स्टेशन बंगलूरु में साइबर अपराधों, आर्थिक अपराधों और नशीली दवाओं की तस्करी संबंधी मामलों से निपटने के लिए समप्पित रूप से कार्य करने हेतु स्थापित किए गए। इससे पहले बंगलूरु महानगर में केवल एक ही साइबर पुलिस थाना स्थापित था।

1 https://www.newindianexpress.com/cities/bengaluru/2020/feb/09/400-cybercrime-cases-cleared-in-15-days-2101091.html

जैसे ही समर्पित सीईएन स्टेशनों ने काम करना शुरू किया, बंगलूरू के साइबर पुलिस थाने ने ऐसी तेजी दिखाई कि मात्र 15 दिनों की अवधि में साइबर अपराध के 400 मामले सुलझा कर रख दिए। जबकि वर्ष 2019 के पूरे वर्ष में 1000 मामले निपटाए जा सके थे। इसका मूल कारण यह था कि सीईएन के गठन के बाद बंगलूरू का साईबर पुलिस थाना केवल लम्बित मामलों के निपटान में जुट गया था, जबकि नए मामले अलग-अलग क्षेत्रों में स्थापित सीईएन स्टेशनों द्वारा दर्ज किए जा रहे थे। इस जीवंत उदाहरण से स्पष्ट होता है यदि साईबर अपराधों के लिए हर नगर में एक समर्पित पुलिस थाना या पूरी तरह से समर्पित व सुप्रशिक्षित टीम हो तो साइबर अपराधों के अन्वेषण में तेजी से सफलताएं मिलना निश्चित है।

2) गुजरात पुलिस ने किया रेलवे की फर्जी भर्ती वेबसाइट का पर्दाफाश[2] :

साइबर अपराधियों के एक शातिर गिरोह द्वारा रेलवे की एक नकली वेबसाइट बना कर देश भर के बेरोजगारों को ठगने का एक सनसनीखेज मामला गुजरात पुलिस ने उजागर किया है। ये अपराधी रेलवे की फर्जी वेबसाइट बना कर बेरोजगारों से करोड़ो रूपए की ठगी कर रहे थे। पुलिस के मुताबिक इन अपराधियों ने रेलवे की एक फर्जी वेबसाइट बना कर भर्ती के लिए आवेदन पत्र आमंत्रित किए थे। और तो और अभ्यर्थियों की ऑनलाईन परीक्षा लेकर उनका परीक्षा परिणाम भी घोषित किया और उन्हें नियुक्ति पत्र भेज कर उनकी ऑनलाईन ट्रेनिंग भी करा दी। रिपोर्ट के अनुसार प्रत्येक अभ्यर्थी से इन साइबर अपराधियों द्वारा 15-15 लाख रूपए वसूल किए गए थे। इस

2 https://navbharattimes.indiatimes.com/metro/lucknow/crime/the-fake-website-of-the-railway-in-lucknow-exposed-the-gang-cheating-in-the-name-of-job/articleshow/81896010.cms

गिरोह का पर्दाफाश गुजरात पुलिस को साइबर अपराधों के क्षेत्र में मिली बड़ी सफलताओं में से एक है।

3) मध्य प्रदेश पुलिस ने बीमा पॉलिसी के नाम पर लाखों की ठगी करने वाले आरोपियों को पकड़ा[3] :

मध्य प्रदेश पुलिस मुख्यालय की साइबर सेल ने अप्रैल 2021 में बंद इंश्योरेन्स पॉलिसी के नाम पर एक सेवानिवृत्त व्यक्ति से लाखों की ठगी करने वाले गिरोह का पर्दाफाश किया है। पुलिस ने इस मामले में कानपुर और दिल्ली से चार आरोपियों का गिरफ्तार करने में सफलता प्राप्त की है, जिन्होंने एक बंद इंश्योरेन्स पॉलिसी को दोबारा चालू करवा कर ज्यादा लाभ दिलाने का लालच देते हुए एक व्यक्ति से पिछले 3-4 सालों में 40 लाख की ठगी की थी। जारी प्रेस विज्ञप्ति के अनुसार ये चारों आरोपी वित्तीय संस्थानों की कार्यप्रणाली का अनुभव रखते थे और दिल्ली में एक दवाई कंपनी की आड़ में बीमा

3 https://twitter.com/mpcyberpolice/status/1382982100731629568/photo/1

पॉलिसियों के जरिये धोखाधड़ी का एक कॉल सेंटर चला रहे थे। इन आरोपियों के पास से 20,000 बीमा पॉलिसियों का डाटा बरामद हुआ है। अभी इस मामले की विवेचना जारी है, क्योंकि ठगी की रकम करोड़ो में हो सकती है। इसीलिए मध्य प्रदेश पुलिस द्वारा मामले से जुड़ी सूचनाएं दूसरे राज्यों से भी साझा की गई है, ताकि इस बड़े गिरोह के गोरखधंधे के विस्तार का सही-सही पता चल सके।

4) साइबराबाद पुलिस द्वारा फर्जी पासपोर्ट गैंग का पर्दाफाश[4] :

हैदाराबाद की साइबराबाद पुलिस ने फर्जी तरीके से पासपोर्ट बनाने के एक गिरोह का पर्दाफाश किया है। पुलिस ने गिरोह में शामिल 2 पुलिस अधिकारियों और 4 बांग्लादेशियों समेत कुल 8 लोगों को गिरफ्तार किया है। यह मामला तब सामने आया जब हैदाराबाद एयरपोर्ट से 3 बांग्लादेशी युवक दुबई के लिए विमान में बैठने वाले थे। इमीग्रेशन विभाग को शक हुआ तो उन्होंने साइबराबाद पुलिस को सूचित किया, जिसके बाद साइबराबाद पुलिस ने जांच-पड़ताल शुरु की तो फर्जी पासपोर्ट बनाने वाले गिरोह का रहस्य खुल कर

4 https://www.indiatv.in/crime/bangladeshi-fake-passport-gang-busted-in-hyderabad-2-police-officers-also-arrested-774261

सामने आ गया। जानकारी के अनुसार बांग्लादेश में रहने वाले चार संदिग्धों ने अपने फर्जी आधार कार्ड बनवा लिए थे, जिसमें इन तीनों को निज़ामाबाद जिले के बोधन शहर का रहने वाला बताया गया था। इस गिरोह में दो पुलिस कर्मी भी शामिल थे, जिन्होंने 72 लोगों के नकली पासपोर्ट बनाने में मदद की थी। पुलिस ने इस सफलता के बाद 72 लोगों के फर्जी पासपोर्ट रद्द करने की पहल कर दी है।

5) भोपाल साइबर सेल द्वारा स्टॉक मार्केट के नाम पर ठगी करने वाले गिरोह का भंडाफोड़[5]:

भोपाल पुलिस की साइबर अपराध शाखा ने लोगों को स्टॉक मार्केट में निवेश के जरिए ज्यादा मुनाफा कमाने का झांसा देकर ठगी करने वाले एक गिरोह का पर्दाफाश किया है। इस मामले में चार आरोपियों को गिरफ्तार किया गया है। इन आरोपियों द्वारा लोगों को ठगने के

5 https://www.naidunia.com/madhya-pradesh/bhopal-four-accused-arrested-for-cheating-gang-by-pretending-to-invest-in-stock-market-6713600

लिए बकायदा एक कॉल सेंटर होशंगाबाद जिले के देहात थाना क्षेत्र में चलाया जा रहा था, जहां 28 लड़कियां और 12 लड़के ग्राहकों से बात करने के लिए नौकरी पर रखे गए थे। इन्हें ग्राहकों को फांसने के लिए रोजाना 500 कॉल करने का टारगेट दिया जाता था। कार्यालय को चलाने के लिए हर महीने तीन लाख रुपये खर्च किए जा रहे थे। प्रारंभिक जांच में पता चला है कि पिछले एक साल में ये आरोपी करीब 1 करोड़ की ठगी कर चुके हैं। सूत्रों के अनुसार मामले की शिकायत कर्नाटक के एक व्यापारी ने की थी। फरियादी ने बताया कि ग्लोबल एस.एन.सी. नामक स्टॉक मार्केट कंपनी से फोन पर संपर्क किया गया। बातचीत करने पर बताया गया कि स्टॉक मार्केट में निवेश करने पर ज्यादा मुनाफा मिलेगा। व्यापारी ने फोन पर बात करने वाली युवती की बातों में आकर कंपनी के बैंक खातों में कुल 2 लाख 20 हजार रुपये जमा करवाए थे। कुछ दिनों बाद उन्हें कहा गया कि शेयर मार्केट में गिरावट के कारण उनका पैसा डूब गया है। इस पर फरियादी ने शिकायत दर्ज कराई थी और पुलिस ने अज्ञात आरोपियों के खिलाफ दर्ज करते हुए जांच शुरू कर दी थी।

6) दिल्ली पुलिस द्वारा फर्जी आधार कार्ड बनाकर कारोबारियों के खातों से करोड़ों की ठगी का पर्दाफाश[6]:

नई दिल्ली सेंट्रल जिले की साइबर सेल ने कारोबारियों के खातों में सेंध लगाकर करोड़ों की ठगी करने वाले गिरोह का पर्दाफाश किया है। पुलिस ने गिरोह के सरगना समेत चार बदमाशों को पकड़ा है। सूत्रों के अनुसार आरोपी फर्जी आधार कार्ड बनाकर कारोबारियों के खाते से अटैच मोबाइल नंबरों के डुप्लीकेट सिम कार्ड निकलवा लेते थे। पीड़ितों को जब तब इसका पता चलता था तब तक आरोपी उनके खातों से रकम निकाल लेते थे। पूछताछ में आरोपियों ने खुलासा किया कि वे लोग गुरुग्राम में एक कारोबारी के खाते से 1 करोड़ 50 लाख और वडोदरा (गुजरात) के कारोबारी के खाते से 50 लाख, आजमगढ़(उ.प्र.) के कारोबारी के खाते से 28 लाख और दिल्ली के एक कारोबारी के खाते से 30 लाख रुपये निकाल चुके हैं। जांच में यह भी पता चला कि यह गिरोह पहले लोगों के खातों की जानकारी जुटा लेते थे, फिर उनके नकली आधार कार्ड बनवाते थे और फिर

6 https://www.haribhoomi.com/local/delhi-ncr/money-fraudsters-arrested-from-bank-accounts-362747

नकली आधार कार्ड के दम पर लोगों की डुप्लीकेट सिम प्राप्त कर लेते थे। सिम पर आने वाले ओटीपी के जरिये रकम अलग-अलग खातों में ट्रांसफर कर दी जाती थे। आरोपियों ने ये अलग-अलग खाते ग्रामीणों को नौकरी का झांसा देकर खुलवाए और बाद में उनकी कमाण्ड अपने हाथ में ले ली थी, जिनके जरिये वे इस फर्जीबाड़े को अंजाम देते थे।

7) उत्तराखण्ड पुलिस को ओ.एल.एक्स ठगों को पकड़ने में सफलता मिली[7]:

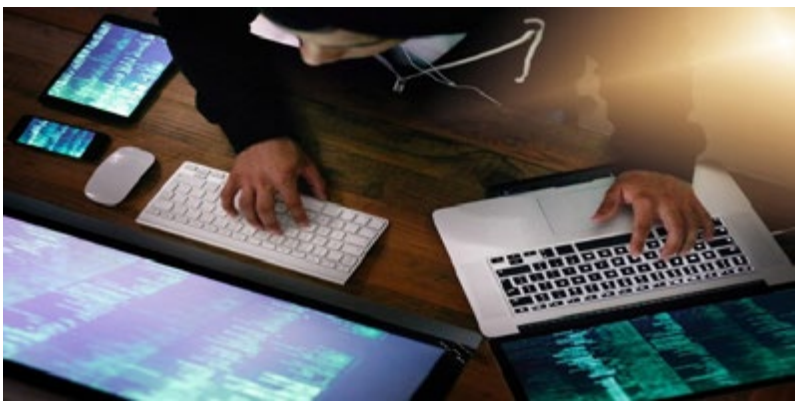
उत्तराखण्ड की एसटीएफ को उस समय एक बड़ी सफलता हाथ लगी जब उन्होंने राजस्थान के मेवात से 2 ऐसे ठगों को गिरफ्तार किया जो खुद को फौजी बता कर ओ.एल.एक्स पर सामान बेचने के बहाने अलग-अलग राज्यों के लोगों को लाखों का चूना लगा रहे थे। इस मामले में उत्तराखण्ड पुलिस ने राजस्थान के मेवात से

7 https://react.etvbharat.com/hindi/uttarakhand/state/dehradun/uttarakhand-stf-has-caught-two-cyber-thugs-cheating-people-through-olx/uttarakhand20210317133526247

मास्टरमाइंड सहित दो शातिर साइबर अपराधियों को गिरफ्तार किया है। गिरफ्तार किए गए साइबर अपराधियों ने ऋषिकेश में एक व्यक्ति को कार बेचने के नाम पर 1 लाख 43 हजार का चूना लगाया। आरोपियों द्वारा ये रकम ऑनलाइन लेनदेन के जरिये हथिया ली गई। ये आरोपी ओएलएक्स पोर्टल के माध्यम से पूरे भारत में भारी संख्या में लोगों को सामान बेचने के नाम पर अब तक लाखों रुपए की ठगी की घटनाओं को अंजाम दे चुके हैं। दोनों आरोपी खुद को भारतीय सेना में सेवारत बता कर लोगों को गुमराह करते थे और सस्ते दामों में कार बेचने के नाम पर लालच देकर लोगों की गाढ़ी कमाई पर ऑनलाइन लेनदेन के जरिये हाथ साफ कर जाते थे ।

8) उत्तराखण्ड पुलिस द्वारा अंतराष्ट्रीय साइबर गिरोह का पर्दाफाश[8]:

स्पेशल टास्क फोर्स ने एक बहुत बड़े अंतरराष्ट्रीय साइबर अपराध नेटवर्क के मास्टरमाइंड को गिरफ्तार करने में सफलता हासिल की है।इसके साथ ही इस अंतरराष्ट्रीय साइबर अपराध गिरोह का पर्दाफाश हो गया है। यह गिरोह अमेरिकी नागरिकों सहित अन्य



8 https://react.etvbharat.com/hindi/chhattisgarh/bharat/international-network-mastermind-arrested-for-making-american-citizen-a-victim-of-cybercrime/na20210408191805193

विदेशी लोगों को विदेश में डॉलर में पेमेंट देने, अवैध धन से सम्पत्ति में निवेश करने और करोड़ों रूपए के बैंकिंग लेनदेन करने जैसे लालच देकर साइबर ठगी करता था। इस गिरोह के तथाकथित मास्टरमांइड का कई बैंकों में करोड़ो रूपए जमा है और बेशकीमती संपत्ति भी है, जबकि उसकी उम्र महज 28 वर्ष है। सूत्रों के मुताबिक इस गिरोह का असली सरगना 2020 में अमेरिका में गिरफ्तार किया जा चुका है। ऐसे में देहरादून सहित देश भर में साइबर अपराध में लिप्त इस गिरोह के कॉल सेंटर बंद कर दिए गए थे और वर्तमान में एक वर्चुअल नंबर से अंतरराष्ट्रीय स्तर पर साइबर अपराधों को अंजाम दिया जा रहा था। गिरोह का मास्टरमांइड पहले अमेरिका के टेक्सॉस में एक कॉलेज में पढ़ा करता था। सूत्रों के अनुसार भारत से संचालित गिरोह के नेटवर्क द्वारा विदेशों में रह रहे लोगों, खास तौर पर अमेरिकी नागरिकों को विभिन्न तरह की सेवाएं देने और कम्प्यूटर को वायरस से बचाने के नाम पर ठगा जा रहा था। गोपनीय सूचनाओं के आधार पर एसटीएफ की एक पूरी टेक्निकल टीम द्वारा पिछले 2 माह से इस गिरोह से जुड़ी सूचनाओं और सुबूतों को एकत्र किया जा रहा था।

9) नेपालियों के फर्जी आधार कार्ड व बैंक खाते से साइबर अपराधों का भंडाफोड़[9] :

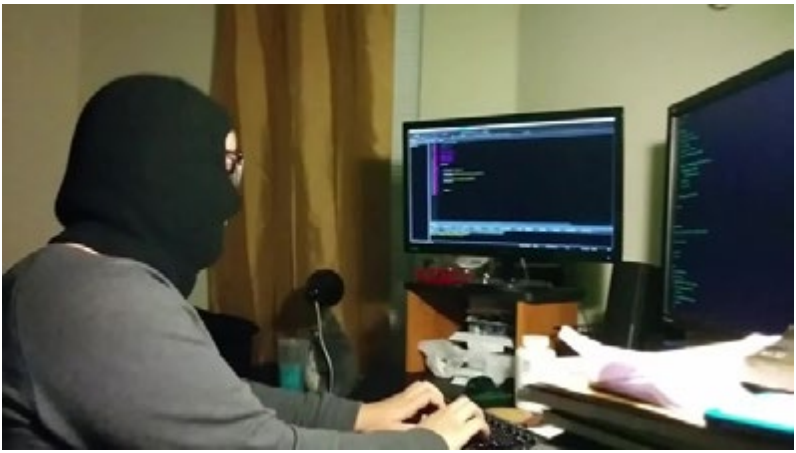
उत्तर प्रदेश में नोएडा पुलिस ने साइबर अपराधियों के एक ऐसे गिरोह का पर्दाफाश किया है, जिसमें 1 महिला एवं 2 पुरुष अंतरराष्ट्रीय एवं अंतरराज्यीय स्तर पर साइबर एवं अन्य प्रकार के अपराधों को अंजाम दे रहे थे। सूत्रों के अनुसार आरोपियों के कब्जे से बैंक ऑफ अमेरिका का चैक, दुबई मेट्रो का ट्रैवलिंग कार्ड, ई-स्टाम्प एग्रीमेन्ट, इंडियन

9 https://www.aajtak.in/crime/cyber-crime/story/uttar-pradesh-cyber-fraud-gang-busted-in-noida-by-up-police-women-arrested-to-1227279-2021-03-24

नॉन ज्यूडिशियल- व्यक्तियों को विदेश भेजने संबंधी 5 दस्तावेज, 18 फर्जी आधार कार्ड, 18 फर्जी पैन कार्ड, 21 चैक बुक, 7 पासपोर्ट, 2 घरेलू गैस कार्ड, 7 दिल्ली मैट्रो ट्रैवलिंग कार्ड, 4 एटीएम कार्ड, 2 भारतीय मतदाता परिचय पत्र, 3 नेपाली नागरिकता प्रमाण-पत्र, 1 लैपटॉप, 1 डोंगल, 500 जीबी हार्ड डिस्क, 3 नए सिम कार्ड, 1 नेपाली सिम कार्ड, 11 मोबाइल फोन एवं अन्य कई दस्तावेज व विदेशी करेंसी बरामद की गई हैं। जांच में पता चला कि ये आरोपी नेपाल से भोले-भाले गरीब लोगों को म्यूजिक कन्सर्ट या अन्य किसी काम के बहाने से भारत ले आते थे तथा उनके असली नाम को बदल कर नकली नाम से आधार कार्ड व पैन कार्ड दिल्ली के मुनरिका से बनवाते थे।

इन आधार कार्डों के जरिये ये लोग अलग-अलग कम्पनियों के सिम कार्ड खरीदते थे तथा आधार कार्ड व पैन कार्ड के जरिये नेपालियों के खाते बैंको में खुलवाते थे। ये सारा काम होने के बाद ये आरोपी उन लोगों को 25 हजार रूपए देकर वापस नेपाल भेज देते थे तथा उनके द्वारा लिए गए मोबाइल नम्बरों एवं बैंक खातों के माध्यम से साइबर अपराधों को अंजाम देते थे। इन आरोपियों के खिलाफ मानव तस्करी और बैंक अकाउंट हैकिंग के कुछ संभावित मामलों की भी छानबीन की जा रही है।

10) पाकिस्तान की मदद से भारत की 500 वेबसाइट हैक करने वाले अपराधी गिरफ्तार[10] :



वर्ष 2018 में दिल्ली पुलिस की स्पेशल सेल ने देश की वेबसाइट हैक करने के मामले में पाक समर्थित दो कश्मीरी छात्रों को गिरफ्तार किया था। ये दोनों अपराधी अलग-अलग संस्थानों से बी.टेक एवं बीबीए के छात्र थे और दोनों ही पाकिस्तान की खुफिया एजेंसियों के संपर्क में थे। पुलिस के द्वारा दोनों की ऑनलाइन गतिविधियों पर काफी समय से नजर रखी जा रही थी। दोनों पाक समर्थित एवं भारत विरोधी हैकरों से भी जुड़े हुए थे। इन दोनों की गतिविधियां देश विरोधी थीं। ये दोनों 'टीम हैकर्स थर्ड आई' नाम से भारत विरोधी हैकिंग ग्रुप चलाते थे। इस ग्रुप का दावा था कि इन्होंने अब तक पांच सौ से अधिक वेबसाइट हैक की थी। इसके अलावा कश्मीर में अशांति के दौरान जब इंटरनेट आदि पर प्रतिबंध लगाया गया था तो ये आरोपी स्थानीय युवाओं को इससे निपटने के गुर सिखाते थे। इन आरोपियों ने 2017 में अप्रैल से

10 https://www.livehindustan.com/national/story-two-kashmiri-hackers-arrested-for-hacking-500-indian-websites-with-the-help-of-pakistan-1928337.html

मई के दौरान इस तरह का अभियान चलाया था। दोनों युवक पाक समर्थित आतंकवाद के समर्थन में देशद्रोह वाली पोस्ट डाला करते थे।

ये घटनाएं पुलिस को मिली सफलताओं का केवल प्रतिनिधित्व करती हैं। ऐसी ही अनगिनत सफलताएं हर जिले की पुलिस के अतीत में स्वर्णिम अक्षरों से लिखी गई हैं। हालांकि परिस्थितियों और तकनीकी कारणों से कई मामलों में पुलिस को सतत अन्वेषण करते हुए ऐसी ही सफलताओं का लम्बे समय तक इंतजार भी करना पड़ता है, लेकिन इसे पुलिस की असफलता करार नहीं दिया जा सकता, क्योंकि यदि कहीं कोई साइबर अपराध घटित हुआ है तो अपराधी का एक न एक दिन पकड़ा जाना निश्चित है।

पुलिस की सफलताओं की एक झलक दिखाने वाली ये घटनाएं अलग-अलग क्षेत्रो से ली गई है और हर घटना में एक अलग तरह का साइबर अपराध दिखाई देता है। वैसे तो आम तौर पर समाचार-पत्रों में साइबर अपराधों की ऐसी खबरें लगभग रोज पढ़ने को मिल जाती हैं, लेकिन यदि इस प्रकार कई सारे मामलों को एक नजर में देखा जाए तो हमें यह ज्ञात होता है कि साइबर अपराधी जीवन के क्षेत्र में लोगों को त्रस्त करने और ठगने का मौका ढूंढ लेते हैं। साइबर अपराधियों की सबसे बड़ी खासियत ये है कि वे लोगों को अपना शिकार बनाने के लिए उन्हीं मुद्दों को जरिया बनाते हैं, जिनके बारे में वर्तमान में देश व समाज में चहल-पहल मची हुई है। हाल ही में कोविड-19 महामारी के उपचार और वैक्सीन के पंजीकरण के बहाने से की गई धोखाधड़ी इसका जीवंत उदाहरण हैं। कोरोना संकटकाल में वैक्सीन की उपलब्धता से पहले यह देखा गया कि साइबर ठग कोरोना वैक्सीन के नाम पर निजी जानकारियां पूछकर बैंक खातों से रुपए निकाल रहे थे। इससे पहले भी ये ठग नि:शुल्क कोविड टेस्ट कराने और बी.पी. व ऑक्सीजन लेवल

मापने के बहाने मोबाइल में ऐप डाउनलोड करवाकर ठगी कर रहे थे। इस दौरान साइबर ठगी के सबसे बड़े अड्डे डार्क-वेब पर साइबर अपराधी कोरोना वैक्सीन बेचने का दावा भी कर रहे थे। वहां वैक्सीन की डील के दौरान क्रिप्टोकरंसी के जरिए लोगों के पैसे हड़पे जा रहे थे।

सार यह है कि भले ही पुलिस को साइबर अपराधियों की धरपकड़ में काफी हद तक सफलता मिलती दिखाई देती हो, लेकिन अभी भी नित्य-नया रूप लेते साइबर अपराधों को रोकना आसान नहीं है। इसका कारण यही है कि कम्प्यूटर, मोबाइल फोन और सूचना-संचार प्रौद्योगिकी में एक आम आदमी उतना ही जानकार और निपुण होता है, जितनी उसकी जरूरत है। वहीं साइबर अपराधी इन संसाधनों के मन-माफिक प्रयोग में इतना अभ्यस्त हो जाते हैं कि वे कोई भी मुद्दा उठा कर सीमित जानकारी रखने वाली आम जनता को बड़ी ही आसानी से अपना निशाना बना लेते हैं। अब कोविड वैक्सीन वाले मामले को ही ले लीजिए। कोराना महामारी का ये दौर ऐसा था, जब सब जगह लोग वायरस के संक्रमण से घबराए हुए थे और ये भी जानते थे कि सरकार की ओर से कोराना परीक्षण एवं वैक्सीन की मुहिम तेज की जा रही है। ऐसे माहौल में यदि कोई साइबर ठग किसी आम आदमी से कोरोना परीक्षण या कोरोना वैक्सीन के बारे में बात करे तो वह आदमी इस मामले में साइबर ठगी जैसी किसी वारदात के बारे में सोच भी नहीं पाता और उससे पहले ही उसके साथ एक साइबर धोखाधड़ी को अंजाम दे दिया जाता है। पुलिस को ऐसे मामलों की जानकारी तब मिलती है जब अपराध घटित हो चुका होता है। ऐसे में बात फिर वहीं आकर रूक जाती है कि साइबर अपराधियों से बचने के लिए सबसे पहले जनता का जागरूक होना परमावश्यक है। नया पैराग्राफ पुलिस अन्वेषण कर सकती है, जांच कर सकती है, मामले की तह तक पहुंच सकती है, अपराधी को पकड़ सकती है, लेकिन साइबर अपराध को होने से रोकने में केवल वहीं व्यक्ति सक्षम है, जिसे साइबर अपराधियों द्वारा सीधे तौर पर निशाना बनाया जा रहा है। ऐसे में पुलिस एवं प्रशासन का यह अहम

कर्तव्य है कि लोगों को वर्तमान परिस्थितियों के मुताबिक साइबर अपराधों की संभावना से भी बारम्बार आगाह किया जाए। इसके लिए पुलिस को हर बार खास तौर पर यह सोचना होगा कि विद्यमान परिस्थितियों में साइबर अपराधी किस-किस तरह से अपराधों को अंजाम दे सकते हैं, यानी पुलिस को मौजूदा माहौल के मुताबिक शातिर साइबर अपराधियों की करतूतों का पूर्वानुमान लगाना होगा, ताकि जनता को उसी हिसाब से सजग बनाया जा सके। निश्चित रूप से साइबर अपराधों को रोकने के लिए पुलिस द्वारा जनता को जाग्रत बनाए रखना नितांत आवश्यक है।

अध्याय 10

बढ़ते साइबर अपराधों के विरुद्ध पुलिस की तैयारियां

पुलिस का जो स्वरूप आज हमें दिखाई देता है, दरअसल वो अतीत में कई वर्षों के विकासक्रम की देन है। यथार्थ रूप से पूरी दूनिया के देशों में पुलिस सत्ता का वह अंग है, जो शांति और कानून-व्यवस्था कायम रखने और अपराधों की रोकथाम के लिए ही बनाई गई है।

इतिहास पर नजर डालें तो 19 वीं शताब्दी के आरंभ होने से पहले शांति-व्यवस्था और अपराधों की रोकथाम तथा उपद्रवों से जूझने की जिम्मेवारी समुदायों और परिवारों के द्वारा नियुक्त किए गए कुछ निजी चौकीदारों या जनजातीय चौकीदारों के हिस्से हुआ करती थी। जब यूरोप का औपनिवेशीकरण हुआ तो इस प्रकार से निजी स्तर पर रखे जाने वाले चौकीदारों या 'हिफ़ाजती मुलाजिमों' से सुरक्षा का यह काम लिया जाता रहा और यह तरीका तत्कालीन विश्व के कई देशों जैसे चीन, अफ्रिका और दक्षिणी अमेरिका में अपनाया जाने लगा। इसके बाद जब शहरों का विकास हुआ तो कतिपय अव्यवस्थाएं फैलने लगीं, उद्योगों के विकास के साथ कई विवाद उत्पन्न होने लगे, दंगे-फसाद होने लगे, अपराधों ने अपना रूप बदला और ऐसे में स्थानीय आधार पर पुलिस जैसी कई 'रक्षक संस्थाएं' गठित की जाने लगीं।

इतिहास साक्षी है कि पुलिस को संस्थागत रुप से गठित करने की दिशा में यूरोप-महाद्वीप के अनेकों देशों में कई बहुत खास किस्म के प्रयोग हुए और ऐसे नियम-कायदे बनाए गए कि पहले चौकीदारों व निजी सुरक्षा कर्मियों

से लिए जाने वाले सारे काम पुलिस के कार्यक्षेत्र में ला दिए गए। इतना ही नहीं वहां लोक-स्वास्थ्य, पासपोर्ट जारी करने, दूध की शुद्धता जांचने, पुस्तकालय को व्यवस्थित रखने जैसे काम भी पुलिस के सुपुर्द कर दिए गए, क्योंकि अपराधों और अव्यवस्थाओं को रोकना पुलिस के कार्यकलापों का एक अंश मात्र ही समझा गया तथा इन सभी कार्यों के साथ-साथ सम्पूर्ण नगरीय जीवन ही पुलिस की निगरानी में आ गया। इसी का परिणाम था कि विश्व के अलग-अलग हिस्सों में पुलिस के गठन के साथ ही उसकी भूमिका बहुआयामी होती चली गई। जैसे-जैसे विश्व में मानव सभ्यता का विकास होता गया और चारों तरफ सामाजिक, आर्थिक, राजनैतिक, वैज्ञानिक और जनसंख्या संबंधी परिवर्तन आते गए, अपराध और अव्यवस्थाएं भी जहां-तहां बढ़ती चली गईं और पुलिस की भूमिका भी उत्तरोतर बदलती चली गई।

परिवर्तन के इसी दौर में पुलिस को यह वर्दीधारी स्वरूप मिला और उसका कार्यक्षेत्र भी कानूनी दायरों के साथ बढ़ता चला गया। पुलिस के उद्भव और विकास की वैश्वकि पृष्ठभूमि को आधार बना कर यदि पुलिस की भूमिका को समग्र रूप से परिभाषित किया जाए तो यह कहना बहुत ही सार्थक होगा कि- 'पुलिस एक संगठित निकाय के रूप में सरकार का वह अभिन्न अंग है, जो शांति व कानून-व्यवस्था बनाए रखने, अपराधों की छानबीन और रोकथाम करने तथा जनता व संपत्ति की रक्षा का कार्य करती है।'

सच कहें तो पुलिस को सरकार के प्रतिनिधि के रूप में, न्यायसंगत ढंग से और आवश्यकता के अनुरूप बल का प्रयोग करते हुए, समाज में शांति और कानून-व्यवस्था बनाए रखने तथा अपराधों को रोकने तथा उनकी जांच पड़ताल कर दोषियों को कानून के सामने पेश करने, अवैध गतिविधियों पर अंकुश लगाने एवं नागरिकों तथा सम्पत्ति की सुरक्षा करने की जिम्मेवारी निभानी होती है। आख़िर यही तो पुलिस की परम्परागत भूमिका है। लेकिन पुलिस की इन सभी जिम्मेदारियों का दायरा बहुत लम्बा-चौड़ा है। वास्तव में

पुलिस सरकार व समाज का सबसे महत्वपूर्ण हथियार है, जिसका इस्तेमाल देश, काल एवं वातावरण के अनुकूल सभी को न्याय दिलाने के लिए सैकड़ों वर्षों से किया जाता रहा है।

दरअसल, पुलिस कर्मी सरकार के वो नुमाइंदे हैं जो लोगों की शिकायतें सुनने और उन पर कार्रवाई करने के लिए प्रत्यक्ष रूप से जनता के सामने होते हैं। जब कभी समाज में कोई संकट, खतरा, असुरक्षा या कठिनाई पैदा होती है तो समाज को सबसे पहले पुलिस की याद आती है। साइबर अपराध भी आधुनिक युग का वो ख़तरा हैं, जिसमें आपका शत्रु अज्ञात है, किन्तु आपका रक्षक यानि आपकी पुलिस शिकायत दर्ज करने के लिए सदैव आपके समक्ष उपलब्ध है। सीधे तौर पर साइबर अपराध से ग्रसित होने वाले हर व्यक्ति या संस्था की पुलिस से पहली गुहार यही होती है कि वह अपराधी को पकड़े और पीड़ित को उसका पूरा हक दिलाए।

सत्ता या शासन के विकास कार्यों और जनकल्याणकारी योजनाओं का यथार्थ रूप से क्रियान्वयन केवल तभी हो सकता है, जब देश में हर स्थान पर शांति और कानून-व्यवस्था कायम रहे। इसका जीता-जागता उदाहरण भारत के वो प्रदेश या इलाके हैं जो बरसों तक आतंकवाद, उग्रवाद और नक्सलवाद का दंश झेलते रहे हैं। भले ही इन क्षेत्रों में सुरक्षा बलों और पुलिस ने शांति-व्यवस्था बहाली हेतु अपनी कोशिशों में कोई कसर न छोड़ी हो लेकिन आतंकवाद, उग्रवाद और नक्सलवाद की विभीषिका यहां अपना भयावह रूप दिखाती आई है और इसका नतीजा ये है कि ये क्षेत्र आज तक विकास और उन्नति के मामले में देश के दूसरे इलाकों की बराबरी नहीं कर पाए हैं।

वस्तुत: साइबर अपराध तो पुलिस की अतिरिक्त जिम्मेवारी हैं। कम्प्यूटर और सूचना व संचार प्रौद्योगिकी दुनिया की उन्नति के मकसद से ही बनाए गए हैं और इनके सकारात्मक परिणाम किसी से छिपे नहीं हैं, लेकिन अपराध

जगत ने इन्हीं संसाधनों का सहारा लेकर पुलिस के लिए नई चुनौतियां खड़ी कर दी हैं। जहां पारम्परिक अपराधों को अंजाम देने में शातिर दिमाग लोग सूचना व संचार प्रौद्योगिकी का इस्तेमाल करने लगे हैं, वहीं इन संसाधनों का प्रयोग करते हुए आम जनता को मानसिक रूप से त्रस्त करने और ठगने वाले साइबर अपराधियों ने भी परिस्थितियों को बद से बदतर बनाने में कोई कोर-कसर नहीं छोड़ी है।

इन हालातों से निपटने के लिए प्रत्येक प्रदेश की पुलिस ने भारत में सूचना प्रौद्योगिकी अधिनियम 2000 के लागू होने के बाद से ही साइबर अपराधों से लड़ने के लिए कुछ न कुछ अभिनव व्यवस्थाएं आरंभ कर दी थीं। हालांकि केन्द्र सरकार की ओर से देश को साइबर अपराधों से बचाने और साइबर अपराधों की रोकथाम एवं अन्वेषण के लिए जो व्यवस्थाएं की गई हैं, वे न केवल देशवासियों बल्कि समूचे देश के पुलिस संगठनों के लिए सबसे ज्यादा सहायक सिद्ध हो रही हैं। कि देश के विभिन्न पुलिस संगठनों ने साइबर अपराधों से जूझने के लिए क्या-क्या बंदोबस्त किए हैं-

केन्द्र सरकार की पहल –

- ☞ सूचना और प्रौद्योगिकी अधिनियम 17 अक्टूबर 2000 को लागू किया गया।
- ☞ वर्ष 2004 में भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (Indian Computer Emergency Response Team) CERT-in की स्थापना की गई, जो साइबर घटनाओं के बारे में सूचनाएं एकत्र करता है, उनका विश्लेषण और प्रसार करता है, साइबर सुरक्षा घटनाओं के बारे में पूर्वानुमान लगा कर चेतावनियां जारी करता है, साइबर सुरक्षा घटनाओं से निपटने के लिए आपात उपाय सुझाता है, साइबर घटना प्रत्युत्तर कार्यकलापों का समन्वय करता है, सूचना सुरक्षा

प्रक्रियाओं, पद्धतियों, रोकथाम, प्रत्युत्तर और साइबर घटनाओं की रिपोर्टिंग से संबंधित दिशानिर्देश जारी करता है, परामर्शी निदेश प्रदान करता है और सुभेद्यता नोट तथा श्वेत पत्र जारी करता है।

- सूचना प्रौद्योगिकी (जनता द्वारा सूचना के उपयोग को अवरुद्ध करने की प्रक्रिया एवं सुरक्षा उपाय) नियम-2009 लागू किए गए।

- वर्ष 2009 में राष्ट्रीय अपराध रिकॉर्ड ब्यूरो को अपराध एवं अपराधी ट्रैकिंग नेटवर्क एवं सिस्टम (सीसीटीएनएस) परियोजना की मॉनिटरिंग, समन्वय तथा कार्यान्वयन की ज़िम्मेदारी सौंपी गई। देश में यह परियोजना लगभग 15000 पुलिस स्टेशनों तथा देश के 6000 उच्च कार्यालयों को जोड़ती है।[1] ब्यूरो को यौन अपराधियों के राष्ट्रीय डाटाबेस (NDSO) की देख-रेख तथा इसे नियमित रूप से राज्यों/संघ प्रदेशों से साझा करने की ज़िम्मेदारी भी सौंपी गई है। 'ऑनलाइन साइबर अपराध सूचना पोर्टल' की तकनीकी एवं परिचालन प्रक्रिया की देखरेख के लिए भी ब्यूरो को नामित किया गया है, जिसके माध्यम से कोई भी नागरिक बच्चों से संबंधित अश्लील बातें, बलात्संग, सामूहिक बलात्संग की शिकायत दर्ज कर सकता है एवं साक्ष्य के तौर पर विडियो क्लिप अपलोड कर सकता है। ब्यूरो ने साइबर अपराधों की जांच तथा अभियोजन में विभिन्न हितधारकों के लिए ऑनलाइन प्रशिक्षण पोर्टल साईट्रेन (CyTrain) की भी शुरुआत की है।

  एनसीआरबी का एक उद्देश्य देश में पुलिस बलों की क्षमता निर्माण के लिए आईटी और अंगुली छाप विज्ञान में प्रशिक्षण प्रदान करना है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो की प्रशिक्षण शाखा इस लक्ष्य को प्राप्त करने की दिशा में हर संभव प्रयास कर रही है। प्रत्येक वर्ष यह शाखा

1 https://ncrb.gov.in/hi/निदेशक-का-संदेश#

भारतीय पुलिस अधिकारियों के लिए औसतन 60 प्रशिक्षण कार्यक्रम आयोजित करती है। इन पाठ्यक्रमों की अवधि 3 दिन से 2 सप्ताह तक होती है। "साइबर अपराध और डिजिटल फॉरेंसिक", "कानून प्रवर्तन में सूचना प्रौद्योगिकी", "डेटा एनालिटिक्स", "अपराध-अपराधी ट्रैकिंग और नेटवर्क सिस्टम(सीसीटीएनएस)"/परियोजना प्रबंधन", "नकली विदेशी मुद्रा नोट", "अंगुली छाप विज्ञान पर प्रशिक्षकों का प्रशिक्षण", "अंगुली छाप विज्ञान पर पुनश्चर्या पाठ्यक्रम", "बुनियादी अंगुली छाप विज्ञान पाठ्यक्रम", "रंगीन पोर्ट्रेट निर्माण प्रशिक्षण", "भारत में अपराध पर प्रशिक्षकों का प्रशिक्षण", "भारत में दुर्घटना में मृत्यु एवं आत्महत्या पर प्रशिक्षकों का प्रशिक्षण", "भारत में जेल सांख्यिकी पर प्रशिक्षकों का प्रशिक्षण", "तलाश सूचना सिस्टम", "ऑटोमैटिक फ़िंगरप्रिंट आइडेंटिफिकेशन सिस्टम पर कार्यशाला" आदि जैसे विभिन्न विषयों पर प्रशिक्षण कैलेंडर के अनुसार नियमित रूप से प्रशिक्षण दिया जाता है।[2]

- माह-अप्रैल 2011 सूचना प्रौद्योगिकी(मध्यवर्ती संस्थाओं के लिए दिशा-निर्देश) नियम 2011, में अधिसूचित किए गए।
- 2 जुलाई 2013 को 'राष्ट्रीय साइबर सुरक्षा नीति-2013' लागू की गई।
- वर्ष 2014 में राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र (National Critical Information Infrastructure Protection Centre- NCIIPC) की स्थापना की गई, जो हवाई नियंत्रण, नाभिकीय तथा अंतरिक्ष संबंधी महत्वपूर्ण रणनीतिक क्षेत्रों में साइबर सुरक्षा संबंधी खतरों से निपटने के उद्देश्य से राष्ट्रीय तकनीकी अनुसंधान संगठन (NTRO) के अंतर्गत कार्य करता है।

2 https://ncrb.gov.in/hi/प्रशिक्षण-शाखा

- वर्ष 2015 में राष्ट्रीय साइबर समन्वय केन्द्र (NCCC) की स्थापना की गई, जो आसन्न और संभावित साइबर सुरक्षा खतरों के प्रति जागरूकता फैलाता है और संबंधित संस्थाओं/सुरक्षा एजेंसियों को समय रहते खतरों की रोकथाम की त्वरित कार्रवाई हेतु सचेत करते हुए आवश्यक सूचनाएं उपलब्ध करवाता है।

- वर्ष 2017 में साइबर स्वच्छता केन्द्र (Cyber Swachhta Kendra) नामक वेबसाइट आरंभ की गई, जिसे राष्ट्रीय साइबर सुरक्षा नीति के लक्ष्यों के अनुरूप तैयार किया गया है, जो बोटनेट स्वच्छता एवं मालवेयर विश्लेषण का केन्द्र (Botnet Cleaning and Malware Analysis Centre) के रूप में कार्य करता है। इस केन्द्र के माध्यम से मेलिशियस प्रोग्राम को पहचानने में मदद मिलती है एवं उसे हटाने के लिए नि:शुल्क टूल भी प्राप्त होता है। यह केन्द्र/वेबसाइट CERT-in के तत्वावधान में संचालित है।

- वर्ष 2017 में गृह मंत्रालय के अंतर्गत साइबर एवं सूचना सुरक्षा (C&IS) प्रभाग की स्थापना की गई। यह प्रभाग साइबर सुरक्षा, साइबर अपराध, राष्ट्रीय सूचना सुरक्षा नीति एवं दिशानिर्देश (एनआईएसपीजी) और एनआईएसपीजी, नैटग्रिड आदि के कार्यान्वयन से संबंधित मामले देखता है।

- दिसम्बर 2018 में साइबर समन्वय केन्द्र के पोर्टल (CyCord) की स्थापना की गई, जिसका मुख्य उद्देश्य विधि-प्रवर्तक एजेंसियों और अन्य भागीदारों द्वारा साइबर अपराधों से निपटने के लिए की जा रही कोशिशों का समन्वय करना और अन्य विषयों जैसे- केस स्टडीज/अनुसंधान निष्कर्षों एवं अनुभवों को साझा करने, अनुसंधान की समस्याओं को सुलझाने और जटिल साइबर समस्याओं का हल खोजने में सहायता प्रदान करना है। साइबर अपराधों से निपटने के लिए यह एक सशक्त मंच है।

- दिसम्बर 2018 में सरकार ने सूचना प्रौद्योगिकी अधिनियम की धारा 69 ए तथा सूचना प्रौद्योगिकी (जनता द्वारा सूचना के उपयोग को अवरुद्ध करने की प्रक्रिया एवं सुरक्षा उपाय) नियम 2009 के नियम 4 प्रदत्त शक्तियों का प्रयोग करते हुए भारत की दस सुरक्षा एजेंसियों- आसूचना ब्यूरो(Intelligence Bureau), स्वापक नियंत्रण ब्यूरो (Narcotics Control Bureau), प्रवर्तन निदेशालय (Enforcement Directorate), केन्द्रीय प्रत्यक्ष कर बोर्ड (Central Board of Direct Taxes), राजस्व आसूचना निदेशालय (Directorate of Revenue Intelligence), केन्द्रीय अन्वेषण ब्यूरो (Central Bureau of Investigation), राष्ट्रीय अन्वेषण एजेंसी (National Investigation Agency), केन्द्रीय सविचालय(रॉ) (Cabinet Secretariat(RAW)), सिगनल आसूचना निदेशालय (Directorate of Signal Intelligence) और दिल्ली पुलिस के कमिश्नर को ऐसी शक्तियां प्रत्यायोजित की गई कि वे इंटरसेप्शन, मॉनिटरिंग और डिस्क्रिप्शन के मकसद से किसी भी कंप्यूटर के डेटा को खंगाल सकती हैं। [3]

- वर्ष 2019 में राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (National Cyber Crime Reporting Portal : www.cybercrime.gov.in) की स्थापना की गई। यह पोर्टल भारत सरकार के गृह मंत्रालय की यह एक नागरिक-केंद्रित पहल है, जो इस पोर्टल के माध्यम से नागरिकों को साइबर अपराधों की शिकायत ऑनलाईन दर्ज करने की सुविधा उपलब्ध कराती है। यह पोर्टल खास तौर पर महिलाओं और बच्चों के विरुद्ध होने वाले साइबर अपराधों और बाल पोर्नोग्राफी,

3 https://economictimes.indiatimes.com/news/politics-and-nation/10-central-agencies-can-now-snoop-on-any-computer-they-want/articleshow/67188875.cms

बाल यौन शोषण सामग्री, रेप/गैंग रेप से संबंधित ऑनलाइन सामग्री आदि से जुड़े अपराधों को अविलम्ब दर्ज करने हेतु उपलब्ध कराया गया है।

☞ वर्ष 2019 में रक्षा साइबर एजेंसी (Defence Cyber Agency-DCA) की स्थापना की गई। साइबर जगत में संभावित खतरों से निपटने के लिए एकीकृत रक्षा स्टाफ (आईडीएस) के तहत यह विशेष साइबर एजेंसी गठित की गई है।

☞ वर्ष 2020 में भारतीय साइबर अपराध समन्वय केन्द्र (इंडियन Cyber Crime Coordination Centre- I4C) की स्थापना की गई है। भारतीय साइबर अपराध समन्वय केन्द्र की योजना व्यापक और समन्वित तरीके से सभी प्रकार के साइबर अपराधों से निपटने के लिए तैयार की गई है। इस योजना के सात घटक हैं- नेशनल साइबर क्राइम थ्रेट एनालिटिक्स यूनिट, नेशनल साइबर क्राइम रिर्पोटिंग पोर्टल, नेशनल साइबर क्राइम ट्रेनिंग सेंटर, साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट, नेशनल साइबर क्राइम रिसर्च एंड इनोवेशन सेंटर, नेशनल साइबर क्राइम फॉरेंसिक लेबोरेट्री ईको सिस्टम और प्लेटफॉर्म फॉर ज्वाइंट साइबर क्राइम इन्वेस्टिगेशन टीम। गृह मंत्रालय की पहल पर 15 राज्यों और केन्द्र शासित प्रदेशों ने अपने यहां क्षेत्रीय अपराध समन्वय केन्द्र स्थापित करने की सहमति दी है।

☞ वर्ष 2020 में केन्द्रीय गृह मंत्रालय ने जनता को साइबर अपराधों के प्रति जागरूक बनाने और सहायता प्रदान करने के लिए एक ट्विटर हैंडल 'साइबर-दोस्त' की शुरुआत की है।

☞ 5 फरवरी 2021 को सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत सूचना प्रौद्योगिकी (मध्यवर्ती संस्थानों के लिए दिशा-निर्देश और

डिजिटल मीडिया आचार संहिता) नियम, 2021 अधिसूचित किए गए हैं।

☞ इतना ही नहीं 17 जुलाई 2019 में एक राज्य सभा प्रश्न के उत्तर में केन्द्रीय गृह राज्यमंत्री जी. किशन रेड्डी द्वारा सदन को अवगत कराया गया कि भारत सरकार ने उपरोक्त के अलावा निम्नलिखित व्यवस्थाएं भी सुनिश्चित की हैं[4] -

- डिजिटल सेवाएं प्रदान करने वाले सभी संगठनों के लिए यह अनिवार्य है कि वे साइबर सुरक्षा से संबंधित मामलों से CERT-In को तत्काल अवगत कराएं।
- विभिन्न एप्लीकेशन्स/अवसंरचनाओं की सुरक्षा के लिए सभी मुख्य सूचना सुरक्षा अधिकारियों (Chief Information Security Officers) को उनके प्रमुख कर्तव्यों और उत्तरदायित्वों के बारे में दिशा-निर्देश जारी किए जाते हैं।
- सभी सरकारी वेबसाइटों और एप्लीकेशन्स को शुरू करने से पूर्व और उनके शुरू होने के बाद नियमित अंतराल पर उनके ऑडिट/निरीक्षण के लिए प्रावधान किए गए हैं।
- साइबर हमलों और साइबर आतंकवाद से निपटने के लिए संकट प्रबंधन योजना बनाई गई है।
- सरकारी एवं अन्य महत्वपूर्ण क्षेत्रों के संगठनों में साइबर सुरक्षा प्रबंधों और तैयारियों का आंकलन करने के लिए समय-समय पर साइबर सुरक्षा संबंधी छद्म अभ्यास (Mock Drills) एवं अन्य अभ्यास करवाये जाते हैं।

4 https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226

➢ सूचना प्रौद्योगिकी की अवसंरचनाओं की सुरक्षा एवं साइबर हमलों से बचाव के उद्देश्य से सरकारी और अन्य महत्वपूर्ण क्षेत्रों के नेटवर्क/ सिस्टम एडमिनिस्ट्रेटर्स एवं मुख्य सूचना सुरक्षा अधिकारियों के लिए नियमित रूप से प्रशिक्षण कार्यक्रम आयोजित किए जाते हैं।

☞ इसी प्रकार, हाल ही में 10 दिसम्बर 2020 को एक लोकसभा प्रश्न का उत्तर देते हुए केन्द्रीय गृह राज्यमंत्री हंसराज गंगाराम अहीर ने सदन को अवगत कराया कि उपरोक्त व्यवस्थाओं के अलावा, साइबर अपराधों से निपटने हेतु 'फोन धोखाधड़ी से निपटने के लिए एक अंतर-मंत्रालयी समिति (Inter Ministry Committee on Phone Fraud-IMCPF)' भी गठित की गई है, जिसमें इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय, भारतीय रिर्जव बैंक और विधि-प्रवर्तक एजेंसियों के सदस्य सम्मिलित हैं। वहीं Fake Indian Currency Note(FICN) Coordination Group (FCORD) को इस उद्देश्य से प्रमुख नोडल एजेंसी बनाया गया है तथा प्रत्येक राज्य में एक अपर महानिदेक या महानिरीक्षक को नोडल अधिकारी नियुक्त किया गया है।[5]

☞ साइबर जगत में बढ़ते अपराधों और साइबर खतरों के प्रति भारत सरकार कितनी सजग व सतर्क है इसका एक जीवंत उदाहरण उस समय देखने को मिला जब सरकार ने जून 2020 के दौरान उन 59 मोबाइल ऐप्लीकेशन्स पर प्रतिबंध लगाया जो भारत की संप्रभुता एवं अखंडता, भारत की रक्षा, राज्य की सुरक्षा और सार्वजनिक व्यवस्था के लिए नुकसानदेह थीं। भारत सरकार ने यह निर्णय सूचना प्रौद्योगिकी अधिनियम की धारा 69 ए तथा सूचना प्रौद्योगिकी (जनता द्वारा

5 https://www.mha.gov.in/MHA1/Par2017/pdfs/par2019-pdfs/ls-10122019/3566.pdf

सूचना के उपयोग को अवरुद्ध करने की प्रक्रिया एवं सुरक्षा उपाय) नियम 2009 के संबंधित प्रावधानों में प्रदत्त शक्तियों का प्रयोग करते हुए और खतरों की उभरती प्रकृति को देखते हुए लिया। इन ऐप्लीकेशन्स में टिक-टॉक, शेयर इट, क्लब फैक्टरी, न्यूज़ डॉग, कैम स्केनर, वी मीट जैसे कई लोकप्रिय एप्लीकेशनस शामिल थीं।[6]

☞ केन्द्रीय अन्वेषण ब्यूरो (CBI) के तत्वावधान में वर्ष 2010 में एक 'साइबर एंड हाइटेक क्राइम इंवेस्टिगेशन एंड ट्रेनिंग सेंटर (CHCIT) स्थापित किया गया है। इस केन्द्र पर सीबीआई अधिकारियों और टेक्निकल एंड फॉरेंसिक सपोर्ट यूनिट(TAFS Units), राज्य पुलिस के अधिकारियों तथा विदेशी पुलिस (अफ्रीका, नेपाल, म्यांमार, भूटान, वियतनाम आदि) के अधिकारियों को विभिन्न प्रशिक्षण दिए जाते हैं। साथी ही साइबर अपराध के बड़े मामलों को सुलझाने में तकनीकी और फॉरेंसिक मदद भी प्रदान की जाती है।[7]

6 https://archive.pib.gov.in/archive2/hindirelease.aspx
7 http://cbiacademy.gov.in/chcit.php

राज्यों में साइबर अपराध के उन्मूलन हेतु पुलिस की तैयारियां – एक विश्लेषण

भारत में वर्तमान में 28 राज्यों और 9 केन्द्र शासित प्रदेशों में साइबर अपराध सुरक्षा तंत्र की यदि समीक्षा की जाए तो यह ज्ञात होता है कि अभी भी यहां हर जिला मुख्यालय पर समर्पित साइबर पुलिस स्टेशन मौजूद नहीं है। केन्द्र सरकार देश भर में साइबर अपराधों पर अंकुश लगाने के लिए वर्ष 2000 में सूचना प्रौद्योगिकी अधिनियम लागू करने के बाद से ही निरंतर सक्रिय रही है और राज्य सरकारों को इस संबंध में समय-समय दिशा-निर्देश भी दिए जाते रहे हैं तथा केन्द्रीय स्तर पर ऑनलाईन अपराध पंजीकरण से लेकर, प्रशिक्षण सुविधाएं, समन्वय केन्द्र, साइबर फॉरेंसिक लैब जैसी सभी सुविधाएं उपलब्ध कराई गई हैं। वस्तुत: भारत के संविधान की सातवीं अनुसूची के तहत 'पुलिस' और 'लोक व्यवस्था' राज्य के विषय हैं और इसलिए अपराध रोकने, पता लगाने, दर्ज करने और जांच-पड़ताल करने तथा अपराधियों के विरुद्ध अभियोजन चलाने की मुख्य जिम्मेदारी, राज्य सरकारों की है। तथापि, केन्द्र सरकार, राज्य पुलिस बलों की आधुनिकीकरण योजना के तहत अस्त्र-शस्त्र, संचार, उपस्कर, मोबिलिटी, प्रशिक्षण और अन्य अवसंरचना के संदर्भ में राज्य सरकारों के पुलिस बलों के आधुनिकीकरण के लिए उन्हें वित्तीय सहायता प्रदान करके उनके प्रयासों में सहायता करती है।

दरअसल वर्तमान परिवेश में साइबर अपराध इतने व्यापक हो चुके हैं कि कोई भी कहीं भी इनका शिकार हो सकता है और इसीलिए महानगरों को छोड़कर देश के हर जिले में कम से कम एक साइबर पुलिस स्टेशन की आवश्यकता से इंकार नहीं किया जा सकता। साइबर अपराधों के अन्वेषण के लिए विशेष किस्म के प्रशिक्षण एवं अनुभव की आवश्यकता होती है। इसमें पुलिस अधिकारियों एवं कर्मियों का नई प्रौद्योगिकी के प्रयोग व बारिकीयों से वाकिफ होना परमावश्यक है। साइबर अपराध सच्चे अर्थों

में ऐसे अपराध हैं, जिनकी जांच पड़ताल बिना तकनीकी ज्ञान व अनुभव के बहुत ही कठिन व दूभर हो जाती है। इसीलिए तो देश के महानगरों में और चुनिंदा शहरों में अलग से साइबर अपराध के अन्वेषण केन्द्र या थाने खोले जाते हैं।

साइबर सुरक्षा तंत्र की बनावट की दृष्टि से भारत में हर राज्य में भिन्नताएं देखी जाती हैं। किसी राज्य में साइबर सुरक्षा तंत्र बहुत मजबूत है तो कहीं अभी साइबर पुलिस थानों की स्थापना की शुरुआत हो रही है। साइबर अपराध के आंकड़ों की दृष्टि से सबसे ज्यादा अपराध कर्नाटक और उत्तर प्रदेश में घटित होते हैं। इसी परिप्रेक्ष्य में प्रमुख राज्यों में साइबर अपराधों के उन्मूलन के उद्देश्य से की गई व्यवस्थाओं की एक झलक यहां प्रस्तुत है-

कर्नाटक

कर्नाटक वो राज्य है जहां वर्ष 2001 में भारत के सबसे पहले साइबर पुलिस स्टेशन की स्थापना बंगलूरु में की गई थी। आज कर्नाटक ही वह राज्य है जहां साइबर अपराध के पुलिस थानों का कमिश्नरेट स्थापित किया गया है, जिसके अंतर्गत कुल 9 रेंज बनाई गई हैं, जिनके अंतर्गत कुल 36 सी.ई.एन. (साइबर क्राइम, इकोनॉमिक ओफेन्स एवं नारकोटिक्स) पुलिस थाने हैं।

उत्तर प्रदेश

वहीं उत्तर प्रदेश में कुल 18 साइबर पुलिस थाने हैं, जिनमें से नोएडा एवं लखनऊ के साइबर पुलिस थाने 2018 में स्थापित किए गए थे और आगरा, अलीगढ़, सहारनपुर, प्रयागराज, बरेली, मुरादाबाद और गोरखपुर स्थित 16 अन्य साइबर पुलिस थाने अगस्त 2020 में स्थापित किए गए थे। हाल ही में उत्तर प्रदेश सरकार ने इन सभी 18 साइबर पुलिस थानों में 'महिला साइबर प्रकोष्ठ' खोलने का निर्णय लिया है, ताकि साइबर स्टॉकिंग/बुलिंग जैसे

अपराधों से निपटा जा सके।[8]

महाराष्ट्र

साइबर अपराधों और अन्य डिजिटल हमलों से निपटने के लिए महाराष्ट्र सरकार द्वारा 'महाराष्ट्र साइबर' नामक नोडल एजेंसी का गठन किया गया है। यह एजेंसी महाराष्ट्र में साइबर अवसंरचना के विकास के साथ-साथ साइबर पुलिस स्टेशनों की स्थापना, एंटी-पायरेसी सिस्टम, पूर्वानुमान आधारित पुलिस व्यवस्था, साइबर अपराधों के बारे में जागरूकता और अन्य अभिनव प्रयासों के लिए कार्य कर रही है। इन कोशिशों ने महाराष्ट्र को देश का पहला ऐसा राज्य बना दिया है जहां 47 साइबर पुलिस थाने और 51 साइबर लैब है जो साइबर अपराधों के अन्वेषण को त्वरित बना रहे हैं। इसके अलावा इस एजेंसी ने एक एंटी-फिशिंग यूनिट तथा एंटी-पायरेसी यूनिट का गठन भी किया है।[9] इसके अलावा महाराष्ट्र में विभिन्न महानगरों के स्तर पर भी साइबर सुरक्षा की दिशा में अभिनव प्रयास किए जा रहे हैं। पुणे में वर्ष 2017 में 5741, वर्ष 2018 में 4461, वर्ष 2019 में 7500 और वर्ष 2020 में 15000 से ज्यादा साइबर अपराध के मामले दर्ज किए गए। इस बीच वर्ष 2018 में पुणे में एक समर्पित साइबर पुलिस थाने की स्थापना की गई थी। अब साइबर अपराध के दुगनी, तिगुनी दर से बढ़ते मामलों को देखते हुए पुणे महानगर में खास तौर पर सिर्फ साइबर अपराधों का निपटान करने के लिए 5 समर्पित टीमें गठित की गई हैं, जिनमें से प्रत्येक का नेतृत्व एक निरीक्षक द्वारा किया जाएगा। ये टीमें अपने-अपने कार्यक्षेत्र में निपुणता से कार्य करेंगी। तदनुसार इन्हें क्रमश: हैकिंग/डाटा चोरी, ठगी/धोखाधड़ी, सोशल नेटवर्किंग, एटीएम कार्ड जालसाजी और प्रशासन के क्षेत्र

8 https://www.hindustantimes.com/cities/noida-news/women-cyber-cell-to-be-set-up-in-cyber-police-stations-across-up-101615139773850.html

9 https://www.reportphishing.in/about-us.php#section2

से जुड़े साइबर अपराधों की जांच व अन्वेषण का जिम्मा सौंपा गया है।[10] वहीं मुम्बई में हाल ही में 4 नए साइबर पुलिस थानों की स्थापना के लिए स्वीकृति प्रदान की गई है, जिन्हें मिला कर वहां अब कुल 5 साइबर पुलिस थाने होंगे।[11] इसके अलावा महाराष्ट्र में महानगरी पुलिस के द्वारा साइबर अपराधों की रोकथाम के लिए ट्विटर हैंडल और फेसबुक पेज भी संचालित किए जा रहे हैं।

गुजरात –

राज्य में साइबर सुरक्षा पर निगरानी रखने और इसमें सतत सहयोग प्रदान करने के उद्देश्य से गुजरात पुलिस ने अत्याधुनिक सुविधाओं से लैस एक नियंत्रण कक्ष स्थापित किया है। ऑनलाईन धोखाधड़ी, साइबर बुलिंग या डाटा अथवा पहचान चोरी जैसे अपराधों से पीड़ित कोई भी नागरिक इस नियंत्रण कक्ष से संपर्क स्थापित कर सकता है। इस नियंत्रण कक्ष के तत्वावधान में एंटी-साइबर-बुलिंग यूनिट 'प्रतिरोध', साइबर अपराध रोकथाम यूनिट 'निवारण', दुर्घटना प्रतिक्रिया यूनिट 'त्वरित', साइबर सुरक्षा लैब आदि भी संचालित हैं। इसके अलावा राज्य में साइबर अपराधों में अन्वेषण संबंधी मदद प्रदान करने हेतु एक आनलॉइन पोर्टल 'https://cybernodal.gujarat.gov.in/ भी मुहैया कराया गया है। साथ ही राज्य साइबर क्राइम सेल का ट्विटर हैंडल और फैसबुक पेज जनता को सहायता कर रहे हैं।

10 https://www.punekarnews.in/pune-police-set-up-5-units-to-tackle-rising-cyber-crime-cases.

11 https://www.hindustantimes.com/cities/mumbai-news/mumbai-to-get-five-new-cyber-police-stations-on-republic-day-101611602298270.html

मध्य प्रदेश -

मध्य प्रदेश में राज्य साइबर पुलिस मुख्यालय की स्थापना की गई है। साथी ही साइबर अपराधों के अन्वेषण में मदद प्रदान करने के लिए ऑनलाइन हैल्पलाईन, ट्विटर हैंडल तथा फेसबुक पेज भी उपलब्ध कराया गया है।

बिहार –

राज्य में साइबर अपराधों से जुड़ी शिकायतों के निपटान हेतु कुल 20 'साइबर क्राइम सोशल मीडिया यूनिट (CCSMUs) गठित की गईं है। इन यूनिटों को राज्य के 20 पुलिस थानों में तैनात किया गया है। इन यूनिटों को ऐसे प्रत्येक जिले में तैनात किया गया है, जहां कम-से-कम 20 थाने हैं। प्रत्येक यूनिट में 1 निरीक्षक, 3 उप निरीक्षक, 2 सिपाही, 1 कम्प्यूटर प्रोग्रामर और 3 डाटा ऑपरेटरर्स/ तकनीकी जानकारों को नियुक्त किया गया है। इन यूनिटों में से प्रत्येक यूनिट के 6 कर्मियों को साइबर अपराधों से निपटने का प्रशिक्षण दिया गया है। इसके अलावा राज्य के 2200 अन्य पुलिस कर्मियों को भी साइबर अपराधों से निपटने के लिए विशेष प्रशिक्षण प्रदान किया गया है।[12]

झारखण्ड–

राज्य के जामताड़ा और देवघर जिले साइबर अपराधों के गढ़ कहे जाते हैं। इन स्थानों से देश भर में फिशिंग और ऑनालाईन धोखाधड़ी के अनगिनत मामलों को अंजाम दिया गया है। राज्य का पहला साइबर पुलिस थाना वर्ष 2016 में रांची में स्थापित किया गया था।[13] यहां वर्तमान में कुल 7 साइबर थाने कार्यरत हैं जो रांची, जमशेदपुर, धनबाद, गिरिडीह, देवघर, जामताड़ा और पलामू में स्थापित हैं। इसके अलावा हर जिले साइबर सेल को सक्रिय

12 https://timesofindia.indiatimes.com/city/patna/74-units-formed-to-curb-cybercrime/articleshow/77858534.cms

13 https://jharkhand.mygov.in/en/group-issue/cyber-crime-police-station

रखा गया है, ताकि साइबर अपराधों की प्रभावी ढंग रोकथाम की जा सके।[14]

केरल -

केरल में साइबर पुलिस थानों की स्थापना वर्ष 2009 में आरंभ कर दी गई थी। ये थाने साइबर अपराधों के मामले में एफआईआर दर्ज कर अन्वेषण करने और न्यायालय के समक्ष प्रकरण को प्रस्तुत करने में सक्षम हैं। तिरुवनन्तपुरम के मुख्य न्यायिक मजिस्ट्रेट के न्यायालय को यहां साइबर अपराधों के लिए विशेष न्यायालय घोषित किया गया है। राज्य में कुल 19 साइबर पुलिस थाने हैं। अक्टूबर 2020 से पहले यहां 4 साइबर पुलिस थाने थे, किन्तु बढ़ते साइबर अपराधों को देखते हुए राज्य में कार्यरत 15 साइबर सेल को साइबर थानों का दर्जा दे दिया गया। ये साइबर थाने क्रमश: तिरुवनन्तपुरम-ग्रामीण, कोल्लम सिटी, कोल्लम-ग्रामीण, पाथानामथिट्टा, कोट्टायम, आलप्पुझा, इडुक्की, एर्नाकुलम-ग्रामीण, तृश्शूर-ग्रामीण, वायनाड, पलक्कड़, मल्लपुरम, कोड़िकोड़-ग्रामीण, कुन्नूर और कासरगोड में स्थापित हैं।[15]

दिल्ली -

देश की राजधानी दिल्ली में साइबर अपराधों से निपटने के पुख्ता प्रबंध किए गए हैं। दिल्ली पुलिस की वेबसाइट के अनुसार यहां दिल्ली पुलिस के 12 जिला साइबर प्रकोष्ठ मुस्तैदी से कार्यरत हैं। साइबर अपराधों से निपटने के लिए दिल्ली पुलिस ने 'साइबर क्राइम फोरेंसिक वेन' भी उपलब्ध कराई है, जो अत्याधुनिक उपकरणों से लैस हैं और सायबर पुलिस के अन्वेषण को त्वरित एवं परिणामोन्मुखी बनाती है।

14 https://www.jhpolice.gov.in/cyber-crime-ps
15 https://keralapolice.gov.in/page/cyber-crime-police-station

असम –

राज्य में साइबर अपराध प्रकोष्ठ सी.आई.डी. मुख्यालय में संचालित है। साथ ही यहां एक साइबर फॉरेंसिक लैब भी स्थापित किया गया है। इस प्रकोष्ठ में उन जटिल मामलों का अन्वेषण एवं निपटान किया जाता है, जिन्हें जिला स्तर पर पुलिस द्वारा तकनीकि ज्ञान एवं अनुभव में कमी के कारण सुलझाया नहीं जाता। साइबर प्रकोष्ठ ने जनता की शिकायतें दर्ज करने और उनकी मदद के लिए एक फेसबुक पेज भी उपलब्ध कराया है।[16]

शेष सभी राज्यों में जिला स्तर पर साइबर अपराध प्रकोष्ठ सक्रिय किए गए हैं और आवश्यकतानुरूप जिला स्तर पर साइबर अपराध थानों की स्थापना यथावसर राज्य सरकार के निर्देशानुसार की जा रही है। बहरहाल हम सारांशत: कह सकते हैं कि देश में हर जिले के स्तर पर साइबर अपराध थानों की स्थापना अभी प्रक्रियाधीन ही है। वहीं कुछ राज्य ऐसे भी हैं जिनमें हाल ही के वर्षों में साइबर अपराध थानों की स्थापना शुरू की गई है। मसलन- हरियाणा के गुरुग्राम में प्रदेश का पहला साइबर अपराध थाना वर्ष 2018 में स्थापित किया गया।[17] वहीं छत्तीसगढ़ राज्य में पहला साइबर अपराध थाना अगस्त 2020 में स्थापित किया गया।[18] वस्तुत: कई राज्यों के स्तर पर अभी साइबर अपराध सुरक्षा तंत्र को और अधिक सुदृढ़ बनाए जाने की आवश्यकता है।

16 https://police.assam.gov.in/frontimpotentdata/cyber-crime-and-cyber-forensics

17 https://www.business-standard.com/article/pti-stories/first-cyber-police-station-of-hry-established-in-gurugram-118030701475_1.html

18 https://www.patrika.com/raipur-news/state-s-first-cyber-police-station-will-start-from-15-in-phq-6317492/

अध्याय 11

सर्तकता और जन-जागृति में पुलिस की भूमिका

पुलिस सरकार की वह संस्था है, जिसे जरूरत के मुताबिक बल का प्रयोग करते हुए देश में कानून व्यवस्था बनाए रखने, सरकार एवं जनता की सम्पत्ति की सुरक्षा करने, नागरिकों के बीच अव्यवस्था तथा अराजकता को फैलने से रोकने के लिए तत्परता से कार्य करना होता है। वस्तुत: विश्व स्तरीय परिप्रेक्ष्य में पुलिस की अवधारणा हजारों वर्ष पुरानी है। समय के साथ विश्व के हर देश में पुलिस के संगठनात्मक रूप में अनेक बदलाव आए हैं, लेकिन बुनियादी रूप से इसका अस्तित्व देश में कानून प्रवर्तन करने वाली केन्द्रीय संस्था के रूप में ही रहा है।

शांति और कानून-व्यवस्था बनाये रखने के लिए पुलिस को सरकार के सबसे प्रथम प्रतिनिधि के रूप में जनता के बीच उतर कर कार्य करना होता है। समाज में शांति व कानून-व्यवस्था बनाए रखना, अपराधों की रोकथाम करना, अपराधों का अन्वेषण कर अपराधियों को कानून से सजा दिलाना, ग़ैरकानूनी गतिविधियों पर रोक लगाना तथा सभी प्रकार की सरकारी और निजी सम्पत्ति की रक्षा करना पुलिस की पारम्परिक और मूल भूमिका रही है। सच कहें तो पुलिस सरकार व समाज का सबसे जिम्मेदार और महत्वपूर्ण अंग है। आख़िर पुलिस ही तो सरकार का वो चेहरा है जो जमीनी तौर पर जनता के सामने होता है। पुलिस कर्मी सरकार के वो प्रतिनिधि हैं, जो जनता को ये अहसास दिलाते हैं कि कानून मौज़ूद है तथा ये भी बताते हैं कि कानून के दायरे में रह कर जनता को क्या करना चाहिए और क्या नहीं।

दरअसल पुलिस ही वो सबसे पहला माध्यम है, जिसके जरिए अपराधों से पीड़ित लोग अपनी शिकायतें कानून के सामने पेश करते हैं। इस दृष्टि से पुलिस देश के विकास की सबसे महत्वपूर्ण कड़ी है, क्योंकि यदि देश में किसी भी स्थान पर अराजकता, अशांति अथवा जन-आक्रोश फैलता है तो वहां विकास बहुत पीछे छूट जाता है। सूचना व संचार प्रौद्योगिकी के इस युग में पुलिस के कार्यक्षेत्र में असीमित विस्तार हुआ है, जिसके चलते पुलिस की पारम्परिक भूमिका को निसंदेह एक परिमार्जित रूप में देखने व समझने की आवश्यकता है।

सूचना व संचार प्रौद्योगिकी के इस युग में जन-जीवन की आपाथापी के बीच निरंतर बढ़ते साइबर अपराध के मामलों को देख कर अब से कुछ 30-35 वर्ष पुराना एक अनूठा अनुभव याद आता है। ये वो दौर था जब गली-मोहल्लों की रात्रिकालीन गश्त के लिए चौकीदार तैनात रहते थे और तेज सीटी बजाकर या डंडा फटकार कर दो-चार सीमित गलियारों में सारी रात गश्त देते थे। इतना ही नहीं वे अक्सर तेज़ आवाज़ में ये वाक्य भी दोहराते चलते थे- 'जागते रहो, जागते रहो'। है न अजीब सी बात, रात को बेवजह भला कौन जागता है! लेकिन अचरज की बात ये है कि उस जमाने में सीटी, डंडे और तेज पुकार की इन कर्कश आवाजों के बीच लोग पल भर को जागते भी थे और सारी रात बेफ्रिक होकर चैन से सोते भी थे। दरअसल, चौकीदार की ये आवाजें उनके लिए सुकून का संदेश थीं, क्योंकि उन्हें लगता था कि उनकी रक्षा के लिए कोई तो जाग रहा है। वो लोग ये भी जानते थे कि उनके घर में और तिजोरी में मजबूत ताले जड़े हुए हैं तथा बाहर चौकीदार पहरा दे रहा है और अब किसी चोर या गिरहकट कि क्या मज़ाल कि वो उनके घर पर धावा बोल दे।

आज के दौर में परिस्थितियां बिल्कुल विपरीत हैं। यहां ताले भी मजबूत हैं, चौकीदार के रूप में सरकार, सुरक्षा एजेंसियां, पुलिस, बैंकिंग संस्थान और

अनेक वित्तीय एवं सामाजिक संस्थाएं लोगों को बार-बार साइबर अपराधों के प्रति सचेत भी कर रहे हैं, लेकिन इसके बावजूद साइबर धोखाधड़ी और साइबर अपराधों के मामले रोज घटित हो रहे हैं। कारण यही है कि अब भले ही घर और तिजोरी की तालाबंदी लाख गुना मजबूत हो, बाहर सुरक्षाकर्मी या पहरेदार तैनात हों, लोग समाज में खुद को सुरक्षित समझें, लेकिन सूचना व संचार प्रौद्योगिकी ने शातिर अपराधियों को इतना सशक्त बना दिया है कि वे एक ज़रा सी चूक का फायदा उठा कर पलक झपकते ही या तो लाखों का चूना लगा जाते हैं या व्यक्तिगत और सामाजिक सम्मान आहत कर जाते हैं। साइबर अपराध लोगों को न केवल धन, बल्कि मानसिक व आत्म-सम्मान से जुड़ी क्षति पहुंचाते हैं। वस्तुत: पुराने जमाने की बेफिक्री जहां सुकून देती थी, वहीं आज के जमाने की जरा सी बेफ्रिकी लाख सुरक्षा इंतेजामों के बावजूद एक बड़ी भूल सिद्ध हो जाती है। यही इस डिजिटल दुनिया का सबसे बड़ा नुकसान है और इस फर्क को जन-जन को समझना होगा, तभी साइबर अपराधों के दंश से समाज को बचाया जा सकेगा।

सूचना व संचार क्रांति के इस युग में साफ तौर पर जनता की अनभिज्ञता, उदासीनता और लापारवाही साइबर अपराधियों के लिए सबसे बड़ा वरदान सिद्ध होती है। इसका मूल कारण यह है कि साइबर अपराध के मामलों में प्राय: पुलिस की भूमिका तब शुरु होती है जब अपराध उजागर हो जाता है, क्योंकि इसके पहले तो सब कुछ अपराधी और पीड़ित के बीच ऑनलाइन ही चलता रहता है। दरअसल साइबर अपराधी जनता के भोलेपन और अनभिज्ञता का सबसे ज्यादा फायदा उठाते हैं।

कम्प्यूटर, इन्टरनेट और स्मार्ट फोन के इस जमाने में हम सभी हमेशा साइबर सुविधाओं से घिरे रहते हैं। हमारा हर काम अब इन्हीं संसाधनों के जरिये निपटता है। चाहे टेक्सी बुक करना हो, फोन या बिजली का बिल भरना हो, सिनेमा की टिकिट बुक करनी हों, फूड ऑर्डर करना हो, हम छोटे से छोटा काम अपने कम्प्यूटर या स्मार्ट फोन/मोबाइल फोन से निपटाते हैं। मनोरंजन

के लिए इन्हीं डिवाइजों का प्रयोग करते हैं। हमारी दोस्ती भी इन्हीं डिवाइजों पर मौजूद विभिन्न सोशल मीडिया एप्लीकेशन्स पर चलती है। कामकाज तो पूरी तरह इंटरनेट पर निर्भर है ही, अब शिक्षा भी ऑनलाईन हो चली है तथा बैंकिग लेनदेन और खरीद-फिरोख्त भी इसी प्लेटफॉर्म से हो रहे हैं। कोविड-19 महामारी ने इलेक्ट्रॉनिक संचार, डिजिटल लेनदेन और सोशल मीडिया के प्रयोग को असीमित रुप से बढ़ा दिया है। यानी अब समाजिक, शैक्षणिक, आर्थिक और बाकी सभी तरह की गतिविधियां पूरी तरह से इंटरनेट के एक ऐसे मंच पर आ चुकी हैं, जहां कोई भी खुद के सुरक्षित होने का दावा नहीं कर सकता। इसका कारण यह है कि हैकर्स और साइबर अपराधी अपने पूरे ज्ञान और अनुभव का प्रयोग करते हुए हर समय इसी ताक में रहते हैं कि किसे, कब और कैसे निशाना बनाया जाए? इस बात में तनिक भी संदेह नहीं है कि हम में से अधिकांश लोग इलेक्ट्रॉनिक एवं डिजिटल सुविधाओं तथा विभिन्न सोशल मीडिया एप्लीकेशन्स और उपकरणों का इस्तेमाल तो सीख लेते हैं, लेकिन इनसे होने वाली संभावित हानियों की ओर कभी ध्यान ही नहीं देते और न ही उपयोग की सावधानियों को बेहतर ढंग से समझते व अमल में लाते हैं। इसी उदासीनता या अनभिज्ञता का नतीजा यह है कि साइबर अपराधों में साल-दर-साल बढ़ोत्तरी हो रही है।

स्पष्ट है कि केवल आर्थिक धोखाधड़ी और पहचान व डाटा की चोरी ही चिंता का विषय नहीं है, साइबर जगत में महिलाओं, बच्चों और समाज के विभिन्न वर्गों के लोगों के विरुद्ध भी गंभीर साइबर अपराध घटित हो रहे हैं। ऐसे में यदि जनता साइबर अपराधों और उनकी बदलती प्रवृत्ति के प्रति जागरुक नहीं होगी तो निश्चित रुप से साइबर अपराध के मामलों में दिन-ब-दिन वृद्धि होती जाएगी। पुलिस अन्वेषण करती रहेगी, साइबर अपराधी अपराधों को अंजाम देते रहेंगे और लोग उनकी शातिराना करतूतों का शिकार बनते रहेंगे।

इसीलिए आज के दौर में यह भी पुलिस की एक नैतिक जिम्मेदारी है कि वह जनता को साइबर अपराधों के प्रति निरंतर जागरूक बनाए रखे। पुलिस के ऐसे जागरूकता अभियानों के दूरगामी परिणाम होंगे। जब घर के बड़े और समझदार लोग साइबर अपराधों के प्रति जागरूक होंगे तो निश्चित रुप से वे आने वाली पीढ़ियों को भी साइबर जगत में सूझबूझ से काम लेने के लिए प्रेरित कर सकेंगे। ऐसे जागरूक और उत्तरदायी सामाजिक वातावरण में साइबर अपराधों में तेजी से गिरावट आएगी और पुलिस को अपनी दूसरी महत्वपूर्ण जिम्मेवारियों की ओर ध्यान देने का ज्यादा अवसर व सामर्थ्य मिल सकेगा। वहीं जनता और समाज के बीच पुलिस की विश्वसनीय छवि और ज्यादा मजबूत होगी तथा कानून-व्यवस्था कायम करने में पुलिस की कार्यप्रणाली पहले से ज्यादा प्रभावशाली बन सकेगी।

साइबर अपराधों को लेकर जनता के लिए जागरूकता अभियान चलाना अत्यंत महत्वपूर्ण कार्य है। इस दिशा में कुछ पुलिस संगठनों द्वारा किए गए अप्रतिम, अनुपम और अनुकरणीय प्रयासों का उल्लेख यहां बेहद प्रासंगिक है, ताकि इनसे प्रेरणा लेकर ऐसे ही और जन-जागरण अभियानों का मार्ग प्रशस्त हो सके-

- **विशाखापट्टनम पुलिस की अनूठी महिला हितेषी पहल : महिला मित्र और साइबर मित्र**

- **राचाकोंडा (आंध्रप्रदेश) में 'साइबर-योद्धा' अभियान की शुरुआत: साइबर अपराधों में लोगों की मदद की अनूठी पहल**

- **बंगलौर में एक महाविद्यालय में पुलिस द्वारा आयोजित जागरूकता अभियान**

- **दिल्ली पुलिस द्वारा दिल्ली यूनिवर्सिटी में आयोजित साइबर जागरुता कार्यक्रम, जिसमें 'BE CYBER SAFE' पुस्तक और इसके ई प्रारूप का विमोचन भी किया गया।**

- **छत्तीसगढ़ में बिलासपुर पुलिस ने कोराना संक्रमणकाल के दौरान बढ़ते साइबर अपराधों के लिए 8 दिवसीय जागरुकता कार्यक्रम "साइबर-मिशन" चलाया।**

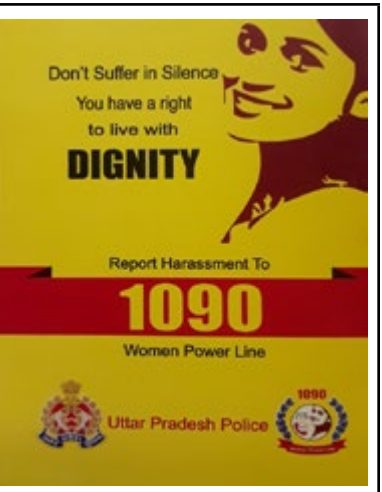
- **अण्डमान तथा निकोबार पुलिस द्वारा साइबर जागरुकता सप्ताह मनाया गया।**

- **नागपुर पुलिस द्वारा स्थानीय कन्या विद्यालय में चलाया गया साइबर जागरूकता कार्यक्रम**

- **पंजाब पुलिस ने विगत 20 नवम्बर 2020 को तीन माह तक चलने वाले साइबर सुरक्षा अभियान की शुरुआत की।**

विभिन्न पुलिस संगठनों द्वारा की गई कुछ अनूठी पहल

तेलंगाना पुलिस की महिला सुरक्षा विंग ने क्यू.आर.कोड स्केन के द्वारा शिकायत दर्ज करने की सुविधा कुछ इस तरह से प्रदान की है।



महिलाओं को प्रताड़ना के विरुद्ध शिकायत दर्ज करने के लिए उत्तर प्रदेश पुलिस द्वारा 1090 'वीमेन पॉवर लाईन' की सुविधा।

साइबर धोखाधड़ी से सचेत करता दिल्ली पुलिस का एक पोस्टर.

क्रेडिट/डेबिट कार्ड जालसाजी से सचेत करता साइबराबाद पुलिस का संदेश

कम्पनियों से आने वाले फर्जी ईमेल से आगाह करता पुणे पुलिस का संदेश

लोन धोखाधड़ी से सचेत करता गुजरात पुलिस का पोस्टर

विभिन्न पुलिस संगठनों द्वारा जन-जागरूकता के लिए चलाए जा रहे ये अभियान और प्रयास केवल सांकेतिक हैं। दरअसल राज्य का यह अहम दायित्व है कि वह अपने पुलिस संगठनों और अन्य संबंधित एजेंसियों के माध्यम से जनता में साइबर अपराधों की बदलती प्रकृति के बारे में निरंतर जागरूकता फैलाए। इसमें पुलिस की अगुवाई में अनेकानेक स्थानीय संस्थाओं का सहर्ष सहयोग प्राप्त हो सकता है। दरअसल पुलिस को साइबर अपराधों में कमी लाने के लिए सामाजिक स्तर पर एक अनुकूल माहौल विकसित करना होगा। सच तो ये है कि जब तक जनता में साइबर-समझ नहीं होगी, साइबर अपराधों पर अंकुश लगाना पुलिस के लिए एक बड़ी चुनौती बना रहेगा।

अध्याय 12

सारांशतया

विद्या वितर्को विज्ञानं स्मृतिः तत्परता क्रिया ।
यस्यैते षड्गुणास्तस्य नासाध्यमतिवर्तते ॥

भावार्थ यह है कि विद्या, तर्कशक्ति, विज्ञान, स्मृति-शक्ति, तत्परता, और क्रियाशीलता, ये छह गुण जिसके पास हैं, उसके लिए कुछ भी असाध्य नहीं है। आज की दुनिया के साइबर अपराधों के बारे में गहनता से सोचें तो आज हर इंसान को साइबर अपराधों से बचने और जूझने के लिए इन्हीं छह गुणों की सबसे ज्यादा आवश्यकता है। यानी कम्प्यूटर, इंटरनेट, स्मार्टफोन जैसे अत्याधुनिक संसाधनों के सुरक्षित इस्तेमाल के लिए हर व्यक्ति के पास पर्याप्त जानकारी (ज्ञान या विद्या), सही या गलत की पहचान की तर्कशक्ति, अपने उपकरण या संसाधन से जुड़ी तकनीकी जानकारी(विज्ञान), अच्छी याददाश्त (स्मृति-शक्ति), निर्णय की तत्परता और अपने हर संभव बचाव की क्रियाशीलता परमावश्यक है।

साइबर अपराधों पर अंकुश लगाने की पुलिस एवं सुरक्षा एजेंसियों की कोशिशों की राह में आने वाला सबसे बड़ा अवरोध साइबर सुरक्षा के प्रति लोगों में पर्याप्त जागरूकता की कमी है। जबकि सरकारों एवं पुलिस संगठनों द्वारा इस हेतु वेबसाइटों एवं दृश्य-श्रव्य विज्ञापनों के माध्यम से निरंतर प्रयास किए जा रहे हैं, फिर भी साइबर अपराधों का न रुकना अपने आप में इस बात का परिचायक है कि आज भी लोग अपनी अनभिज्ञता व अज्ञान की वजह से साइबर अपराधियों के नापाक इरादों का शिकार हो रहे हैं। आज के दौर में डिजिटल लेनदेन और इंटरनेट व सोशल मीडिया का

प्रयोग बेतहाशा बढ़ रहा है और इसी तेजी से साइबर अपराध भी बढ़ रहे हैं।

एक रिपोर्ट के अनुसार भारत में वर्ष 2020 में डिजिटल लेनदेनों में 80 फीसदी की बढ़त दर्ज की गई, वहीं यूपीआई ऐप्प (यूनिफाईड पेमेंट इंटरफेस एप्लीकेशन) के माध्यम से किए जाने वाले लेनदेनों में 120 फीसदी की बढ़त देखी गई है। इस बीच साइबर अपराधों की घटनाओं में 350 फीसदी की बढ़ोत्तरी दर्ज की गई है, जबकि सबसे ज्यादा लोग वैक्सीन बुकिंग और होम डिलेवरी के नाम पर ठगी का शिकार बताए जाते हैं।[1]

वैसे भी आज भारत दुनिया का दूसरा ऐसा देश है जहां इंटरनेट का प्रयोग करने वाली सबसे ज्यादा जनसंख्या रहती है। निसंदेह आज के डिजिटल-समाज पर साइबर ख़तरे भी बढ़ते ही जा रहे हैं। साइबर अपराधों के लिए किसी भी देश या प्रदेश की सरहदें कोई मायने नहीं रखती और इसीलिए सूचना व संचार प्रौद्योगिकी के विकास के साथ ही इन अपराधों में भी तेजी देखी जाती है।

कोरोना संक्रमणकाल में साइबर अपराधों की घटनाओं में बेहिसाब बढ़ोत्तरी हुई है। 'वर्क फॉर्म होम' का विकल्प उन लोगों का सौभाग्य है जिनके पास पक्की नौकरी है, लेकिन उनका क्या जो स्वयं का छोटा-मोटा व्यवसाय करके या इधर-उधर अस्थायी नौकरी करके अपना जीविकोपार्जन करते थे? निश्चित तौर पर वैश्विक महामारी के इस संक्रमणकाल में देश भर में बेरोजगारी और बेकारी बढ़ी हैं। वहीं लोग पूरी तरह से अपने कामकाज और मनोरंजन के लिए इंटरनेट सेवाओं एवं सूचना व संचार प्रौद्योगिकी से जुड़े साधनों पर निर्भर हो गए हैं। ऐसे में बेरोजगार और बेकार बैठे लोग, जिनके भीतर अपनी जरूरतों के लिए पैसा कमाने हेतु आपराधिक प्रवृत्तियां जागृत हो जाती हैं, कई बार साइबर अपराधों की राह पकड़ लेते हैं। दूसरी ओर घरों

1 https://www.patrika.com/crime-news/big-alert-digital-payment-80-and-cyber-crime-350-percent-increase-in-2020-6658741/

में बैठे साधन-सम्पन्न लोग अपने कम्प्यूटरों और स्मार्ट फोन आदि को मनो-विनोद का साधन समझ कर उस पर कुछ न कुछ नया प्रयोग करते रहते हैं और उन्हें यह पता भी नहीं चलता कि वे कब साइबर अपराधियों के नापाक इरादों का शिकार बन जाते हैं।

साइबर अपराधों की बढ़ती घटनाएं सीधे तौर पर ये दर्शाती हैं कि आज भी जनता के बीच सूचना व संचार प्रौद्योगिकी से जुड़े संसाधनों, जैसे-कम्प्यूटर, लेपटॉप, मोबाइल फोन, स्मार्ट फोन आदि तथा सोशल मीडिया और डिजिटल एप्लीकेशन्स के प्रयोग के बारे में जागरूकता की बेहद कमी है। इस पुस्तक के पिछले अध्यायों में केन्द्र सरकार द्वारा साइबर अपराधों से निपटने के लिए लागू किए गए सभी कानूनों, नियम-व्यवस्थाओं और उपलब्ध कराई गई संस्थागत सुविधाओं के बारे में विस्तार से चर्चा की गई है। साथ ही विभिन्न राज्यों द्वारा साइबर अपराधों की रोकथाम के लिए की गई व्यवस्थाओं की झलक भी पेश की गई है। इन सभी व्यवस्थाओं को समग्र दृष्टि से देखने पर यही महसूस होता है कि तेजी से बढ़ते साइबर अपराधों के मद्देनज़र अलग-अलग राज्यों में अभी भी साइबर अपराधों की रोकथाम के लिए आवश्यक विशिष्ट इंतजामों की कमी बनी हुई है। इसे ऐसे भी समझा जा सकता है कि आज भी भारत में हर जिले के स्तर पर साइबर अपराध थाने नहीं बनाए जा सके हैं, जो विशेषज्ञता के साथ इन मामलों की जांच कर सकें। इसी तरह विभिन्न प्रदेशों में अभी तक पर्याप्त मात्रा में साइबर फॉरेंसिंक प्रयोगशालाएं भी स्थापित नहीं की जा सकी हैं। वस्तुत: साइबर अपराध के मामले बहुत ही पेंचीदा किस्म के होते हैं, क्योंकि इनमें अपराधों को सूचना व संचार प्रौद्योगिकी के माध्यम से अंजाम दिया जाता है और पहली नज़र में अपराधी भी प्राय: अदृश्य व अज्ञात ही होता है। इसी प्रकार सोशल मीडिया माध्यमों से अंजाम दिए जाने वाले साइबर स्टॉकिंग/बुलिंग जैसे अपराध तथा नकली एकाउंट बना कर अंजाम दिए जाने वाले अपराध और महिलाओं तथा बच्चों के विरूद्ध अश्लीलता भरे अपराध भी बहुत ही पेंचीदा होते हैं,

जिनके अन्वेषण हेतु लम्बी व कठिन तकनीकी प्रक्रियाओं से गुजरना होता है। यानी साइबर अपराध अपनी प्रकृति से ही सामान्य अपराधों से बिल्कुल भिन्न होते हैं और इनके अन्वेषण के लिए न केवल संगत कानूनी प्रावधानों के विस्तृत ज्ञान, बल्कि ख़ास किस्म के प्रशिक्षण और तकनीकी अनुभव की भी आवश्यकता होती है। वहीं साइबर अपराधों की किस्में इतनी अनूठी हैं, कि उनके बारे में अंदाजा लगाना भी मुश्किल है, क्योंकि साइबर अपराधी देश व समाज में घटित होने वाली हर घटना को अपनी ठगी, जालसाजी और करतूतों का जरिया बना लेते हैं। मसलन- कोराना महामारी के आते ही, इन शातिर साइबर अपराधियों ने कभी होम डिलेवरी, तो कभी कोराना वैक्सीन या कोराना टेस्ट के नाम पर और कभी ऑनलाइन नौकरियों एवं ऑनलाइन शिक्षा के नाम पर लोगों को ठगना शुरु कर दिया था।

इन हालातों में न केवल साइबर अपराधों का अन्वेषण और रोकथाम पुलिस का अहम कर्तव्य है, बल्कि जन-जागरूकता फैलाना भी पुलिस का एक महत्वपूर्ण उत्तरदायित्व बन गया है। अपराधों के बढ़ते आंकड़े अक्सर पुलिस की कार्य-प्रणाली पर प्रश्न चिन्ह लगा देते हैं। यहां लोग अपनी गलतियों की वजह से अपराधों से ग्रसित होकर ये पूछते हैं कि आख़िर पुलिस क्या कर रही है? इसलिए पुलिस के लिए साइबर अपराधों के अन्वेषण से भी ज्यादा महत्व इस बात का है कि साइबर अपराधों को घटित होने से पहले ही कैसे रोका जाए? इस सवाल का केवल एक ही जवाब है और वो ये कि जनता को सबसे पहले साइबर अपराधों के प्रति जागरुक बनाना होगा। हालांकि इस दिशा में सभी राज्यों में कुछ न कुछ प्रयास किए जाते रहे हैं, लेकिन अभी भी पुलिस द्वारा जनता को जागरुक बनाने के लिए सतत रूप से अभियान चलाने की आवश्यकता है।

अब सवाल यह भी उठता है कि साइबर अपराधों से बचाव के लिए जनता को किस प्रकार जागरुक बनाया जाए? सही मायनों में जनता साइबर अपराधों

के प्रति तभी जागरुक हो सकेगी, जब उसे यह विश्वास होगा कि पुलिस स्वयं भी साइबर अपराधों के प्रति बहुत जागरुक है और जनता को इन अपराधों से बचाने के लिए पूरी तरह से तत्पर रहते हुए जनता से भी जागरुक रहने की अपेक्षा रखती है।

स्पष्ट है कि साइबर अपराधों से बचने के लिए जनता को पुलिस का साथ चाहिए और साइबर अपराधों की प्रभावी रोकथाम के लिए पुलिस को जनता का सहयोग चाहिए। इसलिए जहां तक साइबर अपराधों का प्रश्न है, पुलिस और जनता दोनों ही एक दूसरे के पूरक हैं। महत्वपूर्ण बात ये है कि इनमें से किसी एक के भी उदासीन होने पर नुकसान दोनों को ही भुगतना होगा। जहां एक ओर जनता को निजी क्षति पहुंचेगी, वहीं दूसरी ओर पुलिस की कार्यशैली पर प्रश्न चिन्ह लगेगा।

अतएव पुलिस बलों के लिए यह हितकर होगा कि वे अपने-अपने कार्यक्षेत्र में साइबर अपराधों के प्रति जनता को जागरुक बनाने के उद्देश्य से निरंतर अभिनव प्रयास जारी रखें। इसके लिए बुनियादी तौर पर दो तरीके अपनाए जा सकते हैं-

1. सतत् जन-संपर्क कार्यक्रम
2. आवश्यकतानुसार प्रदर्शन योग्य प्रिंटिग-सामग्री का इस्तेमाल और लोक-अवसरों पर विशेष बूथ के माध्यम से साइबर अपराधों के बारे में संक्षिप्त व सारगर्भित पब्लिक-अनाउंसमेंट।

इनमें से **पहले विकल्प** यानी 'जन-संपर्क' के ज़रिये साइबर अपराधों के प्रति जागरुकता फैलाने के उद्देश्य से पुलिस अपने कार्यक्षेत्र (खास तौर पर थाना-क्षेत्र) में स्थित विभिन्न स्थानीय संस्थाओं, जैसे- सरकारी व निजी प्रतिष्ठान, महाविद्यालय, स्कूल आदि के सहयोग से लोगों और छात्रों के लिए साइबर अपराध के जागरुकता अभियान/कार्यक्रम नियमित व सतत

रूप से आयोजित कर सकती है। साथ ही ऐसे अभियानों या आयोजनों का स्थानीय मीडिया के सहयोग से पर्याप्त प्रचार-प्रसार किया जा सकता है, ताकि इन जागरूकता कार्यक्रमों का संदेश और अहम जानकारियां जन-जन तक पहुंच सकें। इस मुहिम के लिए हर बार एक नया स्थान चुना जाना बेहतर होगा, ताकि साइबर अपराधों से जुड़ी जानकारियां नए लोगों तक पहुंच सकें। **दूसरे विकल्प** यानी प्रिंटिंग सामग्री एवं पब्लिक एनाउंसमेंट के लिए भी पुलिस बलों को स्थानीय आधार पर मुद्रण एवं विज्ञापन योग्य सामग्री जुटाते हुए सतत प्रयास करने चाहिए, क्योंकि प्रिंटिंग एवं दृश्य-श्रव्य माध्यम जनता के मन-मस्तिष्क पर गहरी छाप छोड़ते हैं।

जहां तक जनता को साइबर अपराधों से बचाव की सारगर्भित जानकारी देने का प्रश्न है, यह निसंदेह एक नियमित प्रक्रिया है और पुलिस का अहम उत्तरदायित्व है। परंतु, इसके लिए पुलिस को अब किसी विशेषज्ञ की तलाश करने की आवश्यकता नहीं है, क्योंकि इसी सूचना व संचार प्रौद्योगिकी ने पुलिस को ऐसे नायाब संसाधन उपलब्ध करा दिए हैं, जिनके ज़रिये पुलिस अपने ही विभाग में स्थानीय आधार पर कुछ प्रतिभावान अधिकारियों और निपुण कर्मियों की पहचान कर उन्हें विशेषज्ञ बना सकती है, जो साइबर अपराध के मामलों के निपटान तथा जन-जागृति के कार्य में अग्रणी भूमिका निभा सकते हैं। यहां फिर एक नया सवाल उठता है कि आख़िर जिला पुलिस के स्तर पर ये मानव-संसाधन किस प्रकार विकसित किए जा सकते हैं?

इस दिशा में पुलिस बलों द्वारा यदि जिला-स्तरीय पहल की जाए तो साइबर अपराधों की रोकथाम और प्रभावी अन्वेषण के उद्देश्य से यह सारी व्यवस्थाएं बहुत ही थोड़े प्रयासों से जुटाई जा सकती हैं, जिनमें भारत सरकार द्वारा उपलब्ध कराई निम्नलिखित ऑनलाईन सुविधाएं बेहद कारगर सिद्ध होंगी-

1) भारत सरकार गृह मंत्रालय द्वारा राष्ट्रीय साइबर अपराध प्रशिक्षण केन्द्र के तत्वावधान में संचालित 'ऑनलाइन शिक्षण-सह-प्रशिक्षण

पोर्टल'[2] बहुत ही उपयोगी है, जो हिंदी एवं अंग्रेजी दोनों भाषाओं के विकल्प के साथ हर समय उपलब्ध है। इस पोर्टल के माध्यम से आवश्यकतानुसार अधिकारियों एवं पुलिस कर्मियों को प्रशिक्षण दिला कर मैदानी अभियानों के नेतृत्व हेतु तैयार किया जा सकता है।

2) जहां तक जनता को साइबर अपराधों के बारे में प्रयोजन मूलक जानकारी देने का प्रश्न है, जन-जागरूकता के अभियानों में सबसे ज्यादा सहायक भारत सरकार का 'राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल' है, जो न सिर्फ जनता को साइबर अपराधों की ऑनलाइन शिकायत दर्ज करने की सुविधा उपलब्ध कराता है, बल्कि निम्नलिखित अहम जानकारियां भी तत्काल उपलब्ध कराता है-

- साइबर सुरक्षा पर छात्रों के लिए एक ई-पुस्तिका.
- माता-पिता के लिए साइबर जागरूकता और स्वच्छता के उपाय.
- किशोरों और युवा-व्यस्कों के लिए साइबर जागरूकता और स्वच्छता के उपाय.
- संगठनों के लिए साइबर जागरूकता और स्वच्छता के उपाय.
- सामान्यत: पूछे जाने वाले प्रश्न.
- सिटीजन मैनुअल.

आम तौर पर जनता इस प्रकार की ऑनलाईन सुविधाओं और जानकारियों के प्रति उतना सजग नहीं रहती है और पुलिसकर्मी अपने क्षेत्र में ये बहुमूल्य जानकारियां जन-जन तक पहुंचा कर देश में साइबर अपराधों की रोकथाम की प्रक्रिया को सुदृढ़ बना सकते हैं।

2 https://cytrain.ncrb.gov.in

इस पुस्तक में भी साइबर अपराध की अवधारणा, उदभव, इतिहास, विकासक्रम और प्रकारों के बारे में विस्तार से उल्लेख किया गया है, जो जन-जागरूकता के कार्यक्रमों में समर्थनीय सिद्ध हो सकता है।

3) भारत सरकार, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय के अधीन वर्ष 2004 में स्थापित 'भारतीय कम्प्यूटर आपात प्रतिक्रिया दल : CERT-In' की वेबसाइट भी इस दिशा में बहुत उपयोगी है। आज यह संस्थान भारत की साइबर सुरक्षा के क्षेत्र में एक राष्ट्रीय अग्रणी एजेंसी के रूप में कार्य कर रहा है, जिसके निम्नलिखित उद्देश्य हैं-

- साइबर घटनाओं के संबंध में सूचनाओं को एकत्र करना, उनका विश्लेषण करना और संबंधित एजेंसियों को अवगत कराना।
- साइबर सुरक्षा घटनाओं का पूर्वानुमान लगाना और चेतावनी जारी करना।
- साइबर सुरक्षा संबंधी घटनाओं से निपटने के लिए आपात उपाय करना।
- सूचना-सुरक्षा संबंधी कार्यकलापों, प्रक्रियाओं, रोकथाम एवं प्रतिक्रिया के बारे में दिशा-निर्देश, परामर्शी निदेश, सुभेद्यता टिप्पणियां तथा श्वेत पत्र जारी करना और साइबर दुर्घटनाओं की जानकारी देना।
- देश की साइबर सुरक्षा से संबंधित अन्य उपाय करना।

वस्तुत: इस संस्थान की वेबसाइट https://www.cert-in.org.in/ खास तौर पर पुलिस बलों के लिए इस नज़रिये से बहुत ही उपयोगी है, क्योंकि इसमें न केवल बड़े साइबर खतरों की चेतावनियां जारी की

जाती हैं, बल्कि बहुत सी उपयोगी जानकारियां भी प्रदर्शित की जाती हैं और बोटनेट व मालवेयर से निपटने के लिए 'साइबर स्वच्छता केन्द्र' की सुविधा भी नि:शुल्क ऑनलाईन सुरक्षा टूल के साथ उपलब्ध है। इससे भी महत्वपूर्ण बात यह है कि 'साइबर स्वच्छता केन्द्र' की इस वेबसाइट पर निम्नलिखित विशिष्ठ जानकारियां भी उपलब्ध हैं, जो समय-समय पर नवीनीकृत की जाती हैं तथा व्यापारियों, ग्राहकों एवं कम्पयूटर व मोबाइल प्रयोगकर्ताओं के लिए बहुत मददग़ार हैं-

- व्यापारियों के लिए डिजिटल भुगतान संबंधी सुरक्षा उपाय.
- ग्राहकों के लिए डिजिटल भुगतान संबंधी सुरक्षा उपाय.
- सुरक्षित डिजिटल भुगतान के लिए हिंदी व अंग्रेजी भाषा में वीडियो.
- पर्सनल कम्प्यूटर की सुरक्षा के उपाय.
- सामान्य प्रयोगकर्ताओं के लिए डेस्कटॉप/ब्रॉड-बैण्ड/यूएसबी/ मोबाइल फोन सुरक्षा के उपाय और फिशिंग हमले से बचने की तरकीबें।
- https://infosecawareness.in पोर्टल जहां बच्चों, छात्रों, महिलाओं, परिवारों, पुलिस, शिक्षकों, सरकारी कर्मचारियों और सिस्टम/नेटवर्क एडमिनिस्ट्रेटर्स के लिए कुल 10 भाषाओं में प्रशिक्षण एवं जागरूकता कार्यक्रम/कार्यशालाओं की ऑनलाइन सुविधा उपलब्ध है।

इस पोर्टल पर दी गई जानकारियां भी जन-उपयोगी है और साइबर अपराधों की रोकथाम में बेहद कारगार सिद्ध हो सकती है, अत: पुलिस के द्वारा इस प्रकार की ज्ञानवर्द्धक जानकारियां नियमित रुप से जन-जन तक पहुंचाई जानी चाहिए।

4) उपरोक्त के अलावा सामान्यतया पूछे जाने वाले प्रश्नों के उत्तर भी इस दिशा में अहम भूमिका निभा सकते हैं-

सामान्य प्रश्नोत्तर (Frequently Asked Questions)

प्रश्न 1 : साइबर अपराध क्या हैं?

उत्तर : साइबर अपराध ऐसे अपराध हैं, जो कम्प्यूटर और सूचना व संचार प्रौद्योगिकी से जुड़े संसाधनों के माध्यम से अंजाम दिए जाते हैं। ऐसे अपराधों में साइबर माध्यमों से जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, कंप्यूटर से व्यक्तिगत डेटा हैक करना, फ़िशिंग, अवैध डाउनलोडिंग, साइबर स्टॉकिंग, वायरस प्रसार, सहित कई प्रकार की गतिविधियाँ शामिल हैं।

प्रश्न 2 : साइबर अपराधों को मुख्य रूप से कितने भागों में विभाजित किया जा सकता है?

उत्तर : मोटे तौर पर हम साइबर अपराधों को तीन प्रमुख भागों में विभाजित कर सकते हैं-

1) व्यक्ति के विरुद्ध किए जाने वाले साइबर अपराध (जैसे- साइबर बुलिंग/स्टॉकिंग,अश्लीलता फैलाना, बाल यौन शोषण सामग्री का प्रसार व पारेषण)

2) संपत्ति के विरुद्ध किए जाने वाले साइबर अपराध (जैसे-हैकिंग, फिशिंग, डोस अटैक, वायरस/रेनसमवेयर अटैक, डाटा-चोरी आदि)

3) सरकार के विरुद्ध किए जाने वाले साइबर अपराध (जैसे- साइबर जासूसी और साइबर आतंकवाद)

प्रश्न 3 : साइबर अपराधियों की प्रवृत्ति को मुख्य रूप से कितनी श्रेणियों में बांटा जा सकता है?

उत्तर : प्रवृत्तियों को निम्न 5 श्रेणियों में बांटा जा सकता है-

1. ऐसे साइबर अपराधी जो शौकिया ही हैकिंग जैसे अपराध करते हैं।
2. ऐसे साइबर अपराधी जो हैकिंग जैसे अपराधों के जरिये राजनीतिक या अन्य गलियारों में नाम कमाना चाहते है।
3. ऐसे साइबर अपराधी जो विकृत मनोवृत्तियों के चलते साइबर अपराधों को अंजाम देते हैं।
4. ऐसे साइबर अपराधी जो धन कमाने के लिए साइबर अपराध करते हैं या किसी आर्थिक अपराध गिरोह से जुड़ कर संगठित साइबर अपराधों का हिस्सा बन जाते हैं।
5. ऐसे साइबर अपराधी जो बदले की किसी भावना से साइबर अपराधों को अंजाम देते हैं।

प्रश्न 4 : सूचना एवं संचार प्रौद्योगिकी का अपराध जगत पर क्या प्रभाव पड़ा है?

उत्तर : समय के साथ बदलते परिवेश में जैसे-जैसे मानव समाज उन्नत होता रहा, आपराधिक प्रवृत्तियां भी उन्नत होती चली गईं और नित्य-नए रूप में कानून-व्यवस्था के सामने चुनौती बन कर उभरने लगीं। सूचना व संचार क्रांति ने पूरे विश्व को बदल कर रख दिया है और अपराध जगत पर भी इसका प्रभाव स्वाभाविक रूप से देखा जा सकता है। सच कहें तो अपराध जगत ने अपने नापाक इरादों को कामयाब करने की कोशिशों में सूचना व संचार प्रौद्योगिकी का

सबसे जल्दी और सबसे तेज़ इस्तेमाल किया है। नतीजतन, पुराने समय के पारम्परिक अपराधों ने सूचना व संचार प्रौद्योगिकी का हाथ थाम कर नया तथा पहले से और भी ज्यादा भयावह रूप ले लिया है। जहां एक ओर सुरक्षा और कानून-व्यवस्था में कम्प्यूटर तथा सूचना व संचार प्रौद्योगिकी का अग्रणी रूप से प्रयोग किया जा रहा है, वहीं अपराधियों ने भी इसका बेजा इस्तेमाल कई वर्षों पहले ही शुरु कर दिया है। सूचना एवं संचार प्रौद्योगिकी से आपराधिक नेटवर्क को और ज्यादा मजबूती मिली है तथा विश्व भर में बढ़ते आतंकवाद, अलगाववाद, उग्रवाद एवं अन्य अपराधों में इसका प्रयोग खुल कर सामने आने लगा है। इसके अलावा, नशीले पदार्थों की तस्करी, मानव तस्करी, मानव अंगों की तस्करी, हथियारों की तस्करी जैसे संगीन व संगठित अपराधों में भी नई प्रौद्योगिकी के प्रयोग से गंभीर परिवर्तन आए हैं। हालांकि अपराधियों द्वारा प्रयुक्त यही अत्याधुनिक संसाधन उन पर कानून का शिकंजा कसने और उनका भंडाफोड़ करने में भी सहायक सिद्ध होते हैं और जब वे कानून की गिरफ्त में आ जाते हैं तो यही संसाधन उनके खिलाफ पुख्ता सबूत बन जाते हैं।

प्रश्न 5: बौद्धिक संपदा(Intellectual Property) से क्या तात्पर्य है और बौद्धिक संपदा के विरुद्ध अपराध क्या हैं?

उत्तर : ब्रम्हाण्ड के समस्त प्राणियों में मानव जाति को सर्वश्रेष्ठ माना गया है, क्योंकि मानव कुशाग्र बुद्धि का स्वामी है। वह रचना और सृजन का कार्य करता आया है। अपनी बौद्धिक क्षमताओं से उसने इस मानव सभ्यता को रचा है। यही सब उसकी बौद्धिक संपदा है। बौद्धिक संपदा की विषय-वस्तु में ऐसे सभी उत्पाद सम्मिलित हैं, जो मानव-मस्तिष्क की देन हैं। ये उत्पाद/वस्तुएं किसी व्यक्ति,

संगठन, संस्था समूह द्वारा निर्मित, रचित या सृजित कोई गद्य, पद्य या साहित्यिक रचना हो सकती है, संगीत हो सकता है या कोई कलात्मक वस्तु, खोज अथवा डिजाइन आदि हो सकता है। आधुनिक सूचना व संचार प्रौद्योगिकी के युग में अर्थव्यवस्था व्यवसायों एवं उद्यमों के लिए भी बौद्धिक संपदा का विशेष महत्व है। किसी व्यक्ति विशेष/संगठन/संस्था/समूह द्वारा अपनी बौद्धिक क्षमताओं से निर्मित वस्तुओं को स्वेच्छा/स्वप्रेरणा से किसी अन्य व्यक्ति, संस्था या संगठन को बेचा या सौंपा जा सकता है, किन्तु यदि इन वस्तुओं की निर्माण विधि, बनावट आदि की नकल की जाती है, या बिना अनुमति इन्हें मूल स्वरूप में ही प्रयोग किया जाता है या चुरा लिया जाता है तो यह कृत्य अपराध की श्रेणी में आता है और इसे बौद्धिक संपदा के विरुद्ध अपराध कहा जाता है। इन अपराधों की रोकथाम और बौद्धिक संपदा के अधिकार के हनन को रोकने के लिए भारत सरकार ने 12 मई 2016 को "राष्ट्रीय बौद्धिक संपदा अधिकार नीति" लागू की है।

प्रश्न : 6 साइबर अपराध जगत में सोशल मीडिया की क्या भूमिका है?

उत्तर : बड़े पैमाने पर सोशल नेटवर्किंग साइट्स का उपयोग करने वाली जनसंख्या साइबर अपराध के खतरों से अनजान है। विभिन्न सोशल नेटवर्किंग साइट्स के सर्वर अन्य देशों में केंद्रित हैं, जिससे यह डर बना रहता है कि कहीं ये देश लोगों की व्यक्तिगत जानकारी का दुरुपयोग न करें। विभिन्न सोशल नेटवर्किंग साइट्स पर लोग अपनी व्यक्तिगत जानकारियाँ साझा करते हैं, जिससे हैकर्स इन सोशल नेटवर्किंग एकाउंट्स को आसानी से हैक कर लेते हैं और फिर प्राप्त सूचनाओं का दुरुपयोग करते हैं। सोशल नेटवर्किंग साइट्स पर हैकर्स लोगों को ऑनलाइन ठगी का शिकार बनाते

हैं। यह भी अनुभव रहा है कि सोशल मीडिया को जरिया बना कर ऑनलाइन मुद्रा स्थानांतरित करने वाले विभिन्न ऐप्प के माध्यम से आतंकवादियों और देशविरोधी तत्वों को फंडिंग की जाती है। साइबर अपराधी विभिन्न ऑनलाइन गेम्स के माध्यम से बच्चों को अपराध करने के लिये प्रोत्साहित करते हैं। अत: सोशल मीडिया निसंदेह साइबर अपराधों की दुनिया में बहुत बड़ी भूमिका निभाती है।

प्रश्न : 7 आभासी दुनिया(Virtual World) में पुलिसिंग से क्या तात्पर्य है?

उत्तर : सोशल मीडिया जैसे- यू-ट्यूब, ट्विटर, फेसबुक एवं विभिन्न डॉट कॉम साईट्स का असामाजिक तत्वों, भटके हुए व हताश नौजवानों तथा राष्ट्रविरोधी तत्वों द्वारा जमकर दुरूपयोग किया जाता है। ऐसे लोग व्यवस्था के प्रति अपना गुस्सा जाहिर करने, सरकार एवं शासन-व्यवस्था के विरूद्ध जन-आक्रोश भड़काने के लिए इन संसाधनों का बेज़ा इस्तेमाल करते हैं और परिस्थितियों को बद से बदतर बनाने के लिए आम लोगों की धारणाओं को बदलने का दुस्साहस करते हैं। "आभासी दुनिया में पुलिसिंग" से तात्पर्य इसी क्षेत्र यानी वच्युअल वर्ल्ड में पुलिस के प्रभावशाली हस्तक्षेप से है, ताकि अपराध के इन्हीं माध्यमों के जरिये जानकारियां जुटा कर अपराधियों पर शिकंजा कसा जा सके। इतना ही नहीं इस प्रकार की पुलिसिंग आर्थिक एवं अन्य तकनीकी समर्थित अपराधों के अन्वेषण में भी बहुत ही सार्थक सिद्ध होती है। वस्तुत: विभिन्न घटनाओं में इंटरनेट तथा सोशल मीडिया नेटवर्क अकल्पनीय आसूचना एवं सूचनाएं उपलब्ध कराने में काफी हद तक मददग़ार सिद्ध होता है और इस क्षेत्र में पुलिसिंग सफलताओं के नित्य-नए कीर्तिमान स्थापित कर सकती है।

प्रश्न : 8 सूचना और संचार प्रौद्योगिकी पुलिस के लिए एक समस्या भी है और समाधान भी। इस कथन के क्या आधार हैं?

उत्तर : सूचना एवं संचार प्रौद्योगिकी से आए बदलावों से यदि सुरक्षा के बंदोबस्त पहले से कहीं ज्यादा बेहतर और मज़बूत हुए हैं तो इस बात से भी कदापि इंकान नहीं किया जा सकता कि सूचना व संचार प्रौद्योगिकी ने सुरक्षा ख़तरों की प्रकृति और विभीषिका दोनों में चुनौतीपूर्ण बदलाव किए हैं, जिनका सामना सीधे तौर पर पुलिस व सुरक्षा एजेंसियों को करना होता है। दरअसल प्रौद्योगिकी का विकास और प्रयोग दो कभी न खत्म होने वाली प्रक्रियाएं हैं और इनसे आने वाले समस्त बदलाव अनवरत रूप से सुरक्षा परिदृश्य को प्रभावित करते रहेंगे, यह तथ्य संदेह से परे है। अर्थात, सूचना व संचार प्रौद्योगिकी यदि अपने साथ सहूलियतें लाई है तो इससे पैदा होने वाले ख़तरों की गंभीरता और बहुलता को भी नजरअंदाज नहीं किया जा सकता। सही मायनों में सूचना व संचार प्रौद्योगिकी ही पुलिस के लिए आधुनिक परिवेश की सबसे बड़ी भावी चुनौती है, जिसके मूल में ही सुरक्षा ख़तरों का निवारण भी छिपा है। यानी तकनीकी का मुकाबला तकनीकी से ही संभव है। अतएव आधुनिक सुरक्षा परिदृश्य में नई प्रौद्योगिकी पुलिस के लिए एक समस्या भी है और समाधान भी।

प्रश्न 9 : साइबर अपराधों से निपटने के लिए भारत में क्या-क्या कानूनी व सुरक्षा प्रबंध किए गए है?

उत्तर : विभिन्न साइबर अपराधों से निपटने के लिए भारत सरकार द्वारा निम्नलिखित कानूनी एवं सुरक्षा संबंधी बंदोबस्त किए गए हैं-

1) 'सूचना प्रौद्योगिकी अधिनियम, 2000(यथासंशोधित 2008) लागू किया गया है, जिसकी धाराएं-43, 43ए, 66, 66बी, 66सी, 66डी, 66ई, 66एफ, 67, 67ए, 67बी, 70, 72, 72ए और 74 हैकिंग तथा अन्य कई किस्म के साइबर अपराधों के लिए दण्ड का प्रावधान करती हैं। इन अपराधों पर प्रकृति एवं गंभीरता के अनुसार भारतीय दंड संहिता-1860, भारतीय साक्ष्य अधिनियम-1872, कॉपीराइट अधिनियम-1957, लैंगिक अपराधों से बालकों का संरक्षण अधिनियम(पॉस्को एक्ट)-2012, सरकारी गोपनीयता अधिनियम-1923, कम्पनी अधिनियम-1956 एवं कम्पनी अधिनियम-2013, भारतीय रिजर्व बैंक अधिनियम-1934 बैंकर्स बुक एविडेन्स अधिनियम-1991, स्वापक औषधि और मन:प्रभावी पदार्थ अधिनियम-1985 और आयुध अधिनियम-1959 भी आवश्यकतानुसार लागू होते हैं।

2) वर्ष 2004 में भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (CERT-in) की स्थापना की गई।

3) वर्ष 2013 में 'राष्ट्रीय साइबर सुरक्षा नीति-2013' लागू की गई।

4) वर्ष 2014 'राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र(NCIIPC)' की स्थापना की गई।

5) वर्ष 2015 में 'राष्ट्रीय साइबर समन्वय केन्द्र(NCCC) की स्थापना की गई।

6) वर्ष 2017 में 'साइबर स्वच्छता केन्द्र' के रुप में वेबसाइट आरंभ की गई।

7) वर्ष 2017 में ही गृह मंत्रालय में 'साइबर एवं सूचना सुरक्षा प्रभाग' की स्थापना की गई।

8) वर्ष 2019 में 'राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल' की स्थापना की गई।

9) वर्ष 2019 में 'रक्षा साइबर एजेंसी(Defence Cyber Agency)' की स्थापना की गई।

10) वर्ष 2020 में 'भारतीय साइबर अपराध समन्वय केन्द्र(I4C) की स्थापना की गई।

11) वर्ष 2020 में जन-जागरण हेतु 'साइबर दोस्त' नामक ट्विटर हैंडल आरंभ किया गया।

12) इलेक्ट्रानिकी और सूचना प्रौद्योगिकी मंत्रालय द्वारा सूचना सुरक्षा शिक्षा और जागरूकता(Information Security Education & Awareness) परियोजना वर्ष 2015 से 2020 के लिए लागू की गई थी। इसके अंतर्गत एक बहुभाषी वेब पोर्टल और विशिष्ठ यूज़र फ्रेंडली सुविधा उपलब्ध थी, जिससे बच्चों, छात्रों महिलाओं, परिवारों, पुलिस कर्मियों, शिक्षकों, सरकारी कर्मचारियों और सिस्टम/नेटवर्क एडमिन को जागरुक बनाया जा सके।

प्रश्न: 10 'भारतीय साइबर अपराध समन्य केन्द्र' की क्या भूमिका है?

उत्तर : भारतीय साइबर अपराध समन्वय केंद्र जनवरी 2020 में गृह मंत्रालय द्वारा साइबर क्राइम से निपटने के लिये 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cyber Crime Coordination Centre-I4C) की स्थापना की गई है।

इस योजना को संपूर्ण भारत में लागू किया गया है। साइबर अपराध से बेहतर तरीके से निपटने के लिये तथा I4C को समन्वित और

प्रभावी तरीके से लागू करने हेतु इस योजना के निम्नलिखित सात प्रमुख घटक है-

- o नेशनल साइबरक्राइम थ्रेट एनालिटिक्स यूनिट (National Cybercrime Threat Analytics Unit)
- o नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल (National Cyber Crime Reporting Portal)
- o संयुक्त साइबर अपराध जाँच दल के लिये मंच (Platform for Joint Cyber Crime Investigation Team)
- o राष्ट्रीय साइबर अपराध फोरेंसिक प्रयोगशाला पारिस्थितिकी तंत्र (National Cyber Crime Forensic Laboratory Ecosystem)
- o राष्ट्रीय साइबर क्राइम प्रशिक्षण केंद्र (National Cyber Crime Training Centre)
- o साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट (Cyber Crime Ecosystem Management Unit)
- o राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र (National Cyber Research and Innovation Centre)

प्रश्न : 11 कृत्रिम बुद्धिमत्ता (Artificial Intelligence) क्या है?

उत्तर : बुद्धिमत्ता मानव की वो सबसे विलक्षण प्रतिभा है, जिसके दम पर मानव आज इस दुनिया पर राज कर रहा है। मानव ने अपनी बुद्धिमत्ता से निरंतर आगे बढ़ते हुए आज दुनिया को वो रुप दे दिया है, जिसकी उसने कभी खुद भी कल्पना नहीं की थी। विज्ञान

और प्रौद्योगिकी इस संसार को नित्य नई सौगाते दे रहे हैं। कम्प्यूटर विज्ञान ऐसी ही एक सबसे बहूमल्य सौगात है, जिसे और ज्यादा प्रखर व उपयोगी बनाने के लिए मानव निरंतर प्रयत्नशील बना हुआ है। शनै: शनै: हम अपने सब कामकाज कम्प्यूटर आधारित प्रणालियों को सौंपते जा रहे हैं। धीरे-धीरे हमारे हाथ खाली और दिमाग व्यस्त होने लगा है। अब प्रश्न ये था कि जब सब काम कम्प्यूटर आधारित मशीनों से हो रहा है तो फिर सोचने का काम ही मानव के पास क्यों रह जाए। इसी जिज्ञासा ने मनुष्य को ये पहल करने की ओर प्रवृत्त कर दिया कि क्यों न कम्प्यूटर प्रणाली को इस काबिल बनाया जाए कि वह मानव की तरह सोच-विचार कर कार्य कर सके और आख़िरकार मानव ने यह भी संभव कर दिखाया। मानव की तरह सोच कर काम करने की कम्प्यूटर पद्धतियों की इसी विलक्षणता को कृत्रिम बुद्धिमत्ता यानी आर्टिफीशियल इन्टेलीजेंस का नाम दिया गया। सच तो ये है कि हम कभी इस बात पर गौर नहीं फरमाते कि हम लगभग रोज इस 'कृत्रिम बुद्धिमत्ता' तकनीकी से संचालित होने वाली कई एप्लीकेशन्स का उपयोग करते हैं। गूगल मैप, ऑन लाईन शॉपिंग, सर्च इंजन, एलेक्सा (वॉइस कमाण्ड ने चलने वाला डिवाइज) और स्वचलित कार 'टेलसा' इसके बेहतरीन उदाहरणों में से हैं।

प्रश्न :12 इंटरनेट ऑफ थिंग्स किसे कहते हैं?

उत्तर : इंटरनेट ऑफ थिंग्स (IoT) उन उपकरणों का एक समूह है जो इंटरनेट से जुड़े होते हैं। इन उपकरणों में वायरलैस सेंसर, सॉफ्टवेयर, ऐक्ट्यूऐटर और कम्प्यूटर डिवाइज शामिल होते हैं। यानी इंटरनेट ऑफ थिंग्स एक तरह की नेटवर्किंग को कहा जाता है। इस नेटवर्किंग में आपके उपयोग के सभी गैजेट्स और इलेक्ट्रॉनिक डिवाइसेज एक

दूसरे से कनेक्ट होते हैं। यह टेक्नोलॉजी बेहद उपयोगी और कारगर है। इस टेक्नोलॉजी ने हमारी रोजमर्रा की जिन्दगी को बेहद आसान बना दिया है। इसे आसान भाषा में एक उदहारण के जरिए समझाया जा सकता है। इंटरनेट ऑफ थिंग्स के अंतर्गत आपका एक डिवाइज आपके घर, किचन आदि में मौजूद अन्य डिवाइसेज को कमांड देता है। इस तरह से एक डिवाइस को इंटरनेट के साथ लिंक कर के बाकी डिवाइसेज से अपने अनुसार कुछ भी काम करवाया जा सकता है।

प्रश्न : 13समय की मांग क्या है?

उत्तर : आधुनिक सुरक्षा परिदृश्य में पुलिस को प्रभावशाली, सक्षम व सफल बनने के लिए सूचना व संचार प्रौद्योगिकी के प्रयोग को सतत और कुछ ऐसे परिणामोन्मुखी ढंग से बढ़ावा देना होगा कि पुलिस अपराधियों से सदैव दो कदम आगे रहे। इसके लिए सबसे जरूरी है कि पुलिस के प्रशिक्षण कार्यक्रमों में हर स्तर पर साइबर अपराधों की बदलती प्रवृत्ति और अपराध जगत में सूचना व संचार प्रौद्योगिकी के बढ़ते प्रयोग संबंधी ज्ञान एवं अभ्यास का समावेश किया जाए और साथ ही साथ नए जमाने के प्रौद्योगिकी समर्थित अपराधों और आंतकवाद एवं चरमपंथ की अवधारणाओं से पुलिस के अधिकारियों एवं कर्मियों को अपडेट रखा जाए। इसके आलावा केन्द्रीयकृत रूप से योजना बनाते हुए सूचना व संचार प्रौद्योगिकी के क्षेत्र में अवतरित होने वाले नए-नए उपकरणों व संसाधनों की समीक्षा, विश्लेषण एवं इस्तेमाल के तौर-तरीकों से भी निचले स्तर तक पुलिस कर्मियों को निरंतर अवगत कराया जाए, ताकि वे तकनीकी ज्ञान के आभाव में साइबर अपराधों से लड़ने में खुद को असमर्थ न समझें, यही समय की मांग है।

पं. गोविन्द वल्लभ पंत पुरस्कार योजना के अंतर्गत ब्यूरो द्वारा प्रकाशित पुस्तकें

क्र.सं.	पुस्तक का नाम	लेखक का नाम
1	भारतीय पुलिस का इतिहास (अतीत काल से मुगल काल तक)	डॉ. शैलेन्द्र कुमार चतुर्वेदी
2	भारत में केन्द्रीय पुलिस संगठन	श्री एच भीष्मपाल
3	विकासशील समाज में समसामयिक पुलिस की भूमिका	प्रो. आर.एस. श्रीवास्तव
4	ग्रामीण पुलिस–समस्याएं एवं समाधान	श्री रामलाल विवेक
5	ग्रामीण पुलिस–समस्याएं एवं समाधान	श्री शंकर सरोलिया
6	मादक पदार्थ–पुलिस की भूमिका	डॉ. हरीश नवल
7	स्वातंत्रयोत्तर भारत में जनता का उत्तरदायित्व तथा पुलिस की भूमिका	डॉ. कृष्ण मोहन माथुर
8	सामाजिक चेतना के परिप्रेक्ष्य में पुलिस की भूमिका का उदभव	प्रो. मीनाक्षी स्वामी
9	समग्र न्याय व्यवस्था में पुलिस का स्थान एवं भूमिका	ललितेश्वर
10	पुलिस दायित्व एवं नागरिक जागरूकता	डॉ. सी. अशोक वर्धन
11	मानवाधिकार एवं पुलिस एक समीक्षा	डॉ. जी एस वाजपेयी
12	नई आर्थिक नीति एवं अपराध	डॉ. अर्चना त्रिपाठी
13	महिलाएं और पुलिस	श्रीमती अमिता जोशी
14	बाल–अपराध	श्री गिरिश्वर मिश्र
15	न्यायायिक विज्ञान की नई चुनौतियां	डॉ. शरद सिंह
16	नई सहस्त्राब्दि में पुलिस कैसी हो...	डॉ. अजय शंकर पांडेय
17	सामुदायिक पुलिस व्यवस्था	डॉ. तपन चक्रवर्ती एवं डॉ. रवि अम्बष्ट
18	भारत में मानवाधिकार–संरक्षण एवं पुलिस	डॉ. रामकृष्ण दत्त शर्मा एवं डॉ सविता शर्मा
19	संगठित अपराध	श्री महेन्द्र सिंह आदिल
20	पुलिस कार्यों का निजीकरण	डॉ. शंकर सरोलिया
21	साइबर क्राइम	डॉ. अनुपम शर्मा
22	अपराधों की रोकथाम और प्रौद्योगिकी का इस्तेमाल	डॉ. निशांत सिंह
23	अपराध पीड़ित महिलाओं की समस्याएं	डॉ. उपनीत लाली एवं डॉ. ऋता तिवारी
24	व्यावसायिक यौनकर्मियों का सुधार एवं पुनर्वास	श्रीमती नीना लाम्बा
25	वैध समस्याओं के निदान हेतु बढ़ती हिंसा प्रवृत्ति	श्री राकेश प्रकाश

26	बंदियों का सुधार एवं पुनर्वास	प्रो. दीप्ती श्रीवास्तव
27	आतंकवाद एवं जन साझेदारी	श्री विश्वेश प्रकाश
28	महिला कैदी एवं जेल व्यवस्था	श्रीमती अदिती
29	नक्सलवाद और पुलिस की भूमिका	श्री राकेश कुमार सिंह
30	पुलिस नेतृत्व	डॉ. प्रशांत चौबे
31	महिला पुलिस से अपेक्षाएं	डॉ. अनुपम चौबे
32	अपेक्षित परिवर्तन में महिलाओं की भूमिका	डॉ. मंजू देवी
33	पर्यावरण और प्राकृतिक संसाधनों के संरक्षण में पुलिस की भूमिका	डॉ. पंकज श्रीवास्तव एवं नीतू मिश्रा
34	अपराध नियंत्रण में न्यायपालिका की भूमिका	डॉ. अदिती मिश्र
35	महिलाओं के विरूद्ध अपराध की रोकथाम हेतु पुलिस में परिवर्तन	श्रीमती मंजूला वर्मा
36	वरिष्ठ नागरिकों के प्रति पुलिस का व्यवहार	श्री ललितेश्वर
37	नई प्रौद्योगिकी और पुलिस	श्री राजेश प्रताप सिंह
38	स्मार्ट पुलिसिंग	डॉ. प्रशान्त चौबे
39	आर्थिक अपराध तथा पुलिस	डॉ. जालम सिंह
40	बन्दी कल्याण एवं निःशुल्क कानूनी सहायता	डॉ. सरिता भवानी मालवीय
41	साइबर फॉरेंसिक	डॉ. राकेश प्रकाश
42	साईबर अपराध और पुलिस की तैयारियां	श्री दीपक सक्सेना

पुलिस अनुसंधान एवं विकास ब्यूरो
गृह मंत्रालय, राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली - 110 037 द्वारा प्रकाशित एवं मुद्रित

BPRDIndia bprdindia officialBPRDIndia Bureau of Police Research & Development India www.bprd.nic.in