आधुनिक साइबर अपराधको उद्देश्य, कारण तथा समस्या समाधानका उपायहरू

अधिवक्ता गम्भीर बहादुर हाडा
LL.B, M.A. Economic (TU)
सह-प्राध्यापक, अर्थशास्त्र
भक्तपुर बहुमुखी क्याम्पस (अवकासप्राप्त)
Email: gambhirhada@gmail.com

***Article History :** 2025 Septermber 3*

सार (Abstract)

सामान्य अर्थमा कम्प्युटर, इन्टरनेट अपराध र दुरूपयोग नियन्त्रण एवम् निराकरण सम्बन्धि कानुनलाई साइबर कानुन (Cyber Law) भनिन्छ । साइबर कानुनले इन्टरनेट सम्बन्धी अपराध नियन्त्रण गर्न मद्दत गर्दछ । साइबर कानुनले विद्युतिय माध्यमबाट हुने कारोबारलाई वैधता प्रदान गरेर विभिन्न किसिमका इलेक्ट्रोनिक जालसाजी (fraud) नियन्त्रण एवम् निराकरण, साइबर अपराधीलाई कानुनबमोजिम कारबाही आदिद्वारा इन्टरनेट सम्बन्धी अपराध नियन्त्रण गर्दछ । त्यसैले साइबर कानुन महत्त्वपूर्ण छ । हामी कम्प्युटर इन्टरनेटले चलेको समाजमा बाँचिरहेका छौं । कम्प्युटरको कार्य तीव्रता र विश्वसनीयताले हाम्रो दैनिक जीवनलाई सजिलो र आरामदायी बनाइदिएको छ । सञ्चार प्रविधिको आगमनले हाम्रो जीवनमा नयाँ आयाम थपिदिएको छ, तर हरेक नयाँ आयाम सँगसगै नयाँ चुनौतीहरू पनि थपिँदै गइरहेका छन् । सूचनाको बढ्दो आदानप्रदानले गर्दा कतिपय समस्याहरू पनि निम्तिरहेका छन् । केही प्रमुख समस्याहरू, जस्तैः ह्याकिङ (hacking), बौद्रिक सम्पत्ति चोरी, साइबर बदमासी (Cyber bullying), गोपयनीयता भङ्ग आदि व्याप्त छन् ।

कुनै पनि कम्प्युटर, इन्टरनेटको दुरूपयोग वा इलेक्ट्रोनिक जालसाजी जस्ता गतिविधिलाई साइबर अपराध (Cyber Crime) भनिन्छ । अर्को शब्दमा कुनैपनि कम्प्युटर, इन्टरनेट जस्ता सूचना प्रविधिका साधनहरु प्रयोग गरेर हुने गलत र गैरकानुनी कार्यलाई साइबर अपराध भनिन्छ । यस्ता गलत क्रियाकलापहरुलाई रोकथाम गर्न ल्याइएको कानुनलाई साईबर कानुन भनिन्छ । साइबर कानुनले इन्टरनेट सम्बन्धी अपराध विद्युतीय कारोबार ऐन २०६३ ले कम्प्युटर तथा साइबर अपराधसँग सम्बन्धित मुद्दाहरूलाई सम्बोधन गर्नका लागि अलग न्यायिक अङ्गहरू; सूचना प्रविधि न्यायीकरण (Information Technology Tribunal), सञ्चार प्रविधि पुनरावेदन न्यायाधिकरण (Information Technology Appellate Tribunal) को व्यवस्था गरेको छ । न्यायाधिकरणले प्रारम्भिक मुद्दाहरू हेर्ने र पुनरावेदन न्यायाधिकरणले जटिल एवम् महत्त्वपूर्ण मुद्दाहरू हेर्ने व्यवस्था गरिएको छ । सन् २०१४ मा अमेरिकी सङ्घीय अनुसन्धान ब्यूरोमा २ लाख ६९ हजार ४२२ यस सम्बन्धी उजुरी दर्ता भएका थिए । सन् २०१८ मा प्रकाशित म्याफियो नामक संस्थाको प्रतिवेदन अनुसार साइबर क्राइमका कारण विश्वमा सो अवधिमा मात्र ६०० मिलियन अमेरिकी डलर बराबरको आर्थिक नोक्सानी भएको थियो। 'साइबर टेरोरिज्म'को नामले समेत लिइने यस अपराधलाई नियन्त्रण गर्न अमेरिकामा एफ.बि.आइ., सि.आइ.ए. जस्ता सरकारी निकायले करोडौं डलर खर्च गर्ने गरेका छन् ।

साइबर अपराधको क्षेत्रमा देखिएका उल्लेखित समस्याहरुलाई समयमै सम्बोधन गर्नको लागि उपयुक्त कानूनी, स्वागत र संरचनागत संरचनाको निर्माण गर्नुपर्ने हुन्छ जसबाट मात्र वर्तमान र भावी दिनहरुमा हुन सक्ने साइबर अपराध विरुद्धको अभियानलाई प्रभावकारी बनाउन सकिन्छ र साईबर सुरक्षित समाजको निर्माण गर्न सकिन्छ । विद्युतीय कारोबार ऐन, २०६३ को संशोधन वा परिमार्जन गरी वा साईबर अपराध नियन्त्रण सम्बन्धी नयाँ कानूनको निर्माण गरी साईबर अपराध नियन्त्रण सम्बन्धी सबल कानून व्यवस्था गर्ने, साइबर सुरक्षा नीति, २०८० लगायतका नीति कानूनको प्रभावकारी कार्यान्वयन गर्ने कार्य जरुरी देखिएको छ । नेपाल प्रहरी लगायतका सुरक्षा संगठनले संगठन भित्र क्रियाशील संयन्त्रहरुलाई समयानुकुल वैज्ञानिक, परिमार्जन र सशक्त बनाउँदै लैजानुपर्ने, साईबर सुरक्षाको महत्व, यसका जोखिम र बच्ने उपाय सम्बन्धमा नागरिकस्तरमा जनचेतना जगाउनुपर्ने, साईबर अपराध अनुसन्धानमा क्रियाशील जनशक्तिलाई समसामयिक रुपमा तालिमको व्यवस्था गरी क्षमतावान बनाउनुपर्ने, साईबर अपराध नियन्त्रण सम्बन्धमा भएका विश्वव्यापि असल अभ्यास (International best practice) को खोजी र सोको अनुकरण गर्नुपर्ने, फेसबुक, युट्युब लगायतका सामाजिक सञ्जालको सम्पर्क कार्यालय नेपालमा खोल्न पहल गर्नु आवश्यक छ । (अनुसन्धान र नियमनलाई सहज बनाउँछ। सरोकारवाला निकाय तथा अन्तर्राष्ट्रियस्तरमा समन्वय, सहकार्य र साझेदारी अगाडी बढाईनुपर्ने, साईबर अपराध सम्बन्धी मुद्दा काठमाण्डौ जिल्ला अदालतका अतिरिक्त अन्य अदालतबाट पनि सुनुवाई हुने व्यवस्था गर्ने, Telephone Service Provider कम्पनीहरूका CDR, SMS, Subscriber Details लगायतका विवरणहरूको Mirroring (read only format) अनुसन्धानको आवश्यकतानुसार सम्बन्धित निकायले उपयोग गर्न सक्ने कानूनी व्यवस्था गर्नुपर्ने, Internet Service Provider हरूको आवश्यकता अनुसार session history, subscriber details लगायतका अन्य डाटाहरूको Mirroring (read only format) मा अनुसन्धानकर्ताले कानूनबमोजिम प्रयोग गर्न सक्ने व्यवस्था गरिनुपर्ने आवश्यकता रहेको छ ।

संगठित अपराध सामान्यतया: आर्थिक वा अन्य लाभका लागि उच्च मागमा रहेको गैर कानूनी वस्तु वा सेवाको आपूर्ति गरी निरन्तर गरिने आपराधिक उद्यम हो । जुन राष्ट्रसेवकलाई भ्रष्टाचारमा सहभागी गराई वा अन्य किसिमका डर त्रास देखाई यस्ता कार्य गरिन्छ । संगठित अपराध आफैमा कुनै स्वतन्त्र वा खास अपराध होइन बल्की कुनै गम्भीर अपराध गर्नका लागि संगठित भएर गरिने क्रियाकलाप (Organized Criminal Behavior) हो । खासगरी अवैध सेवा (जस्तै मानववेचविखन) अवैध वस्तु (जस्तै बन्यजन्तु खरिद बिक्री) र बैध व्यवसायमा अवैध तरिका (infiltration of legitimate business) (जस्तै वैध कामदारहरूलाई धम्की दिई पैसा उठाउने) जस्ता कार्य पहिचान गरिएका छन् । कुनै गम्भीर कसूर संगठित अपराधको परिभाषाभित्र पर्नका लागि अपराधिक समूहबाट संगठित भएर गरिने अपराधिक क्रियाकलाप हो । यसका लागि अपराधिक समूहको निर्देशनमा अपराधिक समूहको तर्फबाट अपराधिक समूहसँग मिलेर वा अपराधिक समूहको तर्फबाट कार्य गरेको देखिनुपर्छ । कसूर गर्ने तरिका (modus operandi) संगठित नरहेमा संगठित अपराधको परिभाषाभित्र पर्न सक्दैन ।

संगठित अपराध भन्नाले योजना, तयारी, सङ्गठन संजाल, पर्याप्त स्रोत साधन सहित धेरै व्यक्तिहरु सङ्गठित भई मिलेर गरिने एक वा एक भन्दा बढी गम्भीर किसिमको अपराध गर्ने कार्यलाई सङ्गठित अपराध भनिन्छ । यस्तो सङ्गठित अपराध सीमाविहिन, सङ्गठित र योजनाबद्ध रुपमा हुने गर्दछ। सङ्गठित अपराध नियोजित एवं योजनाबद्ध अपराध हो, जुन सम्पूर्णत: वा साधारण अपराध भन्दा गम्भीर हुन्छ। एक व्यक्तिले गरेको कसुर भन्दा फरक हुन्छ । व्यक्ति वा समूहले नै गरेको कसुर भए पनि निश्चित चरित्र वा ढाँचा नभएसम्म त्यो सङ्गठित अपराध मानिँदैन । सैद्धान्तिक रुपले प्रभावित नभएको आपराधिक गतिविधि, पदसोपान सहित (श्रेणीबद्ध रुपमा) संगठित, दक्ष जनशक्ति (पेसागत दक्षता) र क्षेत्र (कार्य) विभाजन सहित संगठित, निश्चित नियमअनुरूप संचालित आपराधिक गतिविधि, स्वेच्छाचारी वा एकछत्र रुपमा गरिने अपराध, पेसेबर अपराधीलाई सदस्य बनाउने प्रवृत्ति वा प्रक्रिया नै सङ्गठित अपराध हो ।

संगठित अपराध अन्तर्गत बिद्युतीय अपराध, बेचबिखन, मिलेमतो र एकाधिकार, आतङ्कवाद, भ्रष्टाचार र अवैध मुद्रा निर्मलीकरण आदि जस्ता शब्दहरु यस अन्तर्गत पर्दछन् ।

संगठित अपराध अन्तर्गत **साइबर अपराध कानूनहरुमा नेपालको विद्युतीय कारोबार ऐन २०६३ अनुसार नेपालमा साइबर अपराध अन्तर्गत निम्न कुराहरु पर्दछन् ।** अर्काको बारेमा अपमानजनक टिप्पणी गर्ने, अर्काको गोप्य कुरा प्रसार गर्ने । मानिसमा घृणा उत्पन्न गर्ने, भड्काउने, जातिय, धार्मिक, विभाजन ल्याउने जस्ता सामग्री राख्ने, मोबाइलबाट धम्की दिने, यौन उत्तेजना पैदा गर्ने तस्बिर राख्ने, अरुको नाममा खाता खोलेर दुःख दिने, इन्टरनेटबाट अरुलाई ठगी गर्ने तथा धोका दिने, अर्काको कम्प्युटर तथा विद्युतीय उपकरणमा क्षती पुऱ्याउने, अर्कालाई जिस्काउने र चरित्र हत्या गर्ने आदि । साइबर अपराध, कानून र सजाय सम्बन्धी जानकारी लिने/दिने कार्यहरु पनि यस ऐन अन्तर्गत पर्दछन् ।

विद्युतीय कारोबार ऐन, २०६३ को दफा ४४ देखि ५९ ले साइबर अपराध र सजायको स्पष्ट परिभाषा र व्याख्या गरेको छ । जस्तै : कम्प्युटर स्रोत सङ्केतको चोरी, नष्ट वा परिवर्तन गर्ने, कुनै व्यक्तिले कुनै कम्प्युटर, कम्प्युटर कार्यक्रम, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्कका लागि प्रयोग हुने कम्प्युटर स्रोतको सङ्केत (सोर्स कोड) लाई चोरी गरेमा, नष्ट गरेमा, परिवर्तन गरेमा वा त्यस्तो काम गर्न लगाएमा निजलाई तीन वर्षसम्म कैद वा दुई लाख रूपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।

कम्प्युटर सामग्रीमा अनधिकृत पहुँचमा कम्प्युटरको धनी वा जिम्मेवार व्यक्तिबाट कुनै अख्तियारी नलिई सो कम्प्युटरको प्रयोग गरेमा वा अख्तियारी लिएको अवस्थामा पनि अख्तियारी दिइएको भन्दा भिन्न कुनै कार्यक्रम, सूचना वा तथ्याङ्कमा पहुँच प्राप्त गर्ने उद्देश्यले कुनै कार्य गरेमा निजलाई कसूरको गम्भीरता हेरी दुई लाख रूपैयाँसम्म जरिबाना वा तीन वर्षसम्म कैद वा दुवै सजाय हुनेछ भनि व्याख्या गरेको पाइन्छ ।

नेपालमा ८१ प्रतिशतभन्दा बढी अनलाइन घटना (साइबर हिंसा/अपराध) सामाजिक सञ्जाल फेसबुकबाट भइरहेका छन् । आर्थिक वर्ष २०८०/८१ मा ६३५ जना बालबालिका (बालक २५३ र बालिका ३८२) र महिला आठ हजार ७४५ जना प्रभावित भएको तथ्याङ्क छ । सुरक्षित इन्टरनेट दिवस २०२५ को सन्दर्भमा भ्वाइस अफ चिल्ड्रेन र इन्टरनेसनल एसोसिएसन अफ वुमन इन रेडियो एन्ड टेलिभिजन (आइवर्ट) द्वारा राजधानीमा आयोजित कार्यक्रममा अनलाइन हिंसाबाट प्रभावित महिला र बालबालिकाको तथ्याङ्क सार्वजनिक गरिएको हो। राष्ट्रिय महिला आयोगकी अध्यक्षले आयोगमा पनि महिला र किशोरीमाथि हुने विभिन्न हिंसालगायत अनलाइन हिंसाको पनि उजुरी आउने गरेको र आयोगले साइबर व्युरोसँग समन्वय गरी दोषीलाई कारबाहीको दायरामा ल्याउने गरिएको बताउनुभयो । प्रविधिको सहयोगमा धेरै राम्रा, उत्पादनमूलक र सूचनामूलक जानकारी पनि हासिल गर्न सकिन्छ र दुरुपयोग हुँदा पनि धेरै दुःख, बदनामी खप्नुपर्ने अवस्था भएकाले सुरक्षित इन्ट्रनरनेट प्रयोगसम्बन्धी संचेतनामूलक कार्यक्रम विद्यालय र समुदायस्तरमा समेत निरन्तर सञ्चालन गर्नुपर्ने आवश्यकता छ ।

राष्ट्रिय साइबर सुरक्षा केन्द्रले सरकारी कार्यालयको सूचना प्रविधि प्रणालीलाई सूरक्षित राख्न एड्भाइजरी जारी गरेको छ । सरकारी वेबसाइट, डाटा र नेटवर्कको सुरक्षाका लागि केन्द्रले १०२ बुँदे 'एड्भाइजरी' जारी गरेको हो । सरकारी कार्यालयको वेवसाइट, एप्लिकेसेज, सर्भर, नेटवर्क, ईस्कटप, ल्यापटप, मोबाइल उपकरण र सामाजिक सञ्जालको प्रयोगसँग सम्बन्धित विभिन्न सुरक्षात्मक उपायहरू समावेश गर्दै केन्द्रले सूचना प्रविधि प्रणालीलाई सुरक्षित राख्न तथा सम्भावित साइवर खतराबाट जोगाउन साइबर सुरक्षा एड्भाइजरी जारी गरेको हो । कार्यालयमा रहेका डेस्कटप/ल्यापटप र प्रिन्टर सुरक्षासम्बन्धी, 'पासवर्ड' व्यवस्थापन तथा सुरक्षासम्बन्धी, 'इन्टरनेट ब्रोसिङ' सुरक्षासम्बन्धी, 'इमेल' तथा 'फिसिङ एट्याक' सुरक्षासम्बन्धी, रिमोभएबल मिडिया' सुरक्षासम्बन्धी, सामाजिक सञ्जाल, सुरक्षासम्बन्धी र मोबाइल सुरक्षासम्बन्धी विषयमा 'एडभाइजरी' जारी गरिएको बताइएको छ ।

आर्थिक वर्ष २०८१/८२ शुरु भएपछि ६ महिनामा मात्रै देशभर करिब ११ हजार साइबर क्राइमका उजुरी दर्ता भए । योमध्ये ६ हजार १ सय १ वटा साइबर अपराध फेसबुकबाट भएको भन्दै उजुरी दर्ता भएका थिए । यस्तै इन्स्टाग्रामको माध्यमबाट साइबर अपराध गरेको भन्दै १ हजार ८ सय ८४ वटा उजुरी दर्ता भएका छन् । ह्वाट्सएप र टिकटकबाट साइबर क्राइम भएको भन्दै क्रमशः १ हजार २ सय ५६ र ९ सय ६१ वटा उजुरी दर्ता भएका छन् ।

नेपाल प्रहरीको साइबर ब्युरोको जानकारी अनुसार सामाजिक सञ्जालको माध्यमबाट हुने अपराध निकै बढ्दो छ । मुख्यतः सामाजिक सञ्जालबाट आर्थिक अपराध र सम्बन्धमा हुँदा खिचेका फोटो भिडियो सार्वजनिक गरेर यौन हिंसा गर्ने प्रवृत्ति बढेको छ । ६ महिनामा करिब ११ हजार साइबर क्राइमको उजुरी आएको तथ्यले समाजमा इन्टरनेटबाट हुने अपराध मौलाइरहेको पुष्टि हुन्छ । यस्तो अपराधको निशानामा बालबालिका, युवादेखि जानेका, बुझ्नेका व्यक्ति र बृद्धबृद्धाहरुमा पनि परिरहेका छन् । गृह मन्त्रालयले जानकारी गराएअनुसार साइबर क्राइम पछिल्लो समय निकै बढेको तथ्यांक प्रस्तुत गरिएको पाइन्छ । गृह मन्त्रालयको प्राथमिकतामा परेका सुरक्षा चुनौतीहरुको विषयमा यो क्षेत्र पनि परेका छन् । २०८१ फागुनसम्म २ करोड ९७ लाख ७६ हजार टेलिफोन प्रयोगमा रहेका छन् । २०८१ असार सम्म यो संख्या ३ करोड ६२ लाख २६ हजार रहेको थियो । २०८१ असारसम्म इन्टरनेट ग्राहकको घनत्व १४४.२३ प्रतिशत पुगेको छ । यस्तो घनत्व २०८० असारसम्म १३५.९ प्रतिशत रहेको थियो ।

साइबर अपराधका गतिविधिका सम्भावित नयाँ निम्न विविधताले कानून प्रणालीका साथै कानून कार्यान्वयनमा समेत जटिलता थपिदिएको छ : **डा.रत्नबहादुर बागचन्दज्यूले आफ्नो लेख साइबर अपराध र यससम्बन्धी कानूनको विकास, सबैका लागि न्याय जर्नलमा यसरी साइबर अपराधको जटिलता सम्बन्धमा उल्लेख गरेका छन् :-**

१. **क्षेत्राधिकारको सीमा नाघ्दैः** साइबर अपराधले क्षेत्राधिकारको सीमा नाघेर अक्सर समाज, राज्य र देशहरूका बहुसंख्यक मानिसहरूलाई पीडित बनाएको पाइन्छ। इन्टरनेटमा पीडितहरूलाई लक्षित गर्ने अपराधीहरूको लागि भौगोलिक स्थान खास प्राथमिक महत्वको कुरा रहँदैन।

२. **पीडितहरूले आफू पीडित भएको कुरा गोप्य राख्दछन्** : धेरै मानिस आफू पीडित भएको कुरा थाहा भएर पनि इन्टरनेटमा भएको अपराधबाट पीडित भएको कुरा लुकाउने गर्दछन् । जहाँसम्म शारीरिक र यौन दुर्व्यवहारमा परेका बालिकाले आफूउपर भएका अपराध साथी, शिक्षक वा अभिभावकहरुलाई भन्न सक्छन् र धेरै जस्तो साइबर अनुसन्धानका क्रममा प्रहरीमा अपराधसँग सम्बन्धित तस्विर वा फुटेज सार्वजनिक गरिँदैनन् ।

३. **गहिरो प्रभाव** : साइबर अपराध परम्परागत अपराधभन्दा व्यापक रुपमा बृद्धि र परिस्कृत भइरहेको र यसको प्रभावबाट समाजमा कुनै व्यक्ति, संस्था र सरकार कुनै न कुनै रूपमा प्रभावित भएको र खासगरी आर्थिक क्षेत्रमा यसको गम्भिर प्रभाव देखिएको छ ।

४. **संरचनागत विशिष्टताः** साइबर अपराधमा मुख्य तीन तरिकाले संरचनागत विशिष्टता रहेको हुन्छ (१) साइबर अपराध प्रविधिगत रूपमा सघन र सीपपूर्ण, (२) साइबर अपराध परम्परागत अपराधभन्दा उच्चस्तरको भूमण्डलीकरण भएको अपराध र (३) साइबर अपराध अपेक्षाकृत नयाँ ।

५. **साइबर अपराधको दुश्चक्रः** साइबर अपराधको पीडित र कानून कार्यान्वयन निकायहरूको छुट्टाछुट्टै विशेषताहरूले गर्दा साइबर अपराधको एउटा दुश्चक्र सिर्जना गरेको पाइन्छ। यसका कारण साइबर अपराधका नयाँ रूपलाई सामना गर्न अधिकांश देशका स्थानीय प्रहरी बलहरू भूमण्डलीयताप्रतिको साइबर अपराधसँग लड्न आवश्यक क्षमताले सुसज्जित छैनन् ।

६. **कानूनी उपचारका लागि यदाकदा मात्र प्रयास गरिने**: उपचारका लागि कोसिस नगरिने वा प्रकाशमा नआउने धेरै अपराधका घटनाहरूमध्ये साइबर अपराध पनि एक हो। साइबर अपराधका धेरै पीडितहरू कानून कार्यान्वयन निकायले आफूमाथि भइरहेको साइबर अपराधलाई रोक्न सक्दैनन् भन्ने सोचेर प्रहरीमा उजुरी गर्न अनिच्छुक हुन्छन् ।

साइबर अपराध सम्बन्धी विश्व इतिहास हेर्दा फ्रान्समा कपडा बनाउने कारखानाका मालिक जोसेफ मेरी जेक्वार्डले कपडा बुन्नको लागि स्वचालित कम्प्युटरहरू जडान गरेपछि त्यसबाट आफ्ना रोजगारी गुम्ने डरले उक्त उद्योगका कम्प्युटरहरू अवैध तरिकाले ध्वस्त गरि दिएपछि साइबर क्राइमले सन् १८२० मा अपराधको रूप धारण गरेको हो । त्यसपछि विभिन्न औद्योगिक मुलुकहरूमा यस सम्बन्धी कानूनहरू ल्याउन थालिएको थियो । जर्मनमा सन् १८७० मा प्रोडक्सन कानून लागु गरेको थियो । अमेरिका लगायतका देशमा विभिन्न कानूनहरू ल्याइएका थिए । साइबर क्राइमका कारण हाल विश्वमा अरबौं अरब डलरको आर्थिक क्षति र नोक्सानी हुँदै आएका छन् ।

सन् २०१४ मा अमेरिकी सङ्घीय अनुसन्धान ब्यूरोमा २ लाख ६९ हजार ४२२ यस सम्बन्धी उजुरी दर्ता भएका थिए । सन् २०१८ मा प्रकाशित म्याफियो नामक संस्थाको प्रतिवेदन अनुसार साइबर क्राइमका कारण विश्वमा सो अवधिमा मात्र ६०० मिलियन अमेरिकी डलर बराबरको आर्थिक नोक्सानी भएको थियो। ‘साइबर टेरोरिज्म’को नामले समेत लिइने यस अपराधलाई नियन्त्रण गर्न अमेरिकामा एफ.बि.आइ., सि.आइ.ए. जस्ता सरकारी निकायले करोडौं डलर खर्च गर्ने गरेका छन् । भारतमा भारतीय केन्द्रीय जाँच ब्यूरो तथा ‘र’ जस्ता संस्थाहरूले ठूलो धनराशी खर्च गर्दै आएका छन् । नेपालमा पनि नेपाल प्रहरीको केन्द्रीय अनुसन्धान ब्यूरो लगायतका विभिन्न महाशाखा र शाखाहरूले अपराधको अनुसन्धान कार्य गर्दै आएका छन् ।

नेपालमा लामो समयदेखि यस सम्बन्धी अपराध हुने गरेको भए पनि सन् १९९० पछिका दिनमा सूचना तथा सञ्चारको क्षेत्रमा आएको व्यापक विकास र विस्तार कारण यससँग सम्बन्धित विभिन्न अपराध बढ्दै आएका देखिन्छन् । विगतमा मुलुकी ऐन तथा अन्य ऐनका विभिन्न दफा लगाए कानूनी कारबाही हुँदै आएकोमा २०६३ सालबाट भने विद्युतीय कारोबार नियन्त्र सम्बन्धी विशेष ऐन नै ल्याई हाल लामु भइरहेको छ । ऐनको दफा ४४ देखि दफा ५८ सम्म विभिन्न प्रकारका कसूरहरूको उल्लेख गरी सो प्रमाणित भएमा कानून अनुसार ५० हजार देखि ५ लाख सम्प जरिबाना तथा ६ महिनादेखि ५ वर्षसम्मका जेल सजायहरू कसूर अपराधको मात्रा हेरी अदालतले तोक्न सक्ने कानूनी प्रावधान राखिएका छन् । यस सम्बन्धी अपराधमा हाल काठमाडौं जिल्ला अदालतमा मुद्दा गर्न सकिने प्रबन्ध रहेकोमा हाल ७७ वटै जिल्लामा उजुरी गर्न पाइने व्यवस्था गरिएको छ। मुलुकी अपराध संहिता २०७४ तथा मुलुकी देवानी संहिता २०७४ का विभिन्न दफाहरूमा समेत अरूलाई हानी नोक्सानी गरेको पाइएमा विभिन्न प्रकारका सजाय हुने व्यवस्था राखिएका छन् । सामान्य अवस्थामा अनुमति नलिई कसैको तस्बिर खिच्नु, सामाजिक सञ्जालमा फोटो राख्नु, गाली वा बेइज्जती हुने गरी अर्काको प्रतिष्ठामा आँच हुनेगरी गरिने कुनै पनि कार्यलाई कानूनले अपराध मानेको अवस्था छ ।

विश्वमा साइबर क्राइममा महिला तथा बालबालिकाको प्रयोग व्यापक ढङ्गले भइरहेको/बढिरहेको छ । जानी-जानी, अज्ञानतावस, भूलवस, प्रलोभनमा परी, डर-धम्की वा अन्य कारणबाट यस सम्बन्धी अपराधमा विभिन्न तरिका र प्रयोजन वा माध्यमबाट महिला तथा बालबालिकाहरूको प्रयोग हुने गरेको पाइन्छ । ‘कानूनको अज्ञानता क्षम्य नहुने’ कानूनको विश्वव्यापी मान्यता भएकोले जसरी अपराध हुन गएपनि कानून अनुसार सजाय भोग्नुपर्ने हुन्छ । विश्वमा बालबालिकाको परिभाषा पनि फरक-फरक रहेका छन् । नेपालको हालको कानूनले १८ वर्ष भन्दा कम उमेरकोलाई नाबालक मानेको छ । यद्यपि, १० वर्ष भन्दा माथिकोलाई

अवस्था र कानूनी व्यवस्था अनुसार विभिन्न खालको सजायको व्यवस्था गरेको पाइन्छ । १० वर्ष भन्दा मुनिकाले भने जस्तोसुकै अपराध गरेकोमा पनि कुनै सजाय हुँदैन ।[३७८]

सूचना प्रविधिको विकास र विस्तारले मानव विकासमा जसरी सहज सरलीकरण गर्दै आइरहेको छ त्यसैगरी यसको विकासले विभिन्न चुनौती पनि सिर्जना गर्ने गरेको छ । सूचना प्रविधिको विकास र विस्तारले सिर्जना गरेको विभिन्न चुनौतीहरूमध्ये पछिल्लो समयमा बढ्दै गइरहेको साइबर अपराध र त्यस अन्तर्गतको साइबर ठगी पनि एक हो । फेसबुक ह्वाट्स् एप, भाइबर, इन्स्टाग्राम जस्ता सामाजिक सञ्जालको प्रयोग गरि विभिन्न प्रलोभनमा पारि सय रूपैयाँ देखि लाखौं रकम एकै पटक वा पटक पटक गरेर ठगी हुने गरेका कयौं घटना अहिले हाम्रो समाजमा प्रशस्त छन् । यस्ता घटनासँग सम्बन्धित सयौं उजुरी प्रहरी कार्यालयमा दिनहुँ आउने गरेका छन् भने प्रहरीले पनि यस्ता घटनाको सन्दर्भमा गम्भिरताका साथ अनुसन्धान र संलग्नलाई कारबाहीको दायरामा ल्याउन अग्रसर भइरहेको छ । साइबर ठगीका बारेमा चर्चा गर्नुपूर्व केही प्रतिनिधिमूलक घटनाको बारेमा चर्चा गर्नु सान्दर्भिक हुन आउछ ।

साइबर अपराधको प्रकृतिको कुरा गर्दा यो अन्तर्राष्ट्रिय अपराध हो । यो अपराध गर्दा अपराधी वारदातस्थलमा भौतिक रूपमा उपस्थित हुनुपर्दैन । साइबर अपराधको कार्य कम्प्युटर नेटवर्कको अदृश्य जगतमा गरिन्छ। बिजुली चम्केजत्तिकै गतिमा चल्ने इन्टरनेटको विकासका कारण साइबर अपराधका लागि चाहिने आवश्यक समय छोट्टिदै गएको पाइन्छ । सीमाहीन विश्वको रूपमा रहने साइबर स्पेस साइवर अपराधीहरूको लागि खेल मैदान भएको छ जहाँ साइवर अपराधीहरू हज्जारौं किलोमिटर टाढाको स्थानबाट वारदातस्थलमा अनुपस्थित रहेरै अपराध गर्दछन् । यो अवस्था भनेको कानूनका लागि खुला चुनौती हो ।

साइबर अपराधको गतिविधिमा बृद्धि साइबर अपराधका गतिविधिका सम्भावित नयाँ निम्न विविधताले कानून प्रणालीका साथै कानून कार्यान्वयनमा समेत जटिलता थपिदिएको छ :

१. **क्षेत्राधिकारको सीमा नाघ्दै**: साइबर अपराधले क्षेत्राधिकारको सीमा नाघेर अक्सर समाज, राज्य र देशहरूका बहुसंख्यक मानिसहरूलाई पीडित बनाएको पाइन्छ । इन्टरनेटमा पीडितहरूलाई लक्षित गर्ने अपराधीहरूको लागि भौगोलिक स्थान खास प्राथमिक महत्वको कुरा रहँदैन। अक्सर अपराधीहरू हजारौँ किलोमिटरको दूरी पार गरी विभिन्न देश र सहरमा गएर उनीहरूले इन्टरनेटमा भेटिएका बालबालिकासँगको यौन गतिविधिमा संलग्न हुन्छन् । त्यसमध्ये त्यस्ता धेरै मुद्दाहरूमा स्थानीय, राज्यसंघीय र अन्तर्राष्ट्रिय कार्यान्वयन संयन्त्रहरू बहुक्षेत्राधिकारमा वर्तमानमा जोडिएर समन्वयात्मक रूपमा कार्य गर्दछन् ।

२. **पीडितहरूले आफू पीडित भएको कुरा गोप्य राख्दछन्** : धेरै मानिस आफू पीडित भएको कुरा थाहा भएर पनि इन्टरनेटमा भएको अपराधबाट पीडित भएको कुरा लुकाउने गर्दछन् । जहाँसम्म शारीरिक र यौन दुर्व्यवहारमा परेका बालिकाले आफूउपर भएका अपराध साथी, शिक्षक वा अभिभावकहरुलाई भन्न सक्छन् र धेरै जस्तो साइबर अनुसन्धानका क्रममा प्रहरीमा अपराधसँग सम्बन्धित तस्विर वा फुटेज सार्वजनिक गरिँदैनन् ।

३. **गहिरो प्रभाव** : साइबर अपराध परम्परागत अपराधभन्दा व्यापक रुपमा बृद्धि र परिस्कृत भइरहेको र यसको प्रभावबाट समाजमा कुनै व्यक्ति, संस्था र सरकार कुनै न कुनै रूपमा प्रभावित भएको र खासगरी आर्थिक क्षेत्रमा यसको गम्भिर प्रभाव देखिएको छ ।

४. **संरचनागत विशिष्टता**: साइबर अपराधमा मुख्य तीन तरिकाले संरचनागत विशिष्टता रहेको हुन्छ (१) साइबर अपराध प्रविधिगत रूपमा सघन र सीपपूर्ण, (२) साइबर अपराध परम्परागत अपराधभन्दा उच्चस्तरको भूमण्डलीकरण भएको अपराध र (३) साइबर अपराध अपेक्षाकृत नयाँ ।

[३७८] **प्रेमराज सिलवाल, साइबर क्राइमको इतिहास र फैलिँदो अपराधको क्षेत्र, प्रहरी (द्वैमासिक प्रकाशन), वर्ष ६६, अंक २, असार-साउन, २०८१, पेज नं. ३९-४१) ।**

५. **साइबर अपराधको दुश्चक्रः** साइबर अपराधको पीडित र कानून कार्यान्वयन निकायहरूको छुट्टाछुट्टै विशेषताहरूले गर्दा साइबर अपराधको एउटा दुश्चक्र (Vicious Circle of Cybercrime) सिर्जना गरेको पाइन्छ। यसका कारण साइबर अपराधका नयाँ रूपलाई सामना गर्न अधिकांश देशका स्थानीय प्रहरी बलहरू भूमण्डलीयताप्रतिको साइबर अपराधसँग लड्न आवश्यक क्षमताले सुसज्जित छैनन् ।

६. **कानूनी उपचारका लागि यदाकदा मात्र प्रयास गरिनेः** उपचारका लागि कोसिस नगरिने वा प्रकाशमा नआउने धेरै अपराधका घटनाहरूमध्ये साइबर अपराध पनि एक हो । साइबर अपराधका धेरै पीडितहरू कानून कार्यान्वयन निकायले आफूमाथि भइरहेको साइबर अपराधलाई रोक्न सक्दैनन् भन्ने सोचेर प्रहरीमा उजुरी गर्न अनिच्छुक हुन्छन् । साथै समाजमा आफ्नो प्रतिष्ठामा आँच पुग्ने डरले त्यस्तो घटना प्रकाशमा ल्याउन नचाहने पनि हुन्छन् । कम्प्युटर अपराध र सुरक्षासम्बन्धी एउटा अध्ययनबाट साइबर अपराधमा उजुरी नगर्ने सत्तरी प्रतिशत पीडितहरूले त्यस्तो उजुरीपछि नकारात्मक प्रचारप्रसार हुने कारणले उजुरी नगरिएको भन्ने उल्लेख गरेको पाइएको छ ।

७. **पक्राउमा न्यून दरः** उजुरी गरिएका साइबर अपराधका वारदातहरूमध्ये धेरै कम उजुरीमा मात्र संदिग्ध व्यक्तिलाई पक्राउ गरिने अवस्था हुने गरेको पाइन्छ । पक्राउ गर्नका लागि सम्भावित संदिग्ध व्यक्तिहरूको समूह पहिचान गर्ने र त्यस्तो समूहबाट निर्दोषहरूलाई एकपछि अर्को अलग्याउँदै जानुपर्ने हुन्छ । साइबर अपराधको विशेषताको कारणले सम्भावित संदिग्ध व्यक्तिहरूको समूह पहिचान र त्यस्तो समूहबाट निर्दोषहरूलाई छुट्याउने कार्य भनेको 'दुधबाट पानी छुट्याउनु जत्तिकै कठिन हुने हुँदा पक्राउमा न्यून दर (Low Rate of Arrest) हुन पुग्दछ ।

८. **कसूर कायममा न्यून दरः** परम्परागत अपराधमा कसूर कायम गर्न शंकारहित ठोस प्रमाणको जति आवश्यकता पर्दछ, त्यति नै साइबर अपराधमा साइबर फरोन्सिक प्रमाण विश्लेषण सम्मिलित कागजातको आवश्यकता पर्दछ। तर त्यस्तो प्रमाणजन्य तयारीको कार्य ज्यादै महँगो र समय खर्चिलो हुने लगायतका अप्ठ्याराहरूले समस्यालाई झन उल्झाउने काम गर्छ । यसका अतिरिक्त साइबर अपराधको नवीनताले अदालती प्रणालीमा चुनौती खडा गरिदिन्छ ।

९. **डिजिटल प्रमाणः** डिजिटल प्रमाण साइबर अपराध अनुसन्धानका लागि मूल्यवान सूचना तथा तथ्यांक हो, जुन विद्युतीय स्थानान्तरण गर्ने वा विशेष स्थानमा भण्डारण गरिएको हुन्छ। अपराध अनुसन्धानका लागि जुन विद्युतीय उपकरणहरु बरामद गरी सुरक्षित राखिन्छ, त्यसमा लुकाई राखिएका फिङ्गर प्रिन्टहरू र डिएनए डिजिटल प्रमाण हुन सक्छन् । डिजिटल प्रमाण शीघ्र तथा सहजै क्षेत्राधिकारको सीमा पार गरेर प्राप्त भएको हुन सक्छ। साथै यो अघिल्लो रूपबाट नयाँ रूपमा परिवर्तन (Altered) भइसकेको हुनसक्छ । उपकरणमा रहेका त्यस्ता डिजिटल प्रमाण सानो लापरवाहीले वा प्रयत्नद्वारा त्यसमा क्षति पुऱ्याउन वा नष्ट गर्न सकिन्छ। डिजिटल प्रमाण समयसीमाभित्र मात्र महत्वपूर्ण हुने र निर्धारित समयपछि त्यस्ता प्रमाणहरू मूल्यहिन हुन सक्ने किसिमको 'समय संवेदनशील हुनसक्छ । डिजिटल प्रमाणका थुप्रै स्रोतहरू हुन सक्छन्, त्यसको प्रमुख रूपमा इन्टरनेटमा आधारित कम्प्युटर वा कम्प्युटरयुक्त उपकरण र मोबाइल उपकरणहरू हुन सक्छन् । डिजिटल प्रमाण विभिन्न रूपमा रहेका हुन सक्छन्, जस्तैः टेक्स्ट वा फाइल छवि तस्वीर र भिडियो । यस्ता डिजिटल प्रमाणले साइबर अपराधको वारदात भएको छ भन्ने तथ्य पुष्टि गर्न र बारवातको सम्बन्ध सम्बन्धित पीडितसँग छ भन्ने कुरा अदालतमा स्थापित गर्न मद्दत गर्दछ ।

१०. **विद्युतीय प्रमाण संकलन विधि र डिजिटल प्रमाणको सिद्धान्तः** डिजिटल प्रमाण भन्नाले त्यस्तो सूचना हो, जुन Digital रूपमा राखिएको हुन्छ। किनकि त्यो सूचना दोहोरो अंक (Digit) एक र शून्य (Zeros) मा विभाजन भएको हुन्छ । जुन चाहिँ सफ्टवेयर वा कोडद्वारा सुरक्षित गरी पुनः हेर्न वा प्राप्त गर्न सकिन्छ । फोटोग्राफ, शब्द, तालिका जस्ता कुनै पनि किसिमका सूचना यस्तो प्रक्रियाद्वारा सिर्जना गरी सुरक्षित राख्न सकिन्छ । यस्तो प्रकारले सिर्जना गरी राखिएको प्रमाणहरू पत्ता लगाउने र तिनको दुरुपयोग गरिने

कार्य फरेन्सिक जाँचको विषय बन्दै आएको र यसको कारण नयाँनयाँ प्रविधिको उत्पत्ति भइरहेको हुन्छ। साइवर अपराधमा डिजिटल प्रमाण (Digital Evidence) को महत्व ज्यादै ठुलो रहेको छ। परम्परागत अपराध स्थापित हुन भौतिक सबुत प्रमाणको आवश्यकता रहे झैं साइबर अपराधमा भौतिक सबुद प्रमाण केही अन्य हदसम्म सान्दर्भिक हुने भए पनि मुख्यत: त्यस्ता भौतिक प्रमाण कम्प्युटरयुक्त उपकरणमा लुकेर रहेको Logs, Device Fingerprint, Video Footage, Image, Archive Active Data जस्ता अभिलेखको अधिकतम उपयोग गरिन्छ। साथै यस्ता विद्युतीय प्रमाण संकलन विधि र विषय पनि परम्परागत भौतिक प्रमाण संकलन विधि र विषयभन्दा फरक र नबीन हुने गर्दछन्।

११. **साइबर फरेन्सिक**: यसको कुरा गर्दा साइबर फरेन्सिक कम्प्युटर फरेन्सिक र डिजिटल फरेन्सिकभन्दा यसको coverage scope केही फराकिलो हुन्छ। डिजिटल फरेन्सिककै अर्को नाम साइबर फरेन्सिक भए तापनि साइबर फरेन्सिकले अफलाइन डिजिटलभन्दा अघि बढेर साइबर स्पेसमा हुने हरेक गतिविधिको प्रमाण विश्लेषण गर्न सक्ने क्षमता राख्छ। 'साइबर शब्द नै कम्प्युटर र डिजिटलभन्दा बढी व्यापक र अत्याधुनिक भएकोले भविष्यमा 'साइबर' शब्दको व्यापक प्रयोगको सम्भावना समेतलाई विचार गरी यहाँ डिजिटल र कम्प्युटरसँग सम्बन्धित अपराध र फरेन्सिकको चर्चा हुँदा 'साइबर अपराध र साइबर फरेन्सिक' शब्दको प्रयोग गरिएको छ। साइबर फरेन्सिकले कुनै साइबर अपराधको मुद्दामा अपराधीलाई उसको अपराध पुष्टि गर्न पेस गरिने संकलित डिजिटल प्रमाणलाई विश्लेषण गर्ने कार्य गर्दछ। साइबर फरेन्सिकको मुख्य उद्देश्य कसले र कसरी अपराध गर्‍यो भन्ने सम्बन्धमा प्रमाणको श्रृंखलाबद्ध कडी (chain of evidence) व्यवस्थित गरी दस्तावेजीकरण गर्ने रहेको हुन्छ।

१२. **डिजिटल डिएनए**: डिजिटल डिएनए पद्धति हरेक कम्प्युटर प्रयोगकर्ताले कम्प्युटर तथ्यांकमा आफ्नै तरिकाले Access गरेको हुन्छ र उसले जे जसरी Access गरेको हुन्छ त्यो तरिकाले आफ्नै छुट्टै डिजिटल फिङ्गरप्रिन्ट सिर्जना गरेको हुन्छ, त्यो तरिका नै उसको डिजिटल डिएनए बन्न पुग्छ। यसरी हरेक Computer User को आफ्ना डिजिटल डिएनए हुने भएपछि एउटा कम्प्युटरका तथ्यांकमा एउटाले Access गरेकोमा त्यसै कम्प्युटरलाई अर्कोले Access गर्दा आफ्नो तरिकाले गर्ने हुँदा ती दुई प्रयोगकर्ताको Access गर्ने तरिकामा आएका Variation ले कम्प्युटर तथ्यांकमा Access गर्ने व्यक्तिका DNA पहिचान गरेर साइबर अपराधको अनुसन्धानमा डिजिटल फरेन्सिकको माध्यमबाट डिएनए म्याचिङ र विश्लेषण गरिने पद्धतिलाई डिजिटल डिएनए भनिएको छ।[३७९]

संगठित अपराधको परिभाषा विभिन्न अनुसन्धानकर्ता र विज्ञहरूले गरेको पाइन्छ तर सर्वमान्य परिभाषा आउन सकेको पाइँदैन। संगठित अपराधले बृहत गैर-कानूनी क्रियाकलापहरू समेट्ने भएकोले विश्वव्यापी रूपमा स्वीकारयोग्य परिभाषा आउन नसकेको हो। संगठित अपराध भन्नाले कसैले अपराधिक समूहको लाभको लागि अपराधिक समूहको निर्देशनमा अपराधिक समूहको तर्फबाट अपराधिक समूहसँग मिलेर वा अपराधिक समूहको संस्थापक सदस्य वा सदस्य भई जानीजानी कुनै किसिमको गम्भीर अपराध गरेमा निजले संगठित अपराध गरेको मानिनेछ। यस प्रावधानअनुसार संगठित अपराध हुनका लागि "आपराधिक समूह" को अस्तित्व देखिनु पर्छ। आपराधिक समूह भन्नाले प्रत्यक्ष वा परोक्ष रूपमा परिच्छेद २ मा उल्लिखित संगठित अपराध गर्ने उद्देश्यले नेपालभित्र वा बाहिर रहे भएको संगठित वा असंगठित तीन वा तीन भन्दा वढी व्यक्तिहरूको समूह सम्झनुपर्छ। "आपराधिक समूह बेगर गरिएको कसूर संगठित अपराध हुन सक्दैन। United Nations Convention against Transnational Organized Crime Article 2(a) बमोजिम संगठित आपराधिक

[३७९] **डा.रत्नबहादुर बागचन्द, साइबर अपराध र यससम्बन्धी कानूनको विकास, सबैका लागि न्याय, (न्याय प्रशासनका विविध आयामहरु सम्बन्धी लेखहरुको सङ्ग्रह), नेपाल निजामती कर्मचारी संगठन, सर्वोच्च अदालत, पहिलो संस्करण २०८०, पेज नं. १३५५-१३५८)।**

समूहलाई निम्नानुसार व्याख्या गरिएको छ । Organized criminal group shall mean a structured group of three or more persons, existing for a period of bine and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit .(Motivation) लाभ हो । लाभ भन्नाले आर्थिक वा अन्य कुनै भौतिक लाभ (Financial or other material benefit) भन्ने बुझिन्छ । यही उद्देश्य (Motivation) तत्वले अन्य सामूहिक अपराधबाट फरक देखिन्छ । भारतीय सर्वोच्च अदालतले संगठित अपराध भनेको गैर-कानूनी कार्यमा निरन्तर उपत रहेको (continuing aunlawfial activity) र संगठित अपराध समूह (organisedime Syndicate) को समष्टिः रहेको भनेको पाइन्छ । सो फैसलाअनुसार संगठित अपराधको आवश्यक तत्वमा निम्नबमोजिम रहेको पाइन्छः

१. कानूनद्वारा निषेधित क्रियाकलाप,
२. ३ वर्ष भन्दा बढी सजाय हुने कसूर,
३. व्यक्तिगत वा सामूहिक रूपमा कसूरमा संलग्नता,
४. संगठित समूह (organized crime Syndicate) को सदस्य भई सहभागी भएको,
५. उही प्रकारको कसूरमा संलग्न रहेको भनी दश वर्षबिच सक्षम अदालतमा एक वा बढी अभियोगपत्र दायर भएको र सो कुरा अदालतको जानकारीमा रहेको,
६. यस्ता क्रियाकलाप हिंसाका धम्की, हर चास वा करकाप वा अन्य अवैध तरिकाले गरिएको,
७. आर्थिक वा अन्य गैर-कानूनी लाभका लागि उक्त कार्य गरेको वा विद्रोह (Insurgency) मच्चाउनका लागि सो कार्य गरेको ।

निष्कर्ष

राष्ट्रिय साइबर सुरक्षा नीति, २०८० का विशेषताहरुमा राज्य व्यवस्थाको सञ्चालन, विकासको व्यवस्थापन, सार्वजनिक सेवा प्रवाह तथा नागरिकका आवक क्रियाकलाप डिजिटल प्रविधिमा निर्भर हुँदै गइरहेको अवस्थामा साइबर सुरक्षा चुनौतीपूर्ण हुँदै गएको छ । दिनानुदिन बढ्दै गइरहेको व्यक्तिगत, संस्थागत डाटा चोरी/दुरुपयोग, सूचना प्रविधि प्रणालीहरू माथिको अनधिकृत पहुँच, राष्ट्रिय तथा अन्तर्राष्ट्रिय सूचना प्रविधि प्रणालीमाथि भइरहेका साइबर आक्रमणको प्रतिरक्षा गर्ने विषयलाई सुनिश्चित गर्न साइबर आक्रमणबाट हुन सक्ने क्षति रोक्न, न्यूनीकरण गर्न र भविष्यमा हुन सक्ने यस्ता आक्रमणबाट सुरक्षित रहनु अत्यावश्यक भएको छ। एकातर्फ सुरक्षित सूचना प्रविधिको प्रयोगबाट पारदर्शी एवम् प्रभावकारी सार्वजनिक सेवा व्यवस्थापनको अपेक्षा पूरा गर्नुपर्ने अवस्था छ भने अर्कोतर्फ नागरिक अधिकारका विश्वव्यापी मान्यता, नेपालको संविधानले प्रदत्त गरेको मौलिक हक कार्यान्वयन गर्नुपर्ने अवस्थासमेत छ । नेपालमा पहिलो पटक २०२८ सालमा राष्ट्रिय जनगणनाको तथ्याङ्क प्रशोधनका क्रममा कम्प्युटर प्रविधिको प्रयोग भएको हो। २०३१ सालमा कम्प्युटरसंग सम्बन्धित पहिलो संस्था सेन्टर फर इलेक्ट्रोनिक डाटा प्रोसेसिङ स्थापना भयो जसको नाम पछि राष्ट्रिय कम्प्युटर केन्द्र भएको हो ।

साइबर आक्रमण रोक्नका लागि नेपाल प्रहरी साइबर ब्युरोले समेत महत्वपूर्ण कार्य गरिरहेको छ । नेपाल प्रहरी साइबर ब्युरोको तथ्याङ्क अनुसार यस आर्थिक वर्षमा नौ हजार १३ वटा साइबर घटना दर्ता भएका छन् । यसले पनि नेपालमा साइबर घटना बढिरहेको देखिन्छ । 'फिड्सएक्स्प्लोइट' नामक ह्याकर समूहले नेपालका वेबसाइटहरू ह्याक गरेको दाबी गरेको छ । 'फिड्सएक्स्प्लोइट' नामक समूहले 'एनोन ब्ल्याक फ्ल्याग/इन्डोनेसिया' नामक टेलिग्राम च्यानलमार्फत नेपालका सरकारी तथा निजी वेबसाइटहरू ह्याक गरेको दाबी गरेको नेपाली सञ्चार माध्यमले जनाएको छ । उक्त समूहले नेपाली नागरिकको संवेदनशील कागजातसहित एक हजार ७५० वटा फाइल आफूसँग रहेको समेत दाबी गरेको छ । सरकारले साइबर आक्रमणलाई रोक्नका लागि सूचना प्रविधि क्षेत्रमा लगानी बढाउनुपर्छ । साइबर सुरक्षा अनुगमन गर्ने उद्देश्यले सञ्चालनमा ल्याएको

राष्ट्रिय साइबर सुरक्षा केन्द्रले पटक पटक साइबर आक्रमण हुँदा पनि कुनै ठोस काम गर्न सकेको देखिँदैन । केन्द्रमा दक्ष जनशक्तिको अभाव पनि छ । यसले कामकाज हुन सकेको छैन । सरकारले साइबर आक्रमण रोकथामका लागि मिडियाको सहयोगमा 'साइबर जागरूकता अभियान' सञ्चालन गर्न अग्रसर हुनुपर्छ ।

इन्टरनेटको प्रयोग गरेर ठगी गर्ने, ह्याकिङ गर्ने, व्यक्तिगत सूचना खुलासा गर्ने, अनलाइनको प्रयोग गरेर धम्की दिने, कम्प्युटर स्रोत, संकेतको चोरी, नष्ट वा परिवर्तन, कम्प्युटर र सूचना प्रणालीमा क्षति पुऱ्याउने, गोपनीयता भंग गर्ने तथा झुठा व्यहोराको सूचना दिने, झुठा प्रमाणपत्र वा इजाजतपत्र पेश गर्ने, कम्प्युटर जालसाजी गर्ने आदि जस्ता समस्याहरु देखिएका छन् । सम्बन्धित विषयमा तालिम प्राप्त दक्ष जनशक्तिको अभाव हुनु र भएका जनशक्तिलाई मैनि retaintion गर्न नसक्नु, अनुसन्धानको लागि आवश्यक नयाँ नयाँ Tools, technique & equipment को अभाव हुनु र Cyber Crime Trans–border crime भएकोले अनुसन्धान गर्न कठिन, सेवा प्रदायक संस्थाहरु कमजोर हुँदा अनुसन्धानका लागि आवश्यक सम्पूर्ण सूचनाहरु समयमा नै उपलब्ध गराउन नसक्नु, Trans border crime भएकोले अन्य मुलुकसँग समन्वय गर्न कठिनाई परेको छ । सामाजिक संजालका सम्पर्क कार्यालय नेपालमा नहुँदा आवश्यक सूचना प्राप्त गर्न असमर्थ हुनु, अपराधलाई स्थापित गर्नका लागि यथेष्ठ प्रमाण संकलनमा कठिनाई हुनु, मुलुकभरको साईबर अपराध सम्बन्धी मुद्दा काठमाण्डौ जिल्ला अदालतबाट अनुसन्धान गर्नुपर्दा मुद्दाको चाप बढ्नु, डिजिटल फोरेन्सिक ल्याबमा पर्याप्त कर्मचारी र उपकरणको अभावका समयमै रिपोर्टहरु प्राप्त नहुनु, साईबर अपराध सम्बन्धी मजबुत कानूनी व्यवस्था नहुनु र विद्युतीय कारोबार ऐन, २०६३ ले साईबर अपराधका सम्पूर्ण पक्षलाई समेट्न नसक्नु, राष्ट्रिय साईवर सुरक्षा रणनीति समयमै तर्जुमा र स्वीकृति गरी कार्यान्वयनमा ल्याउन नसक्नु, साईबर सुरक्षाको उपाय र यसका जोखिम सम्बन्धमा नागरिक स्तरमा जनचेतनाको अभाव हुनु अन्तरनिकाय समन्वय, सहकार्य र साझेदारीको अभाव हुनु आदि जस्ता समस्या तथा चुनौतीहरु सिर्जना भएका छन् ।

सन्दर्भग्रन्थहरु

डा.खुशी प्रसाद थारु, संगठित अपराध : भ्रष्टाचार र सम्पत्ति शुद्धीकरण, सबैका लागि न्याय, नेपाल निजामती कर्मचारी संगठन, सर्वोच्च अदालत, पहिलो संस्करण २०८०, रामशाहपथ, काठमाडौं, नेपाल ।

कालिबहादुर साम्यू लिम्बू, अपराध : अवधारणा, तत्व, प्रकार, चरण, पक्ष, अपूर्ण अपराध र प्रतिरक्षा र सामुदायिक सेवा, सबैका लागि न्याय, नेपाल निजामती कर्मचारी संगठन, सर्वोच्च अदालत, पहिलो संस्करण २०८०, रामशाहपथ, काठमाडौं, नेपाल ।

डा.रत्नबहादुर बागचन्द, साइबर अपराध र यससम्बन्धी कानूनको विकास, सबैका लागि न्याय, नेपाल निजामती कर्मचारी संगठन, सर्वोच्च अदालत, पहिलो संस्करण २०८०, रामशाहपथ, काठमाडौं, नेपाल ।

नेपालको संविधान, २०७२, कानून तथा न्याय मन्त्रालय ।

आर्थिक सर्भेक्षण २०८१/८२, नेपाल सरकार, अर्थ मन्त्रालय, सिंहदरबार, काठमाडौं, नेपाल ।

आर्थिक वर्ष २०८२/८३ को बजेट वक्तव्य, अर्थ मन्त्रालय, सिंहदरबार, काठमाडौं, नेपाल ।

राष्ट्रिय साइबर सुरक्षा नीति, २०८०।

शारदा फुयाल, नवीन कुमार यादव, साइबर अपराधः अवधारणा र यसका आयामहरु, न्यायिक आवाज(न्याय र कानून सम्बन्धी समसामयिक दृष्टिकोणहरु), अङ्क ९, २०८१ असोज, न्यायपालिका अधिकृत समाज, काठमाडौं, नेपाल ।

गम्भीर बहादुर हाडा, नेपालमा सूचना प्रविधिको महत्व तथा आवश्यकता -समस्या र सुझाव क्इचँ क्यअर्ष्बा च्भकभबचअज ँयचग, त्रिपुरासुन्दरी -८, भक्तपुर, वर्ष २, अंक १, २०६२ बैशाख।

गम्भीर बहादुर हाडा, नेपालमा सूचना प्रविधिको महत्व तथा आवश्यकता -समस्या र सुझाव सनराइज नेपाल, पर्यटन वातावरणीय पाक्षिक, भदौ १५-३०, काठमाडौं, नेपाल।