विद्यमान साइबर सुरक्षाका चुनौतीहरू एवं साइबर अपराध नियन्त्रणलाई प्रभावकारी बनाउने उपायका सम्बन्धमा प्रतिवेदन पेश गर्न गठित अध्ययन समितिको

प्रतिवेदन

फाल्गुण, २०७८

विद्यमान साइबर सुरक्षाका चुनौतीहरू एवं साइबर अपराध नियन्त्रणलाई प्रभावकारी बनाउने उपायका सम्बन्धमा प्रतिवेदन पेश गर्न गठित अध्ययन समितिको

प्रतिवेदन

प्रतिवेदन तयार तथा पेश गर्ने

डा. भीष्मकुमार भूसाल	सहसचिव	गृह मन्त्रालय	- संयोजक
श्री विजय कुमार राय	निर्देशक (अधिकृत प्रथम श्रेणी)	नेपाल दूरसञ्चार प्राधिकरण	- सदस्य
श्री नबीन्द अर्याल	प्रहरी वरिष्ठ उपरीक्षक	साइबर ब्युरो, नेपाल प्रहरी	- सदस्य
श्री इन्द्र प्रसाद मैनाली	उपसचिव	सञ्चार तथा सूचना प्रविधि मन्त्रालय	- सदस्य
श्री शिवजीकुमार गुप्ता रौनियार	निर्देशक	सूचना प्रविधि विभाग	- सदस्य
श्री सफल श्रेष्ठ	निर्देशक	राष्ट्रिय सूचना प्रविधि केन्द्र	- सदस्य
श्री सन्ध्या पाण्डे	प्रा. प्र. सेनानी	नेपाली सेना	- सदस्य
श्री दिपक राज अवस्थी	प्रहरी नायब उपरीक्षक	सूचना प्रविधि निर्देशनालय, नेपाल प्रहरी	- सदस्य
ई. सौरभ राज वन्त	सशस्त्र प्रहरी नायब उपरीक्षक	सशस्त्र प्रहरी बल नेपाल	- सदस्य
श्री शंकर आचार्य	अनुसन्धान अधिकृत	राष्ट्रिय अनुसन्धान विभाग	- सदस्य
श्री सुष्मा श्रेष्ठ	वरिष्ठ कम्प्यूटर ईञ्जिनीयर	गृह मन्त्रालय	- सदस्य सचिव

विषयसूची

परिच्छेद १ – परिचय

१.१. पृष्ठभूमि

सूचना प्रविधिको निरन्तर विकास, बढ्दो प्रयोग एवं गतिशिलतासँगै सूचना प्रविधिको प्रयोग गरी चुस्त, पारदर्शी, सहज, छिटोछरितो सार्वजनिक सेवा तथा सूचना प्रवाह, सामाजिक अन्तरक्रिया आदिको माध्यमबाट सुशासनको प्रत्याभूति र पारदर्शी एवं प्रभावकारी सार्वजनिक व्यवस्थापनको अपेक्षा गरिएको छ । सूचना प्रविधिमा भएको तीव्र विकासले अनगिन्ती अवसरहरू ल्याएको छ तथापि अवसरसँगै चुनौती तथा जोखिम बढ्दै गएको विषयलाई नकार्न सकिँदैन । राज्य व्यवस्थाको सञ्चालन, विकासको व्यवस्थापन, सार्वजनिक सेवा प्रवाह तथा नागरिकका दैनिक क्रियाकलापहरू डिजिटल प्रविधिमा निर्भर हुँदै गईरहेको अवस्थामा साइबर सुरक्षा चुनौतीपूर्ण हुँदै गएको छ। दिनानुदिन बढ्दै गैरहेको व्यक्तिगत, संस्थागत डाटा चोरी/ दुरुपयोग, सूचना प्रविधि प्रणालीहरूमाथिको अनाधिकृत पहुँच, राष्ट्रिय तथा अन्तर्राष्ट्रियस्तरमा सूचना प्रविधि प्रणालीमाथि भइरहेका साइवर आक्रमणको प्रतिरक्षा गर्ने विषयलाई सुनिश्चित गर्न, साइबर आक्रमणबाट हुन सक्ने क्षतिलाई रोक्न, न्यूनीकरण गर्न र भविष्यमा हुन सक्ने यस्ता आक्रमणहरूबाट सुरक्षित रहन अत्यावश्यक भएको छ।

डिजिटल प्रविधिको प्रयोगसँगै साइबर सुरक्षा सम्बन्धमा बढ्दै गएको चुनौतीहरुका सन्दर्भमा मिति २०७८।०९।२० गते मंगलबारका दिन गृह मन्त्रालयमा साइबर सुरक्षा सम्बन्धमा सरोकारवाला निकायबीच छलफल भएको थियो। गृह सचिव श्रीमान् टेकनारायण पाण्डेको अध्यक्षतामा आयोजित छलफलमा गृह मन्त्रालयका प्रवक्ता, सुरक्षा तथा समन्वय महाशाखाका प्रमुख, नीति, योजना अनुगमन तथा मूल्याङ्कन महाशाखाका प्रमुख, शान्ति सुरक्षा तथा अपराध नियन्त्रण शाखाका प्रमुख, सूचना प्रविधि शाखाका प्रमुख तथा सूचना प्रविधि शाखाका कम्प्युटर इन्जिनियर लगायतको उपस्थिति रहेको थियो भने छलफलमा गृह मन्त्रालयअन्तर्गतका निकायतर्फ राष्ट्रिय परिचयपत्र तथा पञ्जीकरण विभाग, सशस्त्र प्रहरी बल, नेपाल प्रहरी, सूचना प्रविधि निर्देशनालय र साइबर ब्युरोका यस क्षेत्रसँग सम्बन्धित प्रतिनिधिहरूको सहभागिता रहेको थियो । त्यसैगरी अन्य सरोकारवाला निकायका तर्फबाट राष्ट्रिय अनुसन्धान विभाग, सञ्चार तथा सूचना प्रविधि मन्त्रालय र सो अन्तर्गतका सूचना प्रविधि विभाग, राष्ट्रिय सूचना प्रविधि केन्द्र, नेपाल दूरसञ्चार प्राधिकरणको समेत प्रतिनिधित्व रहेको थियो ।

छलफलमा सञ्चार तथा सूचना प्रविधि मन्त्रालयका तर्फबाट साइवर सुरक्षा क्षेत्रमा विद्यमान कानूनी व्यवस्था सम्बन्धित मन्त्रालयबाट भएका साइवर सुरक्षासँग सम्बन्धित मुख्य मुख्य कार्यहरू, वर्तमान अवस्था, चालू आर्थिक वर्षमा सञ्चालन हुने साइवर सुरक्षासँग सम्बन्धित प्रमुख कार्यक्रम, भावी कार्यक्रमहरू तथा समस्या/चुनौतीहरू सम्बन्धमा प्रस्तुति भएको थियो । कार्यक्रममा हाल बढ्दो सामाजिक सञ्जालको दुरुपयोग, भ्रामक समाचार, Spam/ phishing Email लगायतका विविध विषयहरू औंल्याइएका थिए। विभिन्न निकायका प्रतिनिधिहरूले नेपालमा घटेका साइबर

आक्रमण घटनाहरू, तिनको पहिचान तथा Response प्रक्रिया, घटनाक्रमका प्रवृत्ति, कमीकमजोरी सम्बन्धमा अनुभव साझा गर्नुभएको थियो। सोही क्रममा हालको अवस्थाको बारेमा प्रकाश पार्दै जोखिम न्यूनीकरण तथा सुधारका लागि गर्नुपर्ने कामका सन्दर्भमा आ-आफ्ना सुझावहरू पनि प्रस्तुत गर्नुभएको थियो । सो छलफलको क्रममा उठेका सवालहरूलाई सम्बोधन गर्दै नेपालमा हुने साइबर आक्रमण, तिनका प्रवृत्ति के-कस्ता रहेका छन्, चुनौती तथा जोखिम न्यूनीकरणका लागि हालको वर्तमान व्यवस्था, अवस्था, सोको विश्लेषण र आगामी दिनमा कसरी अगाडि बढ्न सकिन्छ जस्ता विषयमा छलफल गरी कार्ययोजना तयार गर्न समिति गठन गर्ने निर्णय भएको हो ।

१.२. उद्देश्य

डिजिटल प्रविधिको प्रयोग सँगै साइबर सुरक्षा सम्बन्धमा बढ्दै गएको चुनौतीका कारण सरकारी सूचना प्रविधि प्रणाली एवम् तथ्याङ्कको सुरक्षा हालका दिनहरूमा चुनौतीपूर्ण बन्दै गइरहेको छ । सूचना प्रविधि प्रणाली एवम् तथ्याङ्कमा मुलुकभित्र तथा मुलुक बाहिरबाट समेत साइबर आक्रमणका घटनाहरू भइरहेका छन् । साइवर आक्रमण विश्वको कुनै पनि स्थानमा रहेर सहजै गर्न सकिने भएको छ । कार्यालयभित्र पनि यससम्बन्धमा जानकारीप्राप्त कर्मचारीहरू अत्यन्त कम रहेको तथा प्रयोगका क्रममा सजग नहुँदा महत्वपूर्ण तथ्याङ्कहरूको सुरक्षा एवम् संरक्षणमा जोखिम बढ्दै गइरहेको छ ।

तसर्थ, उक्त जोखिमहरू न्यूनीकरणका लागि हालको वर्तमान व्यवस्था, अवस्था, नेपालमा हुने साइबर आक्रमण प्रवृत्ति, के-कस्ता रिक्तता (Gap) रहेका छन्, सोको विश्लेषण र आगामी दिनमा कसरी अगाडि बढ्न सकिन्छ भनी अध्ययन तथा छलफल गरी देहायबमोजिमका विषयवस्तु समावेश गरी राय, सुझाव तथा कार्यान्वयन मैट्रिक्स सहितको प्रतिवेदन पेश गर्नु नै समितिको मुख्य उद्देश्य रहेको छ ।

१.२.१. साइबर अपराधको प्रवृत्ति विश्लेषण ,

१.२.२. प्रभावकारी साइबर सुरक्षाका नवीनतम अभ्यासहरूको अध्ययन,

१.२.३. साइबर अपराध नियन्त्रण एवं प्रभावकारी साइबर सुरक्षाका लागि नीतिगत तथा कानूनी सुधार ,

१.२.४. साइबर सुरक्षा एवं साइबर अपराध न्यूनीकरणका लागि अवलम्बन गर्नु पर्ने अल्पकालीन एवं दीर्घकालीन उपायहरूको पहिचान

१.२.५. साइबर सुरक्षा सम्बन्धमा निकायगत भूमिका (नियामक निकाय एवं कार्यान्वयन गर्ने निकाय) पहिचान

१.३. समिति गठन

गृह मन्त्रालयका सचिव टेकनारायण पाण्डेज्यूकोको अध्यक्षतामा मिति २०७८।०९।२० गते मङ्गलबारका दिन गृह मन्त्रालयमा बसेको बैठकमा साइबर सुरक्षा सम्बन्धमा सरोकारवाला निकायबीच छलफल भएको र उक्त बैठकको निर्णयको बुँदा नं. १ र बुँदा नं. २ मा देहाय बमोजिम रहेको छ।

निर्णयहरू:

१. विद्यमान साइबर सुरक्षाका चुनौतीहरू एवं साइबर अपराध नियन्त्रणलाई प्रभावकारी बनाउने उपायका सम्बन्धमा अध्ययन गरी प्रतिवेदन पेश गर्न देहाय बमोजिमको समिति गठन गर्नेः

क.	सहसचिव, डा. भीष्मकुमार भूसाल, गृह मन्त्रालय	-	संयोजक
ख.	उपसचिव, सञ्चार तथा सूचना प्रविधि मन्त्रालय	-	सदस्य
ग.	निर्देशक, सूचना प्रविधि विभाग	-	सदस्य
घ.	निर्देशक, नेपाल दूरसञ्चार प्राधिकरण	-	सदस्य
ङ.	निर्देशक, राष्ट्रिय सूचना प्रविधि केन्द्र	-	सदस्य
च.	प्रहरी वरिष्ठ उपरीक्षक, साइबर ब्युरो, नेपाल प्रहरी	-	सदस्य
छ.	प्रहरी नायब उपरीक्षक, सूचना प्रविधि निर्देशनालय, नेपाल प्रहरी	-	सदस्य
ज.	सशस्त्र प्रहरी नायब उपरीक्षक, सशस्त्र प्रहरी	-	सदस्य
झ.	प्रा. सेनानी, नेपाली सेना	-	सदस्य
ञ.	अनुसन्धान अधिकृत, राष्ट्रिय अनुसन्धान विभाग	-	सदस्य
ट.	उपसचिव, गृह मन्त्रालय	-	सदस्य सचिव

२. उक्त समितिले साइवर अपराधको प्रवृत्ति विश्लेषण, प्रभावकारी साइबर सुरक्षाका नवीनतम अभ्यासहरूको अध्ययन गरी साइबर अपराध नियन्त्रण एवं प्रभावकारी साइबर सुरक्षाका लागि नीतिगत तथा कानूनी सुधार, साइबर अपराध नियन्त्रणको निकायगत भूमिका, साइबर सुरक्षा एवं साइबर अपराध नियन्त्रणका अल्पकालीन एवं दीर्घकालीन उपायहरू ,नियामक निकाय एवं कार्यान्वयन गर्ने निकाय समेत निर्दिष्ट गरी कार्यान्वयन मैट्रिक्स सहितको प्रतिवेदन एक महिनाभित्र पेश गर्न कार्यादेश दिने ।

१.४. समितिका सदस्यहरू

विद्यमान साइबर सुरक्षाका चुनौतीहरू एवं साइबर अपराध नियन्त्रणलाई प्रभावकारी बनाउने उपायका सम्बन्धमा अध्ययन समितिमा देहायबमोजिम सदस्य रहेका छन् **:**

तालिका १: अध्ययन समितिका सदस्यहरू

क्र.सं.	समिति पद	नाम	पद	कार्यरत निकाय
१	संयोजक	डा. भीष्मकुमार भूसाल	सहसचिव	गृह मन्त्रालय
२	सदस्य	श्री विजय कुमार राय	निर्देशक (अधिकृत प्रथम श्रेणी)	नेपाल दूरसञ्चार प्राधिकरण
३	सदस्य	श्री नबीन्द अर्याल	प्रहरी वरिष्ठ उपरीक्षक	साइबर ब्युरो, नेपाल प्रहरी
४	सदस्य	श्री इन्द्र प्रसाद मैनाली	उपसचिव	सञ्चार तथा सूचना प्रविधि मन्त्रालय
५	सदस्य	श्री शिवजीकुमार गुप्ता रौनियार	निर्देशक	सूचना प्रविधि विभाग
६	सदस्य	श्री सफल श्रेष्ठ	निर्देशक	राष्ट्रिय सूचना प्रविधि केन्द्र
७	सदस्य	श्री सन्ध्या पाण्डे	प्रा. प्र. सेनानी	नेपाली सेना
८	सदस्य	श्री दिपक राज अवस्थी	प्रहरी नायब उपरीक्षक	सूचना प्रविधि निर्देशनालय, नेपाल प्रहरी
९	सदस्य	ई. सौरभ राज वन्त	सशस्त्र प्रहरी नायब उपरीक्षक	सशस्त्र प्रहरी बल नेपाल
१०	सदस्य	श्री शंकर आचार्य	अनुसन्धान अधिकृत	राष्ट्रिय अनुसन्धान विभाग
११	सदस्य सचिव	श्री सुष्मा श्रेष्ठ	वरिष्ठ कम्प्यूटर ईञ्जिनीयर	गृह मन्त्रालय

१.५. समितिको कार्यक्षेत्र

समितिलाई प्रदान गरिएका देहायका कार्यक्षेत्रहरू समावेश गरी प्रतिवेदन तयार गरिएको छ :

१.५.१. साइबर अपराधको प्रवृत्ति विश्लेषण ,

१.५.२. प्रभावकारी साइबर सुरक्षाका नवीनतम अभ्यासहरूको अध्ययन ,

१.५.३. साइबर अपराध नियन्त्रण एवं प्रभावकारी साइबर सुरक्षाका लागि नीतिगत तथा कानूनी सुधार ,

१.५.४. साइबर सुरक्षा एवं साइबर अपराध न्यूनीकरणका लागि अवलम्बन गर्नु पर्ने अल्पकालीन एवं दीर्घकालीन उपायहरू पहिचान,

१.५.५. साइबर सुरक्षा सम्बन्धमा निकायगत भूमिका (नियामक निकाय एवं कार्यान्वयन गर्ने निकाय) पहिचान गरी कार्ययोजना तयारी।

१.६. अध्ययनको नीतिगत आधार

राष्ट्रिय सुरक्षा नीति, २०७३ ले सुरक्षा संयन्त्र र संरचनालाई आधुनिक प्रविधि र उपकरणले सुसज्जित गरी सुदृढ तथा सक्षम तुल्याउँदै यस क्षेत्रमा कार्यरत सबैको सक्रिय सहभागिता र योगदानमा अभिवृद्धि गरी सुरक्षा क्षेत्रको प्रभावकारिता बढाउने उद्देश्य लिएको (परिच्छेद १.३.३) छ भने विज्ञान प्रविधि र आधुनिक उपकरणको दुरुपयोगलाई राष्ट्रिय सुरक्षामा प्रभाव पार्ने तत्वको रूपमा लिइएको (परिच्छेद १.७.१०) थियो। त्यसै गरी उक्त नीतिले सुदृढ सुरक्षा व्यवस्थाका लागि क्षेत्रीय तथा अन्तर्राष्ट्रिय तहमा सूचना समन्वय र साझेदारी गर्ने कार्यनीति लिइएको (परिच्छेद २.८.७.१.५) देखिन्छ।

"विद्युतीय वित्तीय संरचनाको रक्षा र संरक्षणका लागि *साइबर सुरक्षा प्रणालीको निर्माण गर्ने*" कार्यलाई राष्ट्रिय सुरक्षा नीति २०७३ ले " सुदृढ अर्थतन्त्रको विकास र सामाजिक सार्वजनिक सेवाको प्रभावकारी प्रवाहका लागि वातावरण निर्माण र आर्थिक सुरक्षाको प्रत्याभूति गर्ने" रणनीतिक लक्ष्य हासिल गर्नका लागि अवलम्बन गरिने विभिन्न कार्यनीतिहरूमध्ये एक कार्यनीतिको रूपमा अङ्गीकार गरेको (परिच्छेद २.८.८.१.४) देखिन्छ।

सुरक्षा संयन्त्रमा सूचना प्रणाली र सुरक्षा संयन्त्रको प्रभावकारी परिचालनका लागि क्षमता अभिवृद्धि गर्ने तथा सूचना सुरक्षाको प्रत्याभूति गर्ने (२.८.१०) रणनीतिक लक्ष्य अन्तर्गत देहायका कार्यनीतिहरू समावेश गरिएका छन्-

२.८.१०.१.१	चुनौती र जोखिमको विश्लेषण र व्यवस्थापन गर्ने गरी सुरक्षा निकायको अनुसन्धान क्षमतामा अभिवृद्धि गर्दै आवश्यकतानुसार रूपान्तरण गर्ने।
२.८.१०.१.३.२	सुरक्षा संयन्त्रको रूपान्तरणका लागिः अनुसन्धान र विकासमा लगानी गर्ने; सम्भावित खतराको सामना गर्न आवश्यक संयन्त्र निर्माण गर्ने; सूचना सङ्कलन र विश्लेषणका लागि नयाँ प्रविधिको उपयोग गर्ने।

२.८.१०.१.४	राष्ट्रिय सुरक्षा, सामरिक स्थिति, राष्ट्रिय हित र स्वार्थ अनुरूप गोप्य राखिनुपर्ने सूचनाहरूको गोपनीयता कायम राख्ने।
२.८.१०.१.५	सुरक्षा संयन्त्रको परिचालन नीति, विकास र निर्देशनका लागि रणनीतिक सूचनाको सङ्कलन विश्लेषण र उपयोग गर्ने।
२.८.१०.१.६	अन्तर निकाय सहयोग र सूचना समन्वयका लागि संयन्त्रगत व्यवस्था गर्ने।
२.८.१०.१.७	सूचना सङ्कलन र सहयोगका लागि क्षेत्रीय र अन्तर्राष्ट्रिय संयन्त्रको उपयोग गर्ने।
२.८.१०.१.८	आतङ्कवादी उच्च खतरा भएक व्यक्तिहरू, शङ्कास्पद व्यक्तिहरू, निष्काशित अपराधीहरूको पहिचान र अनुगमन गर्ने क्षमताको विकास गर्ने।
२.८.१०.१.११	सम्भाव्य द्वन्द्वकर्ताको पहिचान र अनुगमन गर्ने तथा द्वन्द्व व्यवस्थापन गर्ने क्षमताको विकास गर्ने।
२.८.१०.१.१२	तथ्याङ्क सङ्कलन, विश्लेषण, प्रशोधन तथा उपयोग क्षमतामा अभिवृद्धि गर्ने।
२.८.१०.१.१३	देशको आन्तरिक तथा वाह्य परिस्थितिबारे बहुस्रोत सूचनाको तथ्याङ्कीय आधार विकास गर्ने र सूचना बैङ्क निर्माण गरी सम्बद्ध निकायहरूबीच सूचनामा पहुँच र उपयोगका लागि सञ्जाल तयार गर्ने।
२.८.१०.१.१४	आमसञ्चार संस्था र साधनलाई विदेशी नागरिक वा सङ्गठनको अधीनमा पर्नबाट रोक्ने वा सुरक्षित राख्ने।
२.८.१०.१.१५	कम्प्यूटरमा राखिएका सूचनाहरूको सुरक्षार्थ कानूनी सुरक्षा र राष्ट्रिय संरचना निर्माण गर्ने।
२.८.१०.१.१६	नेपाललाई अन्तर्राष्ट्रिय सूचना सञ्जालमा आवद्ध गर्न र प्रभावकारी संयन्त्रको विकास गर्दै यस्तो संयन्त्रबाट नेपाल सम्बन्धी सत्य तथा वस्तुपरक सूचनाहरू प्रवाह गर्ने।
२.८.१०.१.१७	राष्ट्रिय स्वतन्त्रता, संस्कृति तथा जीवन पद्धति, चालचलन र परम्परालाई नकारात्मक प्रभाव पार्ने सूचना र घुसपैठबाट देशलाई जोगाउने।

त्यसै गरी राष्ट्रिय सुरक्षा नीति, २०७५ को भाग २ "सुरक्षा वातावरण" अन्तर्गत नेपाल लगायत दक्षिण एशियाली मुलुकहरूमा सुरक्षा वातावरणलाई खलल पार्ने विभिन्न तत्वहरूमध्ये एउटा तत्वको रूपमा साइबर हमलालाई लिइएको देखिन्छ भने भाग ६ "चुनौती र खतरा" अन्तर्गत नेपालका राष्ट्रिय मूल्यमान्यताहरू र राष्ट्रहितको संरक्षण र प्रवर्द्धन गर्नमा देशका संवेदनशील निकायमा हुनसक्ने साइबर हमलालाई चुनौती र खतराको रूपमा पहिचान गरिएको छ।

सोही नीतिको भाग ७ ले सरकारी तथा गैरसरकारी क्षेत्रको दैनिक कामकाजमा अपनाइएका कम्प्यूटर प्रविधि र स्वचालित विद्युतीय सञ्चार प्रणालीमाथि हुन सक्ने साइबर हमला विरुद्ध सुरक्षाको सुनिश्चितता गर्ने नीतिगत प्रबन्धमा जोड दिएको देखिन्छ भने नेपाल सरकारका मन्त्रालयहरूले राष्ट्रिय सुरक्षा नीति, २०७५ बमोजिम आआफ्ना मन्त्रालयसँग सम्बन्धित

नीतिहरूका लागि आवश्यक पर्ने कानून, नियमावली र कार्ययोजना बनाई कार्यान्वयन गर्न मार्ग दर्शन गरेको देखिन्छ। सोही नीतिगत मार्गदर्शन बमोजिम प्रस्तुत कार्ययोजना तयार गरिएको छ।

सूचना तथा सञ्चार प्रविधि नीति, २०७२ को दफा ११.२१ मा "सूचना तथा सञ्चार प्रविधि प्रयोगमा सुरक्षा एवं विश्वसनीयता प्रत्याभूति" अन्तर्गत दफा ११.२१.१ मा नागिरकको सूचनाको गोपनीयता तथा वैचारिक स्वतन्त्रता लगायत अन्य मूल्यहरु प्रवर्द्धन गर्न समयानुकूल साइबर सरक्षा नीति, निर्देशिका निर्माण गरी लागू गरिनेछ" भन्ने नीतिगत व्यवस्था गरेको छ |

सूचना तथा सञ्चार प्रविधि नीति, २०७२ को दफा १२.२१ "सूचना तथा सञ्चार प्रविधि प्रयोगमा सुरक्षा एवं बिश्वसनीयता प्रत्याभूति" को उपदफाहरुमा उल्लेखित रणनीतिहरुको समेत आधारमा यो प्रतिवेदन तयार गरिएको छ |

१२.२१.१	प्रभावकारी कानूनी व्यवस्थामा आधारित साइवर अपराधको रोकथाम तथा अभिजनको प्रणाली विकास गरिनेछ। साइबर अपराध रोकथाप तथा अनुसन्धान गर्न कानून कार्यान्वयन निकाय (Law Enforcement Agencies) हरुको क्षमता अभिबृद्धि गर्दै लगिनेछ।
१२.२१.२	अनलाईन सुरक्षा प्रत्याभूत गर्न तथा तत्सम्बन्धी चेतना अभिवृद्धि गर्न व्यक्ति तथा व्यवसाय लक्षित कार्यक्रमहरु तर्तुमा गरी लागू गरिनेछ।
१२.२१.३	सरकारी तालिम केन्द्रहरुसँग समेतको सहकार्यकमा उच्च स्तरको साइवर सुरक्षा चुनौति सामना गर्न एक वृहत क्षमता अभिवृद्धि कार्यक्रम तर्जूमा गरी लागू गरिनेछ।
१२.२१.४	उपयुक्त सरकारी संयन्त्रको मातहतमा एक साइवर सुरक्षा निकाय (Cyber Security Cell) स्थापना गर्दै साइवर आक्रमण पहिचान, रोकथाम, प्रतिरक्षा लगायतका आयामहरुको प्रभावकारी सम्बोधन हुने व्यवस्था मिलाइनेछ। यसै सन्दर्भमा सूचना तथा सञ्चार मन्त्रालयमा आपतकालीन कम्प्यूटर उद्धार समुह (Computer Emergency Response Team) स्थापन गरी साइवर सुरक्षा सम्बन्धी चुनौतिहरु शिघ्र सम्बोधन गर्ने व्यवस्था मिलाइनेछ।
१२.२१.५	सम्बन्धित शैक्षिक संस्थाहरुसँग समेतको सहकार्यमा साइवर सुरक्षाका क्षेत्रमा पर्याप्त जनशक्तिको विकास गरिनेछ।
१२.२१.६	विशेषज्ञताको तालिम (Certified Specialist Training) मार्फत सूचना सुरक्षा विज्ञहरुको निरन्तर दक्षता अभिवृद्धिका कार्यक्रम लागू गरिनेछ।
१२.२१.७	साइवर सुरक्षा शिक्षा प्रदान गरी समग्रमा सूचना तथा सञ्चार प्रविधिको प्रयोगकर्तालाई समक्षम बनाउन विशेष कार्यक्रम तर्जूमा गरिनेछ।
१२.२१.८	विद्युतीय कारोवार ऐन २०६३ मा उल्लेखित प्रावधान अनुरुप सूचना प्रविधि न्यायाधीकरण (IT Tribunal) स्थापन गरिनेछ।

१.७ अध्ययन विधि

समितिलाई दिइएको जिम्मेबारी बमोजिम प्रतिवेदन तयार गर्नका लागि देहायका अध्ययन विधिहरू अवलम्बन गरिएको थियोः

१.७.१. प्रतिवेदन तयार गर्नका लागि समितिका सदस्यहरूबीच विभिन्न चरणमा बैठक बसी विस्तृत छलफल गरिएको।

१.७.२. प्रतिवेदन तयार गर्ने क्रममा साइबर सुरक्षासँग सम्बन्धित विभिन्न कानूनी व्यवस्था, मापदण्ड लगायत विभिन्न मितिमा जारी भएका एड्भाइजरीहरूको अध्ययन गरिएको।

१.७.३. नेपाल सरकारका निकायहरूमा साइबर सुरक्षा सम्बन्धी भए गरेका अभ्यासहरूको अध्ययन गरिएको।

१.७.४. अन्तर्राष्ट्रिय नीति, कानून, मापदण्ड असल अभ्यास आदिको अध्ययन गरिएको।

१.७.५. अन्तर्राष्ट्रिय साइबर जगतमा हुने तथा नेपालमा हुने साइबर जोखिम, साइबर आक्रमण एवम् सूचना सुरक्षाका विद्यमान चुनौतीहरूको अध्ययन गरिएको।

१.७.६. सूचना प्रविधि क्षेत्रसँग सम्बन्धित विज्ञहरूसँग छलफल गरिएको।

१.८. अध्ययनको सीमा

१.८.१. **समय सीमाः** समितिलाई प्रतिवेदन तयार गर्न एक महिनाको मात्र समयसीमा प्राप्त भएको।

१.८.२. **विषय-क्षेत्रः** कार्यक्षेत्रमा उल्लिखित विषय-क्षेत्र (साइबर अपराध नियन्त्रण, साइबर सुरक्षा, सूचना सुरक्षा आदि) रहेको।

परिच्छेद २ – साइबर सुरक्षा तथा साइबर सुरक्षा जोखिम - साइबर आक्रमण/अपराध

२.१. साइबर सुरक्षा

साइबर सुरक्षा भनेको प्रणाली, नेटवर्क, कम्प्युटर, सर्भर, मोबाइल लगायतका उपकरण, प्रोग्राम र डाटामा हुन सक्ने डिजिटल आक्रमण/जोखिम तथा सूचना प्रविधिको दुरुपयोगबाट हुन सक्ने जोखिमबाट जोगाउने, सोलाई न्यूनीकरण गर्ने अभ्यास हो । साइबर सुरक्षा एक बृहत विषय हो ।प्रभावकारी साइबर सुरक्षा उपायहरू लागू गर्नु आज विशेष गरी चुनौतीपूर्ण छ किनभने त्यहाँ मानिसहरू भन्दा धेरै उपकरणहरू छन्, र आक्रमणकारीहरू थप नवीन हुँदैछन्। अनधिकृत पहुँचबाट आफ्नो सफ्टवेयर, नेटवर्क, हार्डवेयर हरूको सुरक्षाले मात्र साइबर सुरक्षामा पुर्णता नमिल्न सक्छ । साइबर सुरक्षाका दृष्टिकोणले सुरक्षित राख्नुपर्ने कम्प्युटर, नेटवर्क, प्रोग्राम वा डाटामा फैलिएको सुरक्षाका धेरै तहहरू हुन्छन् । एक सङ्गठनमा प्रभावकारी साइबर सुरक्षा सिर्जना गर्न व्यक्तिहरू, प्रक्रियाहरू र प्रविधिहरू (PPTs - People, Process, Technology) सबै एकअर्काको पूरक हुनुपर्छ ।

- **व्यक्ति :** प्रयोगकर्ताहरूले आधारभूत डाटा सुरक्षा सिद्धान्तहरू (जस्तैः प्रणालीको सुरक्षित प्रयोग, बलियो पासवर्डहरू छनोट गर्ने, इमेलमा संलग्न स्पाम , फिसिङ लिङ्कहरू आदिबाट सावधान रहन, र डाटा ब्याकअप गर्ने आदि) बुझ्नुपर्छ र पालना गर्नुपर्छ ।
- **प्रक्रिया :** प्रत्येक सङ्गठनहरूसँग जोखिमहरू आँकलन गर्न, प्रणालीहरू सुरक्षित गर्न, प्रयास गरिएका र सफल साइबर आक्रमणहरू पहिचान गर्न, सामना गर्न, धम्कीहरू पत्ता लगाउन र प्रतिक्रिया दिन, र सफल आक्रमणहरूबाट पर्ने असर न्यूनीकरण गर्न, प्रणालीको निरन्तरता, डाटा पुन: प्राप्ति गर्नका लागि मार्गनिर्देशन गर्ने एउटा रूपरेखा/फ्रेमवर्क हुनुपर्छ ।
- **प्रविधि :** सङ्गठन र व्यक्तिहरूलाई साइबर आक्रमणहरूबाट जोगाउन आवश्यक कम्प्युटर सुरक्षा उपकरणहरू तथा प्रविधि (जस्तैः सुरक्षित पूर्वाधार, नेटवर्क, फायरवालहरू, DNS फिल्टरिङ, मालवेयर सुरक्षा, एन्टिभाइरस सफ्टवेयर र इमेल सुरक्षा, ब्याकअप, रिकभरी, अनुगमन संयन्त्र/उपकरण आदि) आवश्यक पर्दछन् ।

CIA लाई साइबर सुरक्षाको मुख्य ३ स्तम्भको रूपमा पनि मानिन्छ। जहाँ कुनै एकको कमी रहेको खण्डमा साइबर आक्रमणको पहुँच सजिलै हुन सक्दछ।

CIA triad

- Confidentiality
- Integrity
- Availability

२.२. साइबर सुरक्षा जोखिम - साइबर आक्रमण/अपराध

साइबर सुरक्षा जोखिमले कुनै पनि सम्भावित दुर्भावनापूर्ण आक्रमण (malicious attack) लाई जनाउँछ जसले अवैध रूपमा डाटा पहुँच गर्न खोज्छ (Confidentiality), डिजिटल सञ्चालनमा बाधा (Availability) पुऱ्याउँछ वा डाटालाई क्षति (Integrity) पुऱ्याउँछ। साइबर जोखिम/आक्रमणहरू सामान्यतया प्रणालीमा अनाधिकृत पहुँच पुऱ्याई गोपनीय वा संवेदनशील डाटा सूचना प्राप्त गर्ने (Confidentiality), डाटा परिवर्तन गर्ने वा नष्ट गर्ने (Integrity) उद्देश्यका हुन्छन् र सोको गलत प्रयोग गर्ने; प्रयोगकर्ताहरूबाट पैसा लुट्ने; वा सामान्य व्यापार प्रक्रियाहरू अवरोध गर्ने गर्छन्। उदाहरणका लागि व्यक्तिगत स्तरमा, साइबर सुरक्षा आक्रमणले पहिचान चोरी (Identity theft), जबरजस्ती लुट्ने प्रयासहरू, व्यक्तिगत / फोटोहरू जस्ता महत्त्वपूर्ण डाटा गुमाउने, आर्थिक नोक्सानी जस्ता हानिकारक परिणाम हुन सक्छ । हामी सबै सरकारी सेवा, अस्पतालहरू, वित्तीय सेवा कम्पनीहरू र पावर प्लान्टहरू जस्ता महत्वपूर्ण पूर्वाधारहरूमा निर्भर छौं। तसर्थ ती र अन्य संस्थाहरूलाई सुरक्षित गरी समाजलाई क्रियाशील राख्न आवश्यक छ।

सूचनाको गोपनीयता तथा सुरक्षा साइबर सुरक्षाको अभिन्न पाटो हो। विश्वका ठूला प्राविधिक संस्थाहरूले प्रयोगकर्ताहरूको गोपनीयता हनन् गर्दै आम निगरानी (mass surveillance)गर्ने गरेको, प्रयोगकर्ताहरूको व्यक्तिगत जानकारीहरू व्यापारिक तथा कुटनैतिक प्रयोजनका लागि खरिद/बिक्री गरेको जस्ता समाचारहरू आइरहेको परिप्रेक्षमा नेपालमा पनि सूचनाको सुरक्षाका विषयमा देखिएका जोखिमका विषयलाई साइबर सुरक्षासँगै विचार गर्नुपर्ने हुन्छ।

१. राष्ट्र, राजनीति तथा कुटनीतिसँग सम्बन्धित सूचना तथा जानकारीहरू सामाजिक सञ्जाल तथा सञ्चार माध्यमहरूमा गोप्यता नै नरहने गरी सार्वजनिक हुने हुँदा राष्ट्रिय सुरक्षाका विषयका महत्वपुर्ण जानकारीहरू नेपालको विरुद्धमा कार्यगर्नेहरूका लागि सहज हुने गरेको।
२. सामाजिक सञ्जालहरूमा सुरक्षा निकायका सम्बन्धमा भ्रामक तथा गोपनियता भंग हुने किसिमका समाचारहरू सार्वजनिक हुने हुँदा सुरक्षा निकायको कार्यसम्पादन तथा त्यहाँ कार्यरत कर्मचारीहरूको गोप्यता नै भङ्ग हुने गरेको।
३. सामरिक दृष्टिकोणले महत्वपुर्ण मानिने स्थान, कार्यालयहरूको नक्सा, तस्विर, श्रव्यदृष्यहरू नेपालभित्र तथा नेपाल बाहिर रहेर कसको के कति पहुँच छ वा हुनुपर्ने भन्ने विषय स्पष्ट नभएको।
४. पुरा विश्व नै सूचना प्रविधिमय रहेको अवस्थामा अपराधिक तथा देश विरोधी प्रयोजनहरूका लागि सुरक्षा निकायहरूले निगरानी गर्न नसकिने किसिमको प्रविधि हरूको प्रयोग हुन सक्ने अवस्था रहेको।
५. सामाजिक सञ्जालमा रहेको करोडौं नेपाली प्रयोगकर्ताहरूको हरेक गतिविधि, क्रियाकलाप माथि विश्वका शक्तिशाली इन्टेलिजेन्स संस्थाहरूबाट भइरहेको आम निगरानी सम्बन्धमा जानकार रहँदा पनि त्यसका विरुद्धमा कुनै कार्य गर्न नसकिएको अवस्था रहेको। सामाजिक सञ्जालको नेपालमा नै सम्पर्क कार्यालयहरू नहुँदा साइबर निगरानी तथा अनुसन्धान कार्य कठीन रहेको।

धेरैजसो जनमानसमा साइबर सुरक्षा जोखिम भनेको इमेल फिसिङ्ग, वेभ साईट ह्याक, एटिएमबाट पैसा चोरी, सामाजिक सञ्जालमा हुने घटना, भण्डारण गरिएका डाटाहरूको चोरी तथा परिवर्तन गरिने आदिलाई बुझिने गरिएको छ। नेपाल

सरकारको इ-गभर्नेन्सको अवधारणा अनुरूप विभिन्न निकायले दिने सेवा सुविधा विद्युतीय माध्यमबाट प्रदान गरिनु पर्ने देखिएको छ। इन्टरनेटको व्यापक प्रयोगले इन्टरनेट अफ थिङ्गस (Internet of Things) जस्ता नयाँ अवधारणा अनुरूप विभिन्न संस्थाहरूबाट स्वचालित सेवाहरू विभिन्न देशहरूमा उपलब्ध गराइरहेको अवस्था छ। सूचना प्रविधिको प्रयोग तथा विकासले हरेक दिन जसो नयाँ नयाँ आविस्कारहरू हुँदै सोही मार्फत् अझ परिस्कृत ढङ्गबाट सेवा सुविधा दिँदै जानुपर्ने देखिन्छ। यसरी दिएका सेवाहरू पाउनबाट सेवाग्राहीहरूलाई बञ्चित गराउनु (Availability) पनि साइबर सुरक्षा जोखिमको वर्गीकरणमा पर्दछ ।

यसरी अर्काको पहिचान अनधिकृत रूपमा प्रयोग, क्रेडिट कार्ड तथा एकाउन्ट आदिको चोरी गरी गरिने बैंकिङ् कसुर, अनाधिकृत डाटा परिवर्तन वा नष्ट, अर्काको कम्प्युटर, विद्युतीय उपकरण तथा नेटवर्कमा पुऱ्याउने क्षति, डिजिटल सेवामा अवरोध लगायत अवैधानिक कार्यलाई साइबर अपराध मानिन्छ । त्यसबाहेक पनि साइबर अपराध कम्प्युटर तथा कम्प्युटर नेटवर्क प्रयोग गरेर हुने अन्य विभन्न प्रकारका अपराधहरू हुन्छन् । उदाहरणका लागि इन्टरनेटको प्रयोगमार्फत गरिने चरित्र हत्या, गलत सूचना प्रवाह, उत्पिडन, हिंसा फैलाउने कार्य, यौनजन्य हिंसा, ठगी आदि ।

२.३. साइबर सुरक्षा जोखिम: वर्गीकरण

साइबर सुरक्षा जोखिमलाई लक्षित समूहको आधारमा निम्नानुसार वर्गीकरण गर्न सकिन्छ ।

- व्यक्तिगत तथा पारिवारिक सुरक्षा जोखिम: Identity Theft, Blackmailing,
- साङ्गठनिक सुरक्षा जोखिम:- Intellectual Property Theft, CIA Breaching, Hacking
- राष्ट्रिय सुरक्षा जोखिम:- Cyber Terrorism, National DNS attack

साइबर सुरक्षा जोखिमलाई श्रोतको आधारमा मुख्य रूपमा २(दुई) प्रकारमा बिभाजन गर्न सकिन्छ । पहिलो आन्तरिक जोखिम (Internal Threat) र दोश्रो बाह्य जोखिम (External Threat)।

- आन्तरिक जोखिम (Internal Threat)

  Internal Threat मुख्य गरी कुनै व्यक्तिको नेटवर्कमा आधिकारिक पहुँच भएको बेला सम्भव हुन्छ। आधिकारिक पहुँच हुनलाई सो व्यक्तिको कम्प्युटर प्रणाली वा नेटवर्कमा खाता (User Account) भएको हुनु पर्दछ वा भौतिक रूपमा पहुँच भएको हुनुपर्छ । यसरी जुनसुकै सङ्घ संस्थाका कर्मचारीहरूको गैह्र जिम्मेवार कार्यशैली वा ज्ञानको कमी तथा उक्त सङ्घ संस्थाका लागि अपनाइएका सुरक्षाका विभिन्न प्रक्रियाहरूको विफलताले Internal Threat उत्पन्न हुन्छ।

- बाह्य जोखिम (External Threat)

External Threat सङ्गठन बाहिर काम गर्ने व्यक्ति वा संस्थाहरूबाट उत्पन्न हुन सक्छन्। External Threat मा कम्प्युटर प्रणाली वा नेटवर्कमा आधिकारिक पहुँच भने हुँदैन। बाह्य आक्रमणहरू मुख्य गरी जडान गरिएका नेटवर्कहरू (तार र तारारहित), भौतिक घुसपैठ (Physical Intrusion) वा साझेदार (Partner) नेटवर्कहरू मार्फत हुन्छन्। साथै प्राकृतिक प्रकोपहरू समेत External Threat अन्तर्गत पर्दछन् । External Threat पनि जानेर वा नजानेर आफ्नै कम्प्युटरमा ज्ञानको कमीले Malware हरू Install भई थाहा नपाई सोही कम्प्यूटरबाट अन्य कमप्युटरमा (Denial-of-Service Attack -DOS) जस्ता आक्रमणहरू भएको हुन सक्छ।

आन्तरिक जोखिम वा बाह्य जोखिम सिर्जना गर्न मुख्य गरी तीन वटा Agents हरूको भूमिका रहेको हुन्छ । ती Agents हरूमा मानिस, प्राकृतिक विपत्ति र प्राविधिक खतरा (Human, Natural Disaster and Technological Threats) रहेका छन् । मानवीय खतरा अन्तर्गत सङ्गठनमा काम गर्ने कर्मचारी वा बाह्य Hacker हरू हुन सक्छन् । नेपालको सन्दर्भमा प्राकृतिक विपत्ति अन्तर्गत मुख्य गरी भूकम्प, डुबान, बाढी,, पहिरो आगलागी आदि रहेका छन्। यसै गरी प्राविधिक खतरा (Technological Threat) अन्तर्गत Malware, Phishing, Hacking/Unauthorized Access, Email Threat, Denial of Service Attack, Social Media, Social Engineering, Online Threats and Harassment/Defame (Social Media), Cyber Stalking, Source Code Theft, Online Fraud आदि पर्दछन ।

२.४. साइबर सुरक्षा जोखिमका सर्जकहरू (Threat Actors)

साइबर सुरक्षा सम्बन्धी जोखिम तथा कमजोरीहरू, चेतनाको कमी वा विकसित प्रविधिको माध्यमबाट दुर्भावनापूर्ण उद्देश्यका साथ सञ्चार तथा सूचना प्रविधि सम्बन्धी उपकरण, नेटवर्क, सेवा वा प्रणालीहरूमा अनाधिकृत पहुँच प्राप्त गर्ने प्रयास गर्ने व्यक्ति, समूह, संस्था वा राज्यलाई साइबर Threat Actors भनिन्छ। यी Threat Actor हरूको मुख्य उद्देश्य लक्षित निशानाको डाटा, उपकरण, नेटवर्क, सेवा वा प्रणालीहरूमा पहुँच प्राप्त गर्नु वा केही परिवर्तन गर्नु रहेको हुन्छ। इन्टरनेटको विश्वव्यापी प्रकृतिको कारण यी Threat Actor हरू शारीरिक रूपमा संसारको कुनै पनि ठाउँमा बसी नेपालमा अवस्थित सञ्चार तथा सूचना प्रविधिको क्षेत्रमा असर पुऱ्याउन सक्छन्। लक्ष्य तथा लगावको आधारमा मुख्यतयाः Threat Actors लाई निम्नानुसार वर्गीकरण गर्न सकिन्छः

---

१. राष्ट्र/राज्य Threat Actor: राष्ट्र/राज्य Threat Actor हरूले राष्ट्रिय हितको निम्ति आणविक, वित्तीय, प्रविधि लगायत धेरै क्षेत्रहरूको सूचना तथा डाटा प्राप्त गर्ने लक्ष्य राख्छन्। केही राष्ट्रहरूले आफ्नै सरकारी गुप्तचर निकायहरू राष्ट्र-राज्य Threat Actor को रूपमा प्रयोग गर्छन् भने केही राष्ट्रहरूले साइबर अपराधमा विशेषज्ञता भएका समूह

वा संस्थाहरू सँग काम गर्छन्। राष्ट्र/राज्य Threat Actor को मुख्य उद्देश्य जासुसी, चोरी वा राष्ट्रको हितलाई बढावा दिने अन्य कुनै गतिविधि गर्नु रहेको हुन्छ।

२. साइबर अपराधी: सञ्चार तथा सूचना प्रविधिको क्षेत्रको प्रयोग गरी डिजिटल प्रणाली वा नेटवर्कहरूमा दुर्भावनापूर्ण गतिविधिहरू सूचना गर्ने व्यक्ति वा समूहलाई साइबर अपराधी भनिन्छ। साइबर अपराधीहरूको मुख्य उद्देश्य कुनै संस्थाको संवेदनशील जानकारी वा व्यक्तिगत डाटा दुरुपयोग गरी पैसा कमाउने अथवा आफ्नो स्वार्थ पूरा गर्ने रहेको हुन्छ।

३. Hacktivist: आफ्नो विश्वास र विचारधाराहरूलाई प्रचार-प्रसार गर्न वा अगाडि बढाउन साइबर अपराध गर्ने व्यक्ति, समूह वा संस्थाहरूलाई Hacktivist भनिन्छ। Hacktivist हरूले गोप्य सूचना सार्वजनिक रूपमा चुहावट गर्ने, नराम्रो मानिएका संस्था वा सरकारी निकायहरूको ICT प्रणालीमा हमला गरी सेवा अवरुद्ध गर्ने लगायतका साइबर अपराधहरू गर्छन् र यी साइबर अपराध प्राय राजनीतिक र सामाजिक मुद्दाहरूबाट प्रेरित हुन्छन्।

४. साइबर आतङ्कवादी: जनमानशमा डर-त्रास तथा आतङ्कबादी फैलाउन वा संवेदनशील सूचना तथा सञ्चार प्रविधि पूर्वाधारहरूको सेवामा अवरोध उत्पन्न गर्न साइबर हमला गर्ने परिचित आतङ्कवादी समूह वा व्यक्तिलाई साइबर आतङ्कवादी भनिन्छ। साइबर आतङ्कवादीहरूले प्रायः सरकारी निकायबाट सूचना चोरी गर्न वा खानेपानी, बिजुली, बाँध, उद्योग जस्ता राष्ट्रिय स्तरका संवेदनशील पूर्वाधारहरूमा अवरोध ल्याउन साइबर हमला गर्छन्।

५. Thrill Seekers: परीक्षण तथा मनोरञ्जनको लागि कुनै ICT उपकरण, नेटवर्क, सेवा वा प्रणालीहरूमा दुर्भावनापूर्ण गतिविधिहरू सूचना गर्ने व्यक्ति वा समूहलाई Thrill Seekers भनिन्छ। केही Thrill Seekers हरू कम्प्युटर प्रणाली र सञ्जालले कसरी काम गर्छ भन्ने बारे थप कुरा जान्न साइबरसपेसमा अवैधानिक गतिविधिहरू गर्छन् भने केही Thrill Seekers सोही काम मनोरञ्जनको लागि गर्छन्।

६. भित्री व्यक्ति Threat Actor: संस्थाको विरोधी वा प्रतिस्पर्धीहरूलाई ICT नेटवर्क वा प्रणालीहरूसँग सम्बन्धित संवेदनशील सूचना बेच्न वा संस्थाले आफूलाई अनुचित व्यवहार गरेको महसुस गरी बदलाको भाव बोकेका असन्तुष्ट कर्मचारीहरूले संस्थाको साइबरस्पेसमा दुर्भावनापूर्ण गतिविधिहरू गर्न सक्छन् र यी कर्मचारीहरूलाई भित्री व्यक्ति Threat Actor भनिन्छ। संस्थामा कार्यरत रहँदा भित्री व्यक्ति Threat Actor हरूलाई संवदेनशील सूचना तथा प्रणालीमा पहुँच हुने हुँदा यस प्रकारको Threat ले गम्भीर नोक्सान पुऱ्याउन सक्छ।

७. प्रयोगकर्ताको गल्ती: संस्थागत प्रयोगकर्ताहरूलाई सो संस्थाको साइबरस्पेसमा उच्च तहको पहुँच हुने हुँदा यी प्रयोगकर्ताहरूले अन्जानमा गरेको गल्तीले ठूलो साइबर Threat निम्त्याउन सक्छ।

परिच्छेद ३ – वर्तमान परिदृश्य / अवस्था

३.१. सूचना तथा सञ्चार प्रविधिको विकास तथा विस्तार

सूचना र सञ्चार प्रविधिको क्षेत्रमा भएको द्रूततर विकासले गर्दा आधुनिक विश्व नै एक गाँउ (Global Village) मा रूपान्तरण भइसकेको छ। नेपालले देशको सामाजिक तथा आर्थिक क्षेत्रको बृहत्तर विकास तथा रूपान्तरणको लागि दिगो विकासका लक्ष्यहरू (Sustainable Development Goals) हासिल गर्नेतर्फ आफ्नो प्रतिबद्धता व्यक्त गर्दै "डिजिटल नेपाल फ्रेमवर्क, २०७६" तर्जुमा गरी लागु गरेको छ। हाल उक्त फ्रेमवर्क बमोजिम कार्यक्रमहरू तयार भई आठवटा प्रमुख क्षेत्र अन्तर्गत ८० वटा पहलहरू पहिचान भई सम्बन्धित जिम्मेवार निकायहरूबाट कार्यन्वयन भइरहेको अवस्था छ।

दूरसञ्चार तथा इन्टरनेट सेवाको पहुँच विस्तार

म्यागनेटो प्रविधिको माध्यमबाट वि. स. १९७० देखि दूरसञ्चारको युगमा प्रवेश गरेको नेपालले हाल देशका ७७ जिल्लामा नै फोरजी (4G) जस्तो अत्याधुनिक प्रविधिको माध्यमबाट सेवा पुऱ्याइसकेको छ भने फोरजी भोल्टे (4G-VOLTE) सेवा समेत प्रारम्भ भइसकेको छ।

नेपाल दूरसञ्चार प्राधिकरणको मंसिर, २०७८ को MIS Report अनुसार टेलीफोनको घनत्व (स्थिर तथा मोबाइल दुवै गरी) करिब १३९ प्रतिशत पुगिसकेको छ, जसमा मोबाइलको योगदान १३६ प्रतिशत रहेको छ। नेपाल दूरसञ्चार प्राधिकरणको माघ २०७८ को रिपोर्ट अनुसार २ करोड ७७ लाख ६ हजारले High Speed Internet, १ करोड ९८ लाख ५३ हजार मोबाइल ब्रोडब्याण्ड प्रयोगकर्ता रहेका छन्। जनसङ्ख्याको हिसाबले करिब ४ करोड २० लाख ग्राहकहरूले सिमकार्ड प्राप्त गरिसकेका छन्। यसबाट एक जना ग्राहकले एक भन्दा बढी सिमकार्ड प्राप्त गरेको भन्ने पनि बुझिन्छ।

ब्रोडब्याण्ड इन्टरनेट (Broadband Internet) तर्फको घनत्व करिब ११९ प्रतिशत जसमा स्थिर (तारवाला) ब्रोडब्याण्ड (Fixed Broadband) को घनत्व करिब ३० प्रतिशत र मोबाइल ब्रोडब्याण्ड(Mobile Broadband) इन्टरनेटको घनत्व करिब ८१ प्रतिशत रहेको पुगिसकेको छ। अर्थात् ब्रोडब्याण्ड इन्टरनेट सेवाको पहुँच विस्तारमा मोबाइल ब्रोडब्याण्डको योगदान बढी रहेको छ। जनसङ्ख्याको हिसाबले हेर्दा करिब ३ करोड ६० लाख ग्राहकहरूको ब्रोडब्याण्ड इन्टरनेट सेवामा पहुँच पुगिसकेको छ।

नेपालका शहरी तथा ग्रामिण क्षेत्रहरूमा 2G (GSM) र 3G (WCDMA and CDMA-EVDO) प्रविधिहरूको माध्यमबाट मोबाइल टेलिफोन सेवा उपलब्ध भएको छ।

त्यस्तै FTTH, Wireless Radio(WiFi), 3G र 4G (LTE) प्रविधिहरूको माध्यमबाट स्थिर र मोबाइल ब्रोडब्याण्ड वा High Speed Internet सेवा उपलब्ध भएको छ ।

नेपालमा मुख्यतः नेपाल दूरसञ्चार कम्पनी लिमिटेड र एनसेल आजियाटाले मोबाइल टेलिफोन सेवा तथा मोबाइल ब्रोडब्याण्ड इन्टरनेट सेवा उपलब्ध गराएका छन् । त्यस्तै एक सय भन्दा बढी इन्टरनेट सेवा प्रदायक संस्थाहरूले पनि नेपालका शहरी तथा ग्रामिण क्षेत्रहरूमा ब्रोडब्याण्ड इन्टरनेट सेवा उपलब्ध गराउदै आएका छन् ।

ब्रोडब्याण्ड इन्टरनेट सेवाको सेवाको विस्तारसँगै सामाजिक सञ्जाल (Facebook, Twitter etc), Online Video (Youtube, Tiktok), Online Media लगायतमा मानिसहरू पहुँच बढेको छ । त्यस्तै शहरी तथा ग्रामिण क्षेत्रहरूमा ब्रोडब्याण्ड इन्टरनेट सेवाको उपलब्धता बढेसँगै उक्त प्रविधिमा आधारित धेरै Government तथा Non-Government Online सेवाहरू जस्तै E-Commerce, Online-Banking, Mobile Banking, Mobile-Wallets, Insurance, E/M-Learning, E/M-Health लगायत र App हरूको निर्माण र पहुँच विस्तार भएका छन्।

सूचना प्रविधिको विकास तथा नेपालमा इन्टरनेट कनेक्टिभिटसँगै विद्युतीय माध्यमबाट डिजिटल कारोबार एवं भुक्तानी तथा बैंकिङ सेवाको प्रयोग व्यापक हुँदै गएको छ । राष्ट्र बैंकको बैशाख २०७८ को तथ्याङ्क अनुसार इन्टरनेट बैंकिङ सेवा एघार लाखभन्दा बढी, मोबाइल बैंकिङ सुविधा १ करोड ३५ लाख भन्दा बढी र बैंकिङ कार्ड सेवा ११ लाख भन्दा बढी व्यक्तिहरूले प्रयोग गरिरहेका छन्। नेपालमा करीब ४० लाख व्यक्तिहरू डिजिटल वालेट प्रयोग गर्छन् । विश्व बैंकको २०१७ को तथ्याङ्क अनुसार नेपालमा ६६ अरब रुपैयाँको सूचना तथा सञ्चार साधन सामग्री आयात भएको देखिन्छ जुन समग्र आयातको ५.२ प्रतिशत हो । धेरैजसो सरकारी, गैरसरकारी सङ्घसंस्था व्यापारिक प्रतिष्ठानहरूले इन्टरनेटमा उपस्थिति जनाइसकेका छन् भने आफ्नो सेवाहरू प्रदान गर्न डिजिटल प्रविधिको प्रयोग गर्दैछन् । सरकारी स्तरमा सार्वजनिक सेवाप्रवाहलाई डिजिटल माध्यमबाट प्रवाहमा जोड दिइएको पाइन्छ ।

इन्टरनेट सेवाग्राहीहरू वा प्रयोगकर्ताहरू साइबर सुरक्षाका विषयमा आफु जागरुक नहुँदा र App तथा Online सेवा प्रदान गर्ने संस्थाहरूले Software App/Website Develop गर्दा प्रयाप्त साइबर सुरक्षाका मापदण्ड तथा उपायहरू अवलम्बन नगर्दा, साथै मोबाईल र इन्टरनेट सेवा प्रदायकहरूले पनि साइबर सुरक्षामा ध्यान नदिदा साइबर सुरक्षा चुनौती बढेको र सेवाग्राहीहरू साइबर आक्रमणका शिकार हुन पुगेका छन् ।

३.२. नेपालः साइबर आक्रमण/ साइबर अपराध

नेपाल सरकारका निकायहरूले आफनो सूचना एवं सेवा प्रवाह छिटो छरितो विश्वसनीय तथा प्रभावकारी बनाउनको लागि सूचना प्रविधिको प्रयोग बढाउँदै लगेको सन्दर्भमा सरकारका महत्वपुर्ण डाटा, प्रणाली उपर आन्तरिक एवं वाह्य सुरक्षा जोखिम पनि बढदै गएको देखिन्छ। सामान्यतया विद्युतीय उपकरणलाई माध्यम तथा लक्ष्य बनाई गैरकानूनी कार्य गर्नु साइबर अपराध हो। साइबर अपराध कुनै एक स्थानबाट सुरु (origin) भई सोही स्थान, शहर, देश तथा अन्तरदेशीय प्रकृतिको हुने गर्दछ। पीडित र पीडक एकै देश भित्रका बासिन्दा वा सो भन्दा बाहिरको पनि हुन सक्ने हुँदा वर्तमान परिप्रेक्षमा नेपालमा हुने गरेका साइबर अपराध तथा आक्रमणहरूलाई पनि देश भित्रबाटै हुने साइबर अपराधहरू (आन्तरिक) र अन्तरदेशीय प्रकृतिको (वाह्य) साइबर अपराधहरू आधारमा वर्गीकरण गर्न सकिन्छ। नेपालमा भैरहेका देहाय बमोजिमका साइबर आक्रमण/अपराधहरु देशभित्र तथा अन्तरदेशीय दुवै प्रकृतीका हुने गरेका छन्।

क) इमेल, म्यासेज फिसिङ, भिसिङ तथा स्पाम सम्बन्धी :

- व्यक्तिगत /व्यवसायिक इमेल तथा म्यासेजहरूमा फिसिङ लिङ्कहरू राखी इमेल, सिस्टम तथा नेटवर्कमा अनधिकृत पहुँच राख्ने।
- डाटावेसमा रहेको डाटा परिवर्तन, फ्रिज गरि फिरौती रकम असुल्ने।
- टोरेन्ट, अनलाइन कालोबजार तथा डार्कवेवमा बिक्रीमा राख्ने।
- म्यासेन्जर, ह्वाट्सएपमा पुरस्कार जितेको भन्दै शङ्कास्पद लिङ्क पेजहरूमा लैजाने।

ख) सरकारी तथा व्यवसायिक वेभसाइटहरूमाथि अनधिकृत पहुँच सम्बन्धी :

- सरकारी तथा धेरै प्रयोगकर्ताहरू रहेका व्यापारिक सङ्घसंस्थाहरूको वेभसाइटमा अनधिकृत पहुँच राखी प्रयोगकर्ताहरूको विवरण दुरुपयोग गर्ने।
- सर्भर तथा सिस्टममा अत्याधिक चाप गराई सेवाग्राहीहरूलाई सेवा लिनबाट बञ्चित गर्ने।

ग) सामाजिक सञ्जालसँग सम्बन्धित:

- सामाजिक सञ्जालको प्रयोग गरेर राष्ट्र, सरकार विरोधी अभियान (campaign) चलाउने।
- दोस्रो व्यक्तिको सामाजिक सञ्जालमा अनधिकृत पहुंच पुऱ्याएर-
  - सहयोगको लागि भनी पीडितका साथि भाइ/परिवारसँग रकम माग्ने।
  - मानहानी हुने अश्लिल, अशोभनीय श्रव्यदृष्य तथा अभिव्यक्ति (स्टाटस) राख्ने।
  - नक्कली(Fake) आइडि बनाई पीडित व्यक्तिको पद/प्रतिष्ठाको दुरुपयोग गर्ने।
- मागेको रकम नदिए अश्लिल तस्विर भिडियो सार्वजनिक गर्ने धम्की दिने (रिभेन्ज पोर्नोग्राफी)।
- व्यक्तिको ज्यान इज्जत मेटाउने धम्की/मानसिक यातना दिने (हनि ट्रयाप)।

- पेजहरू बनाएर बस्तु/सेवाको खरिद बिक्री गर्ने भनी रकम लिएर सम्पर्कविहीन हुने।
- सरुवा रोग, राष्ट्रिय विपद् जस्ता गम्भिर विषयमा भ्रामक सूचनाहरू फैलाई आतङ्क मच्चाउने।
- सामाजिक सञ्जालमा भाइरल हुन सामाजिक सद्भाव, परम्परा, रहन सहनभेषभुषा विपरितका भड्किला सामाग्रीहरू राख्ने।

घ) श्रव्यदृष्य, सङ्गीत, सफ्टवेयर, ग्राफिक डिजाइन तथा अन्वेषण/अविस्कारहरूको पाइरेसीसँग सम्बन्धित-

- चलचित्रहरूको पाइरेसी।
- गीत तथा भिडियोहरूको पाइरेसी।
- अपरेटिङ सिस्टम (OS), वेभ डिजाइन, एप्लिकेसन सफ्टवेयहरूको पाइरेसी।

ङ) व्यक्तिको परिचय चोरी अपराधिक प्रयोजनका लागि प्रयोग गर्ने जोखिम (Identity Theft) :

- सामाजिक सञ्जाल, साइबर, फोटोकपि पसल जस्ता स्थानहरूमा भेटेका/राखिएका व्यक्तिको परिचय खुल्ने कागजातहरू नागरिकता, मतदाता परिचयपत्र, सवारी चालक अनुमतिपत्र, राहदानी, फोटो आदिको प्रयोग गरेर सिम कार्ड, मोवाइल बैङ्किग्, वालेट लगायतका सेवाहरू लिई दुरूपयोग गर्ने।

च) नेटवर्क/ कम्युनिकेसन च्यानलमा अनधिकृत पहुँच पुऱ्याउने सम्बन्धी :

- सरकारी कार्यालय, सुरक्षा निकाय तथा डाटासेन्टरको नेटवर्कमा अनधिकृत पहुँच (Physical and digital access) पुऱ्याउन खोज्ने।

छ) बैंकिङ तथा वित्तीय संस्थाहरू सम्बन्धी

- विदेशी मुलुकका अपराधीहरू नेपालमै आई एटिएम बाट फर्जी कार्ड बनाई तथा पिन ह्याक गरी रकम निकाल्ने तथा रकम स्थानान्तरण गर्ने।
- बैंकिङ सिस्टम/सर्भरहरूमा अनधिकृत पहुँच राखी नेपाल बाहिर रकम स्थानान्तरण गर्ने।

ज) टेलिफोन / मेसेजबाट भ्रममा पारी रकम असुली गर्ने।

झ) नेपालका सरकारी तथा महत्वपुर्ण वेभसाइटहरूमा अनधिकृत पहुँच पुऱ्याई सेवा अवरुद्ध गर्ने, डाटा फ्रिज लगायतका कार्यहरू गर्ने।

ञ) फोन कल/एस एम एस बाइपास गर्ने।

ट) वाह्य देशमा रही नेपालमा रहेका विभिन्न संस्थाहरू वा नेपालमा रही नेपालका विभिन्न संस्थाहरूको प्ल्याटफर्म प्रयोग गरी साइबर अपराध गर्ने।

ठ) बाहिर देशमा रही बाहिरैका विभिन्न संस्थाहरू वा बाहिर देशमा रही नेपालका विभिन्न संस्थाहरूको प्ल्याटफर्म प्रयोग गरी साइबर अपराध गर्ने।

राष्ट्रिय सन्दर्भमा हाल रहेका र हुन सक्ने विभिन्न साइबर जोखिमहरू मध्य प्रमुख रूपमा निम्नानुसार रहेका छन्।

- सूचना चोरी (Information Theft)- सार्वजनिक तथा निजी क्षेत्रका महत्वपूर्ण, गोपनीय, व्यक्तिगत तथा संवेदनशील विवरणहरू चुहावट हुने, गलत प्रयोग हुने, अनधिकृत रूपमा वितरण हुने लगायतका जोखिमहरू।
- जासूसी खतरा (Espionage Threats)- सरकारी निकाय वा कर्पोरेट संस्थाको संवेदनशील डाटा वा बौद्धिक सम्पत्ति जासूसी गरेर चोर्ने लगायतका साइबर आक्रमणहरू।
- साइबर आतङ्कबाद (Cyber Terrorism)- साइबर स्पेशको प्रयोग गरी राज्य वा समाजको विरुद्ध सामाजिक सद्भावमा खलल पुर्याउने, अशान्ति अराजकता फैलाउने, द्वन्द फैलाउने लगायतका आतङ्ककारी क्रियाकलापहरू।
- साइबरमा आधारित पूर्वाग्रही प्रचार (Cyber Propaganda)- कुनै विषय प्रसङ्ग वा घटनालाई अवाञ्छित रूपमा सर्वसाधारणको धारणालाई प्रभावित पार्न साइबर प्रविधिको प्रयोग।
- महत्वपूर्ण पूर्वाधार, औद्योगिक नियन्त्रण प्रणाली, र आर्थिक खतरा (Critical Infrastructure, Industrial Control Systems and Economic Threat)।
- गलत सूचना र दुष्प्रचार (Mis-Information and Dis-Information)

माथि उल्लिखित साइबर आक्रमण तथा अपराधका लागि Hacking (User Account Hacking, System hacking, ATM Hacking), Website Defacing, Malware, Ransomware, Spams, Phising, Denial of Service, SQL Injection, Social Engineering लगायतका प्रविधिहरूको प्रयोग भईरहेको देखिन्छ। नेपालमा प्रचलित साइबर/कम्प्यूटर जोखिमका प्राविधिक शव्दाबलीहरू अनुसूची 1 मा उल्लेख गरिएको छ।

३.२.१ साइबर अपराधको प्रवृत्ति विश्लेषण

विगतमा नेपालमा भए गरेका साइबर अपराधका घटनाक्रमले कुनै पनि बेला ठुलो घटना हुन सक्नेतर्फ सङ्केत गरेको छ। महानगरीय अपराध महाशाखाका अनुसार युवावर्ग बढी सङ्ख्यामा साइबर अपराधमा लागेका छन्। जसमध्ये सामाजिक सञ्जालमार्फत् यौनजन्य हिंसा गर्ने, ठगी गर्ने, ह्याकिङ गर्ने, जथाभावी गलत सूचना फैलाउने, युट्युबमा जे पायो त्यही

पोष्ट गर्ने, नक्कली कम्पनी बनाएर अरूको आर्थिक खातामा जालसाजी गर्ने जस्ता अपराधहरू शीर्ष स्थानमा रहेका छन्।पछिल्ला दिनमा विशेषगरी फेसबुक ट्विटर, इन्स्ट्राग्राम, भाइबरलगायतका माध्यम किशोरकिशोरी माझ लोकप्रिय छन्। यिनै माध्यमले हत्या, हिंसा, बलात्कार, यौन दुर्व्यवहार, लुटपाट, तथा मानव बेचबिखनका घटना हुने गरेका छन्। कतिपय घटना जानेर भएका छन् भने कतिपय अञ्जानमा पनि हुने गरेका छन्। नेपालमा साइबर अपराधबाट सबैभन्दा बढी २० देखि ४० वर्ष उमेर समूहका महिला र त्यसपछि "अन्डरएज" बालबालिकाका पीडित भएको घटनाक्रमहरूले देखाउँछ।

पछिल्ला घटनाक्रमहरू हेर्दा राज्यका विभिन्न पद र ओहदामा बसेका व्यक्तिलाई लक्षित गर्दै अशिष्ट भाषा प्रयोग गरेर उनीहरूको चरित्र हत्या गर्ने काम भइरहेको छ। त्यस्तै, सरकारी निकाय तथा विभिन्न सङ्घ-संस्थालाई गाली बेइज्जत गर्ने कार्यहरू पनि इन्टरनेटमा प्रशस्त देख्न पाइन्छ। अनलाइन सञ्चारमाध्यमबाट पनि पक्षवादी समाचार सम्प्रेषण गर्ने, पर्याप्त आधारबिना व्यक्तिलाई दोषी दाबी गरी मानहानी गर्ने, जस्ता घटनाहरू पनि युट्युव लगायतमा बढ्दो क्रममा रहेको छ।

नेपालको सन्दर्भमा हेर्दा हाल सरकारी निकाय, सुरक्षा निकाय र बैङ्किङ तथा आर्थिक क्षेत्रमा जोखिम बढ्दै गएको छ। राष्ट्रिय स्तरमा कमजोर साइबर सुरक्षाको संरचनाले पनि जोखिमलाई अझ बढावा दिइरहेको छ। नेपालमा सरकारी क्षेत्र, सुरक्षा निकाय, वित्तीय संस्था, गैरसरकारी संस्था, एयरलाइन्स, इन्टरनेट सेवा प्रदायक र दुरसञ्चार प्रणालीमा साइबर सुरक्षाको जोखिम बढिरहेको पाइन्छ ।

प्रविधिको पहुँच बढ्दै गएको भए पनि बैङ्किग कारोबार अनि गोपनीयताजस्ता विषयबारे धेरै सर्वसाधारण जानकार नहुँदा, उचित सुरक्षा संयन्त्रको प्रयोग नहुँदा, ठगी गर्नेहरूको सङ्ख्या समेत व्यापक रूपमा बढेको छ। नेपालमा अझै पनि साइबर साक्षरता कमजोर रहेको अवस्थामा हाम्रा प्रयोगकर्ताहरू अझ बढी जोखिममा रहेका छन्। चिट्ठा परेको भन्दै सर्वसाधारणहरूको गोप्य विवरणहरू प्राप्त गर्ने र त्यसको दुरुपयोग गर्दै सम्बन्धित व्यक्तिको खाताबाट रकम हिनामिना गर्ने घटनाहरू धेरै रहेका छन्। कुनै व्यक्तिले बैङ्क वा कुनै वित्तीय सेवा प्रदायकको परिचय दिएर फोन गर्ने र विवरणहरू माग्ने पनि गर्छन्।केही समयदेखि नेपालका सङ्घसंस्था तथा व्यक्तिहरू "ह्याकिङ", "बैंकिङ्ग ठगी" लगायत विभिन्न प्रकारका साइबर आक्रमणका घटनाहरूबाट पीडित भएको देखिन्छ । अन्तराष्ट्रिय साइबरस्पेसमा निकै मौलाएको Ransomware जस्तो फिरौती तिर्नुपर्ने साइबर आक्रमण नेपालको साइबर स्पेसमा समेत बिस्तारै बढ्दै गइरहेको छ। Phishing आक्रमणबाट गैर-सरकारी निकाय मात्र नभई सरकारी तथा सुरक्षा निकाय समेत शिकार भइसकेका छन्।

राष्ट्रिय तथा अन्तर्राष्ट्रिय संवेदनशील विषयहरूमा समय-समयमा विवाद देखा परेको बेला सरकारी तथा निजी क्षेत्रका महत्वपूर्ण प्रणालीहरूमा साइबर आक्रमणको क्रम समेत बढेर गएको देखिन्छ । सरकारी निकायहरूको वेबसाईट Defacement, वित्तीय प्रणाली एवम् अन्य महत्वपूर्ण प्रणालीहरूमा अनधिकृत पहुँच तथा सेवा अवरोध गर्ने लगायतका साइबर आक्रमणहरू राष्ट्रिय सुरक्षाको दृष्टिकोणले समेत चुनौतीपूर्ण रहेका छन् ।

वित्तिय संस्थाहरूमा पनि अन्तर्राष्ट्रिय साइबरस्पेसबाट हुने हमलाहरूमा उल्लेखनीय रूपमा वृद्धि भइरहेको छ र केही हमला सफल समेत भएका छन्। करिब दुई वर्षअघि नेपालको "क" वर्गको बैंकबाट ह्याकरहरूले करिब ४६ करोड रुपैयाँ चोरेका थिए। त्यस्तै, समय समयमा ATM ह्याकका घटनाहरू समेत बाहिरिएको छ। वृहत् नेटवर्कमा कमजोर सुरक्षा प्रणाली, Unaware Users, Vulnerable उपकरणको प्रयोग, Traffic logs कायम नराख्नु, आदिले राष्ट्रिय नेटवर्कलाई अझ Vulnerable बनाएको छ। हाल नेपालका सुरक्षा निकाय, विभिन्न सरकारी निकायहरूमा sidewinder, sidecopy लगायत विभिन्न APT समुहहरूबाट हमलाहरू भएको भनी विभिन्न समाचार माध्यममा समेत आइसकेका छन् ।

यस्ता किसिमका साइबर हमला तथा आक्रमणबाट जोगिन निश्चित अवधि तोकेर योजना बनाउन आवश्यक छ र साइबर सुरक्षालाई प्राथमिकताका साथ अगाडि बढाउन जरूरी छ। नेपालका लागि साइबर हमलाका यस्ता विषयमा गम्भीर नहुने हो भने एकै पटक ठूलो जोखिमको सामना गर्नुपर्ने हुनसक्छ।

परिच्छेद ४ – विद्यमान व्यवस्था

४.१. अन्तराष्ट्रिय अभिसन्धि /सन्धि तथा सम्झौता

साइबर सुरक्षा सम्बन्धी विभिन्न अन्तराष्ट्रिय सन्धि तथा सम्झौताहरूले मुख्यत: CIA (Confidentiality, Integrity and Availability) लाई परिभाषित गरेको पाइन्छ। साइबर सुरक्षा सम्बन्धमा विश्वभरका मुलुक एवं अन्तर्राष्ट्रिय सङ्घ संस्थाहरूबाट समय समयमा विभिन्न सन्धि, सम्झौता, ऐन, नियम, निर्देशिका, मापदण्ड आदि जारी गरेको पाइन्छ । Internet Governance Forum (IGF) द्वारा त्यस्ता मुख्य मुख्य निम्न लिखित सन्धि, सम्झौता, ऐन, नियम, निर्देशिका, मापदण्ड, प्रतिवेदन आदिबारे Background Paper to the IGF Best Practices Forum on Cybersecurity मा उल्लेख गरेको पाईएको छ ।

क) Convention on Cybercrime (Budapest Convention on Cybercrime)

About the scope of Budapest Convention Harmonization of (Criminalising Conduct + Procedural Tools + International Cooperation)		
Criminalising Conduct	**Procedural Tools**	**International Cooperation**
• Illegal Access • Illegal Interception • Data Interference • System Interference • Misuse of devices • Fraud and Forgery • Child Pornography • IPR - offences	• Expedited Preservation • Search and Seizure • Interception of Computer Data	• Extradition • MLA • Spontaneous Information • Expediated Preservation • MLA for accessing computer data • MLA for interception • 24/7 points of contact

साइबर अपराध सम्बन्धी राष्ट्रिय कानूनहरू बीच तालमेल मिलाउने, साइबर अपराध अनुसन्धान प्रविधिमा सुधार र अन्तर्राष्ट्रिय सहयोग अभिवृद्धि गरी कम्प्युटर सम्बन्धी अपराध कम गर्ने उद्देश्यले गरिएको यो पहिलो अन्तर्राष्ट्रिय सम्झौता हो। यो convention 2001 AD मा हस्ताक्षरका लागि खोलिएको थियो र 2004 AD मा लागू भएको थियो ।यो फ्रान्सको स्ट्रासबर्गमा काउन्सिल अफ युरोपका पर्यवेक्षक राज्यहरू क्यानडा, जापान, फिलिपिन्स, दक्षिण अफ्रिका र संयुक्त राज्य अमेरिकाको सक्रिय सहभागितामा बनाइएको थियो। यस convention लाई हाल सम्म ६६ वटा विभिन्न राष्ट्रहरूले अनुमोदन गरेका छन्।

ख) African Union Convention

अफ्रिकी सङ्घ (AU), अफ्रिकी एकता सङ्गठनलाई प्रतिस्थापन गर्न २००२ मा गठन गरिएको थियो जुन विभिन्न ५५ वटा अफ्रिकी राज्यहरू मिलेर बनेको छ। यसको मुख्य उद्देश्यहरूमा शान्ति र सुरक्षा स्थापना, र अफ्रिकी महाद्वीपमा विकास र सामाजिक-आर्थिक एकीकरणलाई प्रोत्साहन दिनु रहेको छ। अफ्रिकामा इलेक्ट्रोनिक लेनदेन, व्यक्तिगत डेटाको संरक्षण, साइबर सुरक्षाको प्रवर्द्धन, ईलोक्ट्रोनिक-शासन र साइबर अपराध विरुद्ध लड्न साइबर सुरक्षाको लागि एक विश्वसनीय ढाँचा स्थापना गर्न साइबर सुरक्षा र व्यक्तिगत डाटा संरक्षणमा African Union Convention 2011 मा मस्यौदा गरिएको थियो। June 2014 मा यस Convention लाई AU ले अपनाएको थियो जसलाई ५५ AU सदस्यहरू मध्ये ५ (घाना, गिनी, मौरिसस, नामिबिया र सेनेगल) ले मात्र अनुमोदन गरेका थिए भने १४ देशहरूले यसमा हस्ताक्षर गरेका थिए तर अनुमोदन गरेका थिएनन्।
यस महासन्धिले तीन मुख्य क्षेत्रहरूलाई सम्बोधन गर्दछ:

(१) इलेक्ट्रोनिक लेनदेन, (२) व्यक्तिगत डाटा सुरक्षा, (३) साइबर सुरक्षा र साइबर अपराध।

ग) UN Cyber Crime Convention

जुलाई २७, २०२१ मा रसियन फेडेरेसनले "Countering the use of Information and Communication Technologies for the Criminal Purposes" नाम रहेको अभिसन्धिलाई संयुक्त राष्ट्रसङ्घको तदर्थ समिति (Ad Hoc Committee) समक्ष पेश गरेको थियो। यो मस्यौदा संयुक्त राष्ट्रसङ्घका अन्य अभिसन्धिहरू (जस्तैः UN Conventions against Transnational Organized Crime and UN Convention against Corruption) and regional instruments, including Convention on Cybercrime of the Council of Europe (the Budapest Convention) मा आधारित रही तर्जुमा गरिएको दाबी गरिएको छ। यसरी प्राप्त मस्यौदामा तदर्थ समितिले आफ्नो ७८औँ अधिवेशन (१२-३० सेप्टेम्बर २०२३) मा महासभासमक्ष मस्यौदा पेश गर्न कम्तीमा ६ (छ) वटा अधिवेशन बोलाएर आफ्नो काम सम्पन्न गर्नेछ।

यस अभिसन्धिमा नेपाल सरकारबाट समेत आवश्यक राय प्राप्त गर्न नेपाल स्थित रुसी राजदूतावासले परराष्ट्र मन्त्रालय मार्फत गृह मन्त्रालय उक्त दस्तावेज पठाइएको थियो ।

घ) Digital Geneva Convention

फेब्रुअरी १४, २०१७ मा Microsoft का सभापति Brad Smith ले RSA (Rivest, Shamir, and Adleman) Conference अन्तर्गत यस अभिसन्धिको आवश्यकता रहेको भनी उल्लेख गरेको पाइन्छ । Brad Smith का अनुसार जसरी चौथो जेनेभा महासन्धिले लामो समयदेखि युद्धको समयमा नागरिकहरूलाई सुरक्षित राखेको छ, हामीलाई अब एउटा डिजिटल जेनेभा कन्भेन्सन चाहिन्छ जसले राष्ट्र-राज्य साइबर आक्रमणहरू (nation-state attacks) का बेला आम नागरिकहरूलाई जोगाउन सरकारहरूलाई प्रतिबद्ध गर्नेछ भनि व्यख्या गरिएको थियो ।

ङ) The Tallinn Manual

यो Manual कानूनका विद्वानहरूको अन्तर्राष्ट्रिय समूहद्वारा The NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) को अनुरोधमा विकास गरिएको थियो, जुन इस्टोनिया देशको टालिनमा अवस्थित छ ।

- मार्च, २०१३ मा ट्यालिन म्यानुअलको प्रथम संस्करण प्रकाशित भएको थियो । जसले साइबर युद्धमा अन्तर्राष्ट्रिय कानूनको प्रयोगको विश्लेषण गर्ने पहिलो व्यापक र आधिकारिक प्रयास गरेको थियो।
- यसै गरी The Tallinn Manual 2.0, फेब्रुअरी, २०१७ मा जारी गरिएको थियो। Tallinn 2.0 ले सशस्त्र आक्रमणको समयमा गौण रहने द्वेषपूर्ण साइबर अपरेशनहरूमा कसरी अन्तर्राष्ट्रिय कानुनी सिद्धान्तहरू लागू गर्न सकिन्छ भनेर मूल्याङ्कन गर्ने दायरा फराकिलो बनाएको थियो।
- यसका साथै Tallinn Manual 3.0 विकास हुने क्रममा रहेको छ जसले २०१७ को संस्करणको Tallinn Manual २.० लाई परिमार्जन र विस्तार गर्नेछ।

यसरी Tallinn Manuals ले एक दशकको देखि नीतिज्ञ र कानुनीविद्हरूका लागि कसरी अन्तर्राष्ट्रिय कानून साइबर अपरेशनहरूमा लागू हुन्छ भन्ने विषयमा एक आवश्यक उपकरणको रूपमा सेवा दिइरहेको छ ।

च) General Data Protection Regulation (GDPR)

GDPR युरोपेली सङ्घ (EU) मा डाटा गोपनीयता कानूनहरू अद्यावधिक र एकीकृत गर्ने कानून हो । GDPR अप्रिल १४, २०१६ मा युरोपेली संसदले अनुमोदन गरेको थियो र मे २५, २०१८ मा लागू भएको थियो। यसको मुख्य उद्देश्य हरेक व्यक्तिहरूको जीवन, कार्यक्षेत्र र घटनाक्रमसँग सम्बन्धित विभिन्न डाटाहरूको सुरक्षा गर्नु हो।

साथै उक्त डाटा सङ्कलन गर्ने संस्थालाई समेत जिम्मेवार बनाई सुरक्षित डाटा सङ्कलन गर्न सुनिशचित गर्नु समेत हो। यसरी GDPR ले व्यक्तिगत डाटाहरू सुरक्षित रूपमा राख्न समेत सम्बन्धित संस्थालाई मार्गनिर्देश गर्दछ र यस नियमनले व्यक्तिगत डाटालाई "अनधिकृत वा गैरकानूनी प्रशोधन, र आकस्मिक हानि, विनाश वा क्षति विरुद्ध" सुरक्षित राख्नु पर्दछ भन्ने कुरामा विभिन्न सूचना प्रणाली प्रयोग गरी डाटा सङ्कलन हरेक संस्थालाई जिम्मेवार बनाँउदछ।

छ) अन्य

- Southern African Development Community Model Laws on Cybercrime
- Paris Call for Trust & Security in Cyberspace
- UNGGE Consensus Report of 2015
- Cybersecurity Tech Accord
- Siemens Charter of Trust
- GCSC Six Critical Norms
- Freedom Online Coalition Recommendations for Human Rights Based Approaches to Cybersecurity
- Shanghai Cooperation Organization Agreement on Cooperation in the Field of Ensuring the International Information Security
- Mutual Agreed Norms for Routing Security (MANRS)
- Brazzaville Declaration
- EU Cybersecurity Act
- EU NIS Directive
- Draft EAC Framework for Cyber Laws
- NATO Cyber Defense Pledge
- EU Joint Communication: Resilience, Deterrence and Defense
- CSDE Anti-botnet Guide

४.२. साइबर सुरक्षा अनुपालन कार्यढाँचाहरू

विभिन्न संस्थाहरूले विभिन्न सेवाहरू प्रविधिको प्रयोग गरी आफ्नो ग्राहकहरूलाई उपलब्ध गराएका हुन्छन्। सोही सेवाहरूको प्रयोगबाट सेवाग्राहीले आफ्नो जानकारीहरू मार्फत उक्त सेवाहरू लिएका हुन्छन् । उक्त व्यक्तिगत जानकारी अरु कसैको पहुँचमा पुग्नु हुन्न। त्यस्तै अन्य कुनै कारणले ग्राहकलाई दिएको सेवाहरू समयमै उपलब्ध हुनु पर्ने हुन्छ। यस्ता विभिन्न कुराहरूको प्रयोग र यसलाई ह्याकरबाट सुरक्षित बनाउनको निम्ति विभिन्न संस्थाहरूले केही कम्प्लयान्स अनुसार सेवाहरू दिन पूर्वाधार तथा प्रक्रियाहरूको व्यवस्था पनि गर्नु पर्ने हुन्छ। जस मध्य केही Cybersecurity Compliance Framework निम्न रहेका छन्:-

१. NIST (National Institute of Standards and Technology) Cybersecurity Framework: यस फ्रेमवर्कले साधरणतया डाटाहरूको सुरक्षा कसरी गर्ने भन्ने कार्य निर्देश गरेको छ। यस फ्रेमवर्कमा डाटा भण्डारण तथा डाटा ट्रान्जिटमा सुरक्षा गर्न के कस्ता नियमको पालना गर्ने विषय उल्लेख गरिएको छ।

२. SOC2 Framework: यो फ्रेमवर्क वित्तीय संस्थाहरूले आफ्नो ग्राहकहरूको सुरक्षित डाटा व्यवस्थापन भए नभएको यकिन गराउने Auditing Standard हो ।

३. HIPPA Framework: यो फ्रेमवर्क साधारणतया स्वास्थ्य क्षेत्रतर्फ रहेको व्यक्तिगत स्वास्थ्य सम्बन्धी डाटाको सुरक्षा तथा गोपनीयताको बारे यकिन गराउने फ्रेमवर्क हो।

४. ISO 22301: विभिन्न निकायहरूले दिइने सेवाहरूको बिना अवरोध सेवा प्रवाहलाई निरन्तरता दिन यस फ्रेमवर्कको सहयोग लिन सकिन्छ।

५. ISO 27001, ISO 27002 Certification: विभिन्न सङ्घ संस्थाहरूद्वारा आफ्नो काम गर्ने विधि सुरक्षित रहेको यकिन गराउनको लागि संस्थाहरूलाई विभिन्न सुरक्षाका तहहरूमा विभाजन गरिएको हुन्छ जसलाई CCMMI (Cybersecurity Capibility Maturity Model Integration) भनिन्छ। सुरक्षाका माथिल्लो तह प्राप्त गर्न ISO 27001, ISO 27002 Certification लिने गरिन्छ।

माथि उल्लेखित विभिन्न फ्रेमवर्क, अनुपालन संयन्त्रहरू लगायतका विभिन्न फ्रेमवर्कहरूको प्रयोग अन्ताराष्ट्रिय स्तरमा गर्ने गरिएको छ। विभिन्न सन्धि तथा सम्झौताहरू लगायत विभिन्न अनुपालन संयन्त्रहरूलाई पनि मध्यनजर गरी प्रयोगमा ल्याउन जरुरी हुन्छ। जस्तै:-

- स्वास्थ्य क्षेत्र : Health Insurance Portability and Accountability Act (HIPAA).
- आर्थिक क्षेत्र : PCI-DSS, ISO/IEC 27001, SOX, GLBA, FINRA, PSD 2.

४.३. नीतिगत व्यवस्थाहरू

हालसम्म साइवर सुरक्षासँग सम्बन्धित सम्बन्धित निम्नानुसारको ऐन, नीति, नियमावली, निर्देशिका एवं कार्यविधि रहेका छन् ।

- विद्युतीय कारोबार ऐन, २०६३
- विद्युतीय कारोबार नियमावली, २०६४
    - विद्युतीय कारोबार ऐन, २०६३ र विद्युतीय कारोबार नियमावली, २०६४ मा विद्युतीय तथ्याङ्क आदान–प्रदानको माध्यमबाट वा अन्य कुनै विद्युतीय सञ्चार माध्यमबाट हुने कारोबारलाई भरपर्दो र सुरक्षित बनाई विद्युतीय अभिलेखको सिर्जना, उत्पादन, प्रशोधन, सञ्चय, प्रवाह तथा सम्प्रेषण प्रणालीको मान्यता, सत्यता, अखण्डता र विश्वसनीयतालाई प्रमाणीकरण तथा नियमित गर्ने व्यवस्था गर्न र विद्युतीय अभिलेखलाई अनधिकृत तवरबाट प्रयोग गर्न वा त्यस्तो अभिलेखमा गैरकानूनी तवरबाट परिवर्तन गर्ने कार्यलाई नियन्त्रण गर्ने; डिजिटल हस्ताक्षरको सिर्जना र सुरक्षण, नियन्त्रक तथा प्रमाणीकरण गर्ने निकाय, परीक्षक तथा कार्य सम्पादन परीक्षण, डिजिटल हस्ताक्षर तथा प्रमाणपत्र सम्बन्धी व्यवस्थाको बारेमा उल्लेख गरिएको छ ।

विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ (प्रमाणीकरण र प्रकाशन मिति २०६३/८/२२) परिच्छेद ९: कम्प्युटर सम्बन्धी कसूर
४४. कम्प्युटर स्रोत सङ्केतको चोरी, नष्ट वा परिवर्तन गरेमा तीन वर्षसम्म कैद वा दुई लाख रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ ।
४५. कम्प्युटर सामग्रीमा अनधिकृत पहुँच : दुई लाख रुपैयाँसम्म जरिबाना वा तीन वर्षसम्म कैद वा दुवै सजाय हुनेछ ।
४६. कम्प्युटर र सूचना प्रणालीमा क्षति पुर्याउने : दुई लाख रुपैयाँसम्म जरिबाना वा तीन वर्षसम्म कैद वा दुवै सजाय हुनेछ।
४७. विद्युतीय स्वरूपमा गैरकानूनी कुरा प्रकाशन गर्ने : एक लाख रुपैयाँसम्म जरिबाना वा पाँच वर्षसम्म कैद वा दुवै सजाय हुनेछ ।
४८. गोपनीयता भङ्ग गर्ने : एक लाख रुपैयाँसम्म जरिबाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।
४९. झुट्टा व्यहोराको सूचना दिने : एक लाख रुपैयाँसम्म जरिबाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

५०. झुट्टा इजाजतपत्र वा प्रमाणपत्र पेश गर्ने वा देखाउने एक लाख रुपैयाँसम्म जरिबाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

५२. कम्प्युटर जालसाजी गर्ने : एक लाख रुपैयाँसम्म जरिबाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

५३. कम्प्युटर सम्बन्धी कसूर गर्न दुरुत्साहन : पचास हजार रुपैयाँसम्म जरिबाना वा छ महिनासम्म कैद वा दुवै सजाय हुनेछ।

- सूचना तथा सञ्चार प्रविधि नीति, २०७२
    - विद्युतीय व्यापार (e-Commerce), विद्युतीय सरकार (e- Government) मा जोड, इन्टरनेट सेवा सहितका सूचना केन्द्रको विस्तार गर्ने, ग्रामीण दूर सञ्चार विकास कोष परिचालन, e-School, e-learning, e-education मा जोड, Software & Services Promotion Board को स्थापना गर्ने, (Payment Infrastructure Services) हरूको स्थापना, टेलिमेडिसिन योजना तर्जुमा, स्मार्ट सिटी (smart city) को अवधारणा अघि सारिएको।
- सूचना प्रविधि आकस्मिक सहायता समूह (सञ्चालन तथा व्यवस्थापन) निर्देशिका, २०७५
    - सूचना प्रविधिको विकास तथा बढ्दो प्रयोग सँगै देखिएको साइबर सुरक्षा जोखिमको पहिचान, त्यसबाट हुने असरको न्यूनीकरण र आकस्मिक साइबर सुरक्षाको व्यवस्था गर्न उपयुक्त संयन्त्र गठन, सञ्चालन तथा व्यस्थापन सम्बन्धमा व्यवस्था गरिएको।
- अनलाइन बालसुरक्षा निर्देशिका, २०७६
    - सूचना तथा सञ्चार प्रविधिको विकाससँगै अनलाइन माध्यममा बालबालिकामाथि बढ्दो दुर्व्यवहारका घटनालाई सरोकारवालाहरूको संयुक्त पहलबाट न्यूनीकरण गर्न तथा बालबालिकाको लागि इन्टरनेटको सुरक्षित प्रयोगको लागि दूरसञ्चार ऐन, २०५३ को दफा १३ बमोजिम यो निर्देशिका बनाइएको हो। सेवा प्रदायकले गर्नुपर्ने कार्य (गैरकानुनी तथा हानिकारक सामग्रीको उपलब्धता न्यूनीकरण, बाल दुर्व्यवहारजन्य सामग्री तुरुन्त हटाउने, त्यस्ता सामग्री वा लिङ्क उजुरी गर्ने संरचना विकास, सेवा प्रदायकले उपलब्ध गराएको सेवा तथा सामग्रीमा उमेर समूह स्पष्ट अवगत हुने व्यवस्था सम्बन्धी), घरपरिवार तथा समाजले गर्नुपर्ने कार्य (कम्प्युटरको सुरक्षित प्रयोग, कम्प्युटरको सुरक्षित प्रयोग सम्बन्धमा अभिमुखीकरण गर्ने, बालबालिकाले प्रयोग गर्ने वेबसाइट तथा एप्सको जानकारी राख्ने, विद्यालयको कम्प्युटरमा इन्टरनेटको सुरक्षित प्रयोग गर्नुपर्ने, सरोकारवाला संस्थाहरूको दायित्व सम्बन्धी), तथा नेपाल दूरसञ्चार प्राधिकरणले गर्ने कार्य सम्बन्धमा उल्लेख गरिएको छ ।
- साइबर सुरक्षा विनियमावली, २०७७ (Cyber Security Byelaw, 2077)

- नेपाल दुरसञ्चार प्राधिकरणले लागू गरेको 'साइबर सुरक्षा विनियमावली, २०७७' मा सञ्चार प्रविधिका पूर्वाधार लगायत सूचना प्रणालीलाई विभिन्न प्रकारका साइबर आक्रमणबाट जोगाउन प्राधिकरणबाट अनुमतिपत्र प्राप्त सबै दूरसञ्चार सेवा प्रदायकहरू (आधारभूत दूरसञ्चार, टेलिफोन, मोबाइल, नेटवर्क, इन्टरनेट लगायत) ले अन्तर्राष्ट्रिय रूपमा प्रचलित मापदण्ड तथा अभ्यास अनुसार सुरक्षाका विषयमा गर्नुपर्ने कार्यहरू, सेवाप्रदायकले गोप्य राख्नुपर्ने ग्राहकका सूचना, प्रयोग गर्नुपर्ने सफ्टवेयर तथा सबै सिष्टमहरू लगायत सेवाप्रदायकले आइपि अडिट गरी तीन देखि ६ महिनामा प्राधिकरणमा बुझाउनुपर्ने, बुझाइएको लेखापरीक्षण प्रतिवेदनमा प्राधिकरणले क्रस चेक समेत गर्न सक्ने व्यवस्था सम्बन्धमा उल्लेख गरिएको छ।

- Government Enterprises Architecture 2.0
    - यसको उद्देश्य सुरक्षा व्यवस्थापनको लागि देशव्यापी रूपरेखा स्थापना गर्नु हो। यसले कसरी सुरक्षा प्रक्रियाहरू र नियन्त्रणहरू तथा तिनीहरूले सङ्गठनको समग्र प्रणाली कसरी सम्बन्धित छन् भनेर वर्णन गर्दछ। यी प्रक्रियाहरू र नियन्त्रणहरूले सूचना सुरक्षाको सीआईए ट्राइड गोपनीयता, इन्टेग्रीटि र उपलब्धता जस्ता प्रणालीको गुणस्तरका विशेषताहरू कायम राख्ने उद्देश्यका लागि कार्यढाँचा प्रदान गर्छ। यसले सूचना र सम्पत्तिहरूको पहिचान, र सुरक्षाका लागि नीतिहरू, मापदण्डहरू, प्रक्रियाहरू र दिशानिर्देशहरूको विकास, दस्तावेजीकरण र कार्यान्वयन समावेश गर्दछ, र सूचना सुरक्षा सम्बन्धी आवश्यक स्रोतहरू वर्णन गर्दछ।

- सुरक्षित पासवर्ड सम्बन्धी अभ्यासहरू, २०६७
    - सुरक्षित पासवर्ड प्रयोगका अभ्यासहरू सम्बन्धी, जस्तैः १२३४५६, ०००० , २४६८ तथा डब्लु एक्स वाइ जेड जस्ता कमजोर तथा सबैले अनुमान गर्न सक्ने खालका पासवर्ड प्रयोग नगर्ने; आफ्ना श्रीमती, बच्चाबच्ची, अपार्टमेन्ट, मनपर्ने खेल वा क्लब, आफ्नो अफिसको नाम जस्ता कुराहरू पनि पासवर्डमा नराख्ने; एक दुई अक्षर अपरकेस अर्थात् क्यापिटल लेटरमा राखी लामो तथा स्पेसल क्यारेक्टरवाला सुरक्षित पासवर्डको प्रयोग गर्नुपर्ने उल्लेख गरिएको ।
- सम्बन्धित अन्य
    - मुलुकी देवानी संहिता ऐन, २०७४ र मुलुकी अपराध संहिता ऐन, २०७४

भाग-१ परिच्छेद–३ दफा २१. गोपनीयताको अधिकार अतिक्रमण गरिएको मानिनेमा ख. कसैको चिठ्ठीपत्र खोलेमा वा त्यसको प्रयोग गरेमा, टेलिफोन वा अन्य प्रविधिको माध्यमबाट लिएको कुराकानी, बोली, ध्वनिको टेप वा रेकर्डिङ गरेमा वा सारेमा, घ) कसैको आकृति वा तस्वीर खिचेमा, ङ. अरूको नाम, आकृति, तस्वीर वा आवाजको नक्कल गरी सार्वजनिक गरेमा।

- बैङ्किग कसूर तथा सजाय ऐन, २०६४
    - परिच्छेद–२ को दफा ६: विद्युतीय माध्यमको दुरुपयोग वा अनधिकृत प्रयोग गरी भुक्तानी लिन वा दिन नहुने। कसैले पनि क्रेडिट कार्ड, डेबिट कार्ड, अटोमेटेड टेलर मेशिन (एटीएम) कार्ड वा अन्य विद्युतीय माध्यमको दुरुपयोग वा अनधिकृत प्रयोग गरी भुक्तानी लिन वा दिन हुँदैन ।

- केही सार्वजनिक (अपराध र सजाय) ऐन, २०२७
- पेटेण्ट डिजायन र ट्रेडमार्क ऐन, २०२२
- प्रतिलिपि अधिकार ऐन, २०५९
    - अनाधिकार प्रतिलिपिहरूको पैठारीमा प्रतिबन्ध:
      सजाय: प्रतिलिपिहरू जफत गरी निजलाई कसूरको मात्रा अनुसार दश हजार रुपैँयादेखि एक लाख रुपैयाँसम्म जरिवाना हुनेछ र प्रतिलिपि अधिकार प्राप्त व्यक्तिलाई त्यस्तो पैठारीबाट भएको नोक्सानीको क्षतिपूर्ति समेत सो पैठारी गर्ने व्यक्तिबाट भराइदिनु पर्नेछ।
    - रचयिता वा प्रतिलिपि अधिकार धनीको अनुमति प्राप्त नगरी, अर्काको रचनाको स्वरूप वा भाषाको माध्यम परिवर्तन, अनधिकृत पुनरुत्पादन गर्न हतोत्साहित गर्न आदि।
      सजाय: दश हजार रुपैयाँदेखि एक लाख रुपैयाँसम्म जरिवाना वा छ महिनासम्म कैद वा दुवै सजाय हुनेछ र दोस्रो पटकदेखि पटकैपिच्छे बीस हजार रुपैया देखि दुई लाख रुपैयाँसम्म जरिवाना वा एक वर्षसम्म कैद वा दुवै सजाय हुनेछ । त्यसरी प्रकाशन वा पुनरुत्पादन गरेको वा वितरण गरेको वा पुनरुत्पादन गर्न प्रयोग गरिएका सामग्रीहरू जफत हुनेछ । संरक्षित अधिकारको उल्लंघन गर्ने व्यक्तिबाट प्रतिलिपि अधिकार प्राप्त व्यक्तिलाई परेको नोक्सानीको क्षतिपूर्ति समेत भराइदिनु पर्नेछ ।

- उपभोक्ता संरक्षण ऐन, २०७५
    - सूचना चहाउनेलाई कारबाही- निरीक्षण वा अनगुमन नहुँदै चुहावट गर्न - बिगो खुलेकोमा बिगो बमोजिम र बिगो नखुलेकोमा पचास हजारदेखि एक लाख रुपैयाँसम्म जरिवाना गर्नेछ र त्यस्तो संस्थालाई कालो सूचीमा समावेश गर्ने।
    - झुठ्ठा वा भ्रमपूर्ण विज्ञापन गर्ने वा भ्रमपूर्ण विज्ञापन गरेमा - दुई वर्षदेखि पाँच वर्षसम्म कैद वा चार लाखदेखि छ लाख रुपैयाँसम्म जरिवाना वा दुवै सजाय।

- सरकारी कार्यालयको वेबसाईट निर्माण तथा व्यवस्थापन सम्वन्धी निर्देशिका, २०७८
    - वेवसाइटमा राखिने विषय वस्तुहरू सम्बन्धी, वेवसाइटको निर्माण तथा प्रकाशन सम्बन्धी, प्रचार प्रसार सम्बन्धी, मुल्याङ्कन सम्बन्धी।
- सरकारी निकायमा विद्युतीय पत्राचार (इमेल) व्यवस्थापन सम्बन्धी निर्देशिका, २०७५
    - सरकारी एकीकृत इमेल प्रणाली प्रयोग गर्नुपर्ने, व्यक्तिगत इमेल खाता सम्बन्धी व्यवस्था, पद अनुसारको इमेल खाताको सम्बन्धी व्यवस्था, विद्युतीय माध्यमबाट पत्राचार गर्नुपर्ने, विद्युतीय हस्ताक्षरको प्रयोग गर्नुपर्ने सम्बन्धी व्यवस्था।
- सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका, २०७१
    - विद्युतीय माध्यमबाट सरकारी कार्यालय सञ्चालन तथा सेवा प्रवाह गर्न आवश्यक सूचना प्रविधि प्रणालीको संरचनामा एकरूपता कायम गर्न, त्यस्ता सूचना प्रविधि प्रणालीहरूको अन्तर-सञ्चालन हुने व्यवस्था।
- नागरिक एप (सञ्चालन तथा व्यवस्थापन) निर्देशिका, २०७८
    - सार्वजनिक निकायमा रहेका विद्युतीय सूचना प्रणालीबीच अन्तर आवद्धता कायम गरी नागरिकलाई छिटो, छरितो, मितव्ययी र प्रभावकारी रूपमा एउटै विद्युतीय प्रणालीबाट सेवा र सूचना प्रवाहको व्यवस्था गर्न निर्मित नागरिक एपको सञ्चालन तथा व्यवस्थापन सम्बन्धमा।
- सरकारी निकायका मोवाइल एपहरूको मापदण्ड, २०७५
    - अङ्ग्रेजी र नेपाली दुवै भाषामा हुनुपर्ने तथा एपमा हुनु पर्ने विभिन्न सुविधा तथा विशेषताहरूको व्याख्या गरिएको।

- निर्माणको चरणमा रहेको
    - सङ्घीय संसदमा दर्ता भई प्रक्रियामा रहेको सूचना प्रविधि विधेयक, २०७४ (मस्यौदा) (IT ACT, 2074 (Draft))
        - विद्युतीय अभिलेखको मान्यता, डिजिटल हस्ताक्षर, विद्युतीय अभिलेख सम्प्रेषण, प्राप्ति तथा स्वीकार सम्बन्धी व्यवस्था, विद्युतीय शासन, सूचना प्रविधि सम्बन्धी व्यवसाय, सूचना सुरक्षा सम्बन्धी व्यवस्था, साइबर सुरक्षा सम्बन्धी व्यवस्था, कसूर तथा सजाय, सूचना प्रविधि न्यायाधीकरण सम्बन्धी व्यवस्था सम्बन्धमा उल्लेख गरिएको।

- राष्ट्रिय साइवर सुरक्षा नीति, २०७८ को मस्यौदा (National Cyber Security Policy, 2021) स्वीकृतिका लागि मन्त्रिपिरषदमा पेश हुने क्रममा रहेको ।

मुख्यतः विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ को प्रावधान बमोजिम साइबर सुरक्षा तथा अपराधका विषयहरू नियमन तथा नियन्त्रण भइरहेका छन् । प्रविधिको रूपान्तरणसँगै सूचना प्रविधि क्षेत्रमा आएको परिवर्तनसँगै साइबर सुरक्षासँग सम्बन्धित नीतिगत, कानुनी तथा संस्थागत व्यवस्थाहरू समयानुकुल परिमार्जन तथा सुदृढ हुन सकेको देखिदैन। यद्यपि साइबर सुरक्षाको क्षेत्रमा सुधारका विविध प्रयासहरू भइरहेका छन्। सञ्चार तथा सूचना प्रविधि मन्त्रालय अन्तर्गत सूचना प्रविधि आकस्मिक सहायता समूह (सञ्चालन तथा व्यवस्थापन) निर्देशिका, २०७५ बमोजिम गठन भएको राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह (NITERT) ले समय समयमा साइबर सुरक्षासँग सम्बन्धित एडभाइजरी जारी गर्ने गरेको छ। साइबर सुरक्षा क्षेत्रसँग सम्बन्धित विभिन्न निकायहरूले साइबर सुरक्षा सम्बन्धी निकायगत नीति निर्देशिका अनुसार काम गर्दै आइरहेको देखिन्छ।

हाल व्यवस्थापिका संसदमा विचाराधीन रहेको सूचना प्रविधि विधेयकको प्रस्तावना र परिच्छेद १२ मा साइबर सुरक्षा सम्बन्धी व्यवस्था गरेको पाइन्छ । प्रस्तावित यस विधेयकले साइबर अपराध नियन्त्रण, साइबर सुरक्षा सुदृढीकरण, संस्थागत विकास लगायतका विषयहरू समेटेको छ । यसै गरी प्रस्तावित राष्ट्रिय साइबर सुरक्षा नीति, २०७८ ले साइबर जोखिमलाई सम्बोधन गर्दै व्यक्ति, व्यवसाय एवं सरकारका लागि भरपर्दो, सुरक्षित एवं लचिलो साइबर स्पेश निर्माण गर्ने दीर्घकालीन सोच राखेको छ ।

४.४. पूर्वाधार सम्बन्धी व्यवस्थाहरू

सूचना प्रविधिको विकाससँगै नेपालमा इन्टरनेट कनेक्टिभिटि, सामाजिक सञ्जालको प्रयोग, डिजिटल माध्यमबाट सार्वजनिक सेवाको प्रयोग, विद्युतीय माध्यमबाट डिजिटल कारोबार एवं भुक्तानी तथा बैंकिङ सेवाको प्रयोग व्यापक हुँदै गएको छ । धेरैजसो सरकारी, गैरसरकारी सङ्घसंस्था व्यापारिक प्रतिष्ठानहरूले इन्टरनेटमा उपस्थिति जनाइसकेका छन् भने आफ्नो सेवाहरू प्रदान गर्न डिजिटल प्रविधिको प्रयोग गर्दैछन् । सरकारीस्तरमा सार्वजनिक सेवाप्रवाहलाई डिजिटल माध्यमबाट प्रवाहमा जोड दिइएको पाइन्छ । नेपाल सरकार, प्रदेश सरकारहरू तथा स्थानीय निकायहरूले समेत विद्युतीय माध्यमबाट सेवा प्रवाह गरिरहेका छन् । सरकारी तथा निजी क्षेत्रले प्रयोग गर्ने प्रमुख साइबर पूर्वाधारको रूपमा इन्टरनेट सञ्चाल रहेको छ जुन नेपाल दूरसञ्चार प्राधिकरणले नियमन गर्ने गर्दछ । साइबर पूर्वाधारको रूपमा सरकारी निकायहरूले मूलतः राष्ट्रिय सूचना प्रविधि केन्द्रद्वारा सञ्चालित सरकारी एकीकृत डाटा सेन्टर तथा डिजास्टर रिकभरी सेन्टर एवं आ-आफ्नो संस्थागत डाटा सेन्टरको प्रयोग गरिरहेका छन् । बैंक तथा वित्तीय संस्था एवं अन्य व्यावसायिक क्षेत्रमा स्वेदशी एवं अन्तर्राष्ट्रिय पब्लिक क्लाउड तथा निजी डाटा सेन्टर प्रयोगमा रहेका छन् ।

नेपाल सरकारले सरकारी तथा निजी क्षेत्रका महत्वपूर्ण सूचना प्रणालीहरूको सञ्चालनको लागि साइबर पूर्वाधार विकास सम्बन्धी कानूनी व्यवस्था वा मापदण्डको एकीकृत व्यवस्था गरिसकेको अवस्था नभएकोले सबैजसो निकाय तथा संस्थाहरूले आ-आफ्नो क्षमता तथा विज्ञताको आधारमा पूर्वाधार व्यवस्थापन गरिरहेका छन् ।

सरकारी स्तरबाट साइबर सुरक्षा तथा पूर्वाधार व्यवस्थाको लागि सञ्चालनमा ल्याइएका मूख्य-मूख्य पुर्वाधार तथा संस्थागत संरचनाहरूको सूची देहायबमोजिम रहेको छः

- राष्ट्रिय सूचना प्रविधि केन्द्रद्वारा सञ्चालित Government Integrated Data Centre (GIDC) र Disaster Recovery Center,
- सूचना प्रविधि विभागबाट सञ्चालित Government Cloud (G-Cloud),
- सञ्चार तथा सूचना प्रविधि मन्त्रालयद्वारा सञ्चालित राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह Information Technology Emergency Response Team Nepal (NITERT),
- सञ्चार तथा सूचना प्रविधि मन्त्रालयमा रहेको राष्ट्रिय साइवर सुरक्षा अनुगमन केन्द्र,
- प्रमाणीकरण नियन्त्रकको कार्यालयमा रहेको साइवर फरेन्सिक ल्याव,
- विभिन्न सरकारी निकायहरूले सञ्चालन गरेका डाटा सेन्टरहरू,
- नेपाल प्रहरीमा स्थापित साइबर ब्यूरो र डिजिटल फोरेन्सिक ल्याब।

केही सङ्गठनहरूले आफ्नो server तथा डाटाको भण्डारण GIDC सर्भरको प्रयोग साथै सरकारी Cloud मा पनि राख्ने गरेको पाइन्छ । त्यस्तै, सङ्गठनहरूले आफ्नै सुरक्षित नेटवर्कको लागि Intranet प्रविधिको प्रयोग समेत गर्दै आएको पाइन्छ । आफ्नो आन्तरिक नेटवर्कलाई बाहिरी नेटवर्कबाट सुरक्षित बनाउन IPS तथा IDS ((Intrusion prevention and detection system) विशेषता रहेको firewall र manageable switch हरूको समेत प्रयोगलाई बढावा दिदै आएको पाइन्छ। केहि सङ्गठनहरूमा Central Enterprise Antivirus software को प्रयोग गरिरहेको पनि पाइन्छ।

तथापि सूचना प्रविधिसँग सम्बन्धित पूर्वाधारहरू विभिन्न निकायहरूले आ-आफनो किसिमले अध्ययन, विश्लेषण, आवश्यकता एवं औचित्य वेगर नै विकास गरिरहेको पाइएको छ । यसरी साइबर सुरक्षाको ख्यालै नगरी सूचना प्रविधि पूर्वाधारहरूको विकास हुँदै गर्दा साइबर सुरक्षाको विषय झन् झन् जटिल बन्दै गएको देखिन्छ। केही निकायहरूमा साइबर सुरक्षाका लागि आवश्यक पर्ने न्यूनत्तम पूर्वाधार (जस्तै: firewall) समेत राखिएको पाइदैन।

४.५. संस्थागत व्यवस्था

नेपाल सरकार कार्यविभाजन नियमावली, २०७४ ले साइबर सुरक्षा सञ्चार तथा सूचना प्रविधि मन्त्रालयको कार्यक्षेत्रमा राखेको छ । प्रस्तावित एवं सङ्घीय संसदमा विचाराधीन अवस्थामा रहेको सूचना प्रविधि विधेयकले साइबर सुरक्षा

विषय सञ्चार तथा सूचना प्रविधि मन्त्रालयको कार्यक्षेत्र भित्र पर्ने उल्लेख गरेको पाइन्छ। त्यसैगरी अपराध रोकथाम तथा नियन्त्रण सम्बन्धी नीति, कानून, मापदण्ड, नियमन; अपराध अनुसन्धान तथा अपराध नियन्त्रणसम्बन्धी अन्तराष्ट्रिय, क्षेत्रीय समन्वय तथा सहयोग गृह मन्त्रालयको कार्यक्षेत्रमा उल्लेख गरिएको छ भने राष्ट्रिय तथा रणनीतिक सुरक्षा सम्बन्धी सूचना सङ्कलन, विश्लेषण, सञ्चार प्रणाली एवं सञ्चालन र व्यवस्थापन रक्षा मन्त्रालयको कार्यक्षेत्रमा उल्लेख गरिएको छ। साइबर सुरक्षासँग सरोकार राख्ने देहायबमोजिमका निकायहरूबाट साइबर सुरक्षासँग सम्बन्धित कार्यहरू हुँदै आइरहेको छ।

१. सञ्चार तथा सूचना प्रविधि मन्त्रालय
    क) सूचना प्रविधि विभाग
    ख) प्रमाणीकरण नियन्त्रकको कार्यालय
    ग) नेपाल नेपाल दूरसञ्चार प्राधिकरण
    घ) राष्ट्रिय सूचना प्रविधि केन्द्र
    ङ) राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह
२. नेपाल प्रहरी (साइबर व्युरो र सूचना प्रविधि निर्देशनालय)
३. सशस्त्र प्रहरी बल, नेपाल
४. नेपाली सेना
५. राष्ट्रिय अनुसन्धान विभाग
६. विभिन्न मन्त्रालय तथा निकायहरू

साइबर सुरक्षाका मापदण्डहरू र उत्कृष्ट अन्तर्राष्ट्रिय अभ्यासहरू अवलम्बन गर्दै डिजिटल सेवामा इन्टरनेट प्रयोगकर्ताहरूको विश्वास कायम राख्न र ICT Infrastructure and Information System लाई विभिन्न खालका साइबर आक्रमणहरूबाट जोगाउन नेपाल दूरसञ्चार प्राधिकरणले लागु गरेको साइबर सुरक्षा विनियमावली, २०७७ ले दूरसञ्चार सेवा प्रदायकहरूलाई सेवा ग्राहकहरूको विवरण सुरक्षित राख्नुपर्ने, ३/३ महिनामा VAPT गराउने, वर्षमा दुई पटक अन्तरिक रूपमा Information System Audit गर्नुपर्ने र प्रत्येक आर्थिक वर्षमा एक पटक तेस्रो पक्षबाट Information System Audit गराउनुपर्ने र सो को प्रतिवेदन प्राधिकरणलाई उपलब्ध गराउनुपर्ने व्यवस्था गर्नुका साथै यस विनियमावलीले प्राधिकरणको बोर्डबाट नीतिगत निर्णय लिनुपर्ने विषयमा सिफारिस गर्न प्राधिकरणका अध्यक्षको अध्यक्षता रहने गरी एक सञ्चालक समितिको व्यवस्था गरेको छ।

साइबरका घटनाहरू (Cyber Incident) हुन नदिन र त्यस्ता घटना भएमा क्षति न्यूनीकरण गर्दै अध्ययन अनुसन्धान गर्न तथा दूरसञ्चार सेवा प्रदायकहरू लगायत सम्बन्धित निकायहरूसँग समन्वय गर्न यो विनियमावलीले प्राधिकरणको निर्देशकको संयोजकत्वमा ५ जनाको एक Cyber Security Task Force (NTA-CERT) को समेत व्यवस्था गरेको छ।

४.६. जनशक्तिको व्यवस्था

सूचना प्रविधि क्षेत्र दिनानुदिन बृहत एवं व्यापक हुँदै गर्दा चुनौतीहरू पनि बढ्दै गइरहेको परिप्रेक्ष्यमा नेपाल सरकारको विभिन्न निकायहरूमा रहेको सूचना प्रविधिसँग सम्बन्धित स्वीकृत दरबन्दी संरचना ज्यादै न्यून रहेको छ। हाल नेपाल सरकार मातहत सूचना प्रविधिसँग सम्बन्धित जनशक्तिको संरचना निम्नानुसार रहेको छ।

तालिका २: सूचना प्रविधिसँग सम्बन्धित जनशक्तिको संरचना

क्र.सं.	श्रेणी	पद	दरबन्दी
१.	रा.प.प्रथम श्रेणी	सूचना प्रविधि विज्ञ/महानिर्देशक/सहसचिव	३ (१: ९.७)
२.	रा.प.द्वितीय श्रेणी	सूचना प्रविधि निर्देशक/वरिष्ठ कम्प्यूटर इन्जिनियर/उपसचिव	२९ (१: १३.९)
३.	रा.प.तृतीय श्रेणी	कम्प्यूटर इन्जिनियर	४०२
		कम्प्यूटर अधिकृत/ सूचना प्रविधि अधिकृत	

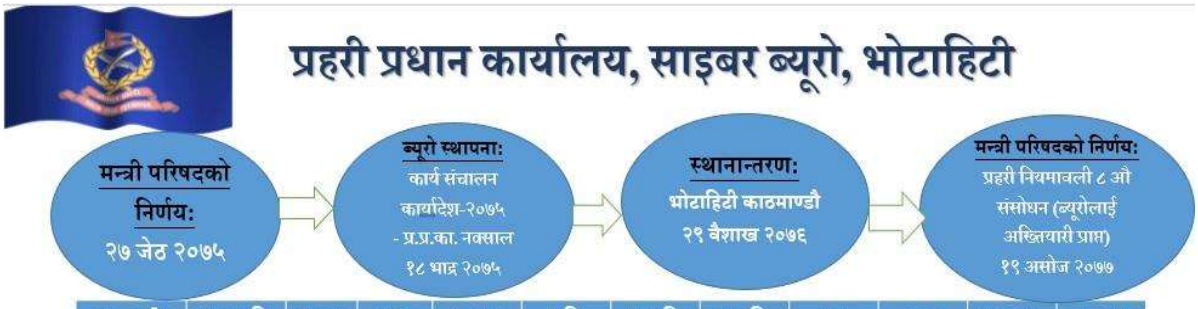
सञ्चार तथा सूचना प्रविधि मन्त्रालयको सूचना प्रविधि महाशाखा अन्तर्गत साइवर सुरक्षा शाखामा निम्नानुसार (तालिका ३)जनशक्ति रहेको छ।

तालिका ३: साइवर सुरक्षा शाखा, सञ्चार तथा सूचना प्रविधि मन्त्रालयको जनशक्ति अवस्था

क्र.सं.	पद	स्वीकृत दरबन्दी	पदपूर्ति
१	उप सचिव (प्रा.)	१	१
२	कम्प्युटर इन्जिनियर	२	२

सूचना प्रविधिसँग सम्बन्धित स्वीकृत दरबन्दी संरचना ज्यादै न्यून रहेकोमा उक्त दरबन्दी बमोजिमको जनशक्ति समेत पूर्णरूपमा पदपूर्ति नभएको अवस्था छ। उदाहरणका लागि साइबर ब्युरो जस्तो साइबर अपराध, साइबर सुरक्षा तथा सूचना प्रविधिको क्षेत्रमा महत्वपूर्ण कार्य गर्ने सङ्गठनमा प्राविधिक तर्फ ३७ र अप्राविधिक तर्फ ३३ दरबन्दी रहेकोमा हाल कार्यरत जनशक्ति प्राविधिक तर्फ १५ र अप्राविधिक तर्फ ६२ रहेको छ।

तालिका ४: साइबर ब्युरो – जनशक्ति अवस्था



दरबन्दी	प्रनामनि	प्रबउ	प्रउ	प्रनाउ	प्रनि	प्रनानि	प्रसनि	प्रह	प्रज	प्रकास	जम्मा
प्रशासन	१	-	१	१	३	३	५	७	७	२	३०
कानूनी परामर्श	-	-	-	१	१	१	-	-	-	-	३
प्राविधिक	-	१	१	२	५	८	८	६	६	-	३७
जम्मा	१	१	२	४	९	१२	१३	१३	१३	२	७०
कार्यरत	**प्रनामनि**	**प्रबउ**	**प्रउ**	**प्रनाउ**	**प्रनि**	**प्रनानि**	**प्रसनि**	**प्रह**	**प्रज**	**प्रकास**	**जम्मा**
प्रशासन	१	-	१	२	३	५	७	१४	२६	३	६२
प्राविधिक	-	१	१	२	२	५	३	१	-	-	१५

त्यसैगरी नेपाल दूरसञ्चार प्राधिकरणसँग हाल NTA-CERT को लागि छुटै कर्मचारी दरबन्दीको व्यवस्था नरहेको र प्राधिकरणको महाशाखा/शाखामा कार्यरत अधिकृतहरूले थप कार्यभारको रूपमा Cybersecurity सँग सम्बन्धित कार्य पनि गर्दै आएको छ।

सूचना प्रविधिसँग सम्बन्धित जनशक्ति नै न्यून रहेको अवस्थामा साइबर सुरक्षा जस्तो सूचना प्रविधिको विशिष्टीकृत क्षेत्रका लागि आवश्यक पर्ने विशिष्टीकृत जनशक्ति सरकारी संयन्त्रमा प्राय: नगण्य नै रहेको अवस्था छ। निकायहरूमा साइबर सुरक्षा सम्बन्धी विज्ञको अभाव र सबै निकायमा दक्ष जनशक्ति सहित साइबर सेलको अभाव रहेको छ भने हाल साइबर सुरक्षाको क्षेत्रमा काम गरिरहेका सूचना प्रविधिसँग सम्बन्धित जनशक्तिहरूलाई आवश्यक पर्ने क्षमता अभिवृद्धि कार्यक्रमहरू राष्ट्रियस्तरमा केही रहेपनि पर्याप्त छैन भने अन्तर्राष्ट्रियस्तरको जनशक्ति आपूर्तिको अवस्था प्राय: शून्य बराबर छ।

परिच्छेद ५ - समस्या तथा चुनौती

५.१. समस्याहरू

सूचना प्रविधि क्षेत्रसँग सम्बन्धित विभिन्न किसिमका समस्याहरू रहेका छन् जसलाई निम्नानुसार उल्लेख गर्न सकिछः

- राष्ट्रिय साइबर सुरक्षा कमजोर हुनुमा सूचना प्रविधि र साइबर सुरक्षा सम्बन्धी आवश्यक नीति तथा कार्ययोजनाको अभाव; समयानुसार परिमार्जनको अभाव,
- विद्यमान विद्युतीय कारोबार ऐन २०६३ ले सीमापार अपराध लगायतका पछिल्ला साइबर सुरक्षाका चुनौतीहरू सम्वोधन गर्न नसकेको।
- विभिन्न संस्थाहरूले डिजिटल प्लेटफर्मको प्रयोग गरी सेवा दिने गरेको तर त्यस्तो सेवा दिँदा साइबर सुरक्षामा चाहिने निम्न स्तरको अनुपालन संयन्त्र (compliance mechanism) पनि कायम गरेको नदेखिएको।
- सूचना प्रविधि क्षेत्र तथा साइबर सुरक्षामा पर्याप्त लगानी हुन नसकेकाले मुलुकमा साइबर सुरक्षाका चुनौती सम्बोधन गर्न कठिन भएको।
- आन्तरिक एवं वाह्य सुरक्षा जोखिमलाई कम गर्न उचित संयन्त्रको अभाव।
- एकीकृत समन्वयात्मक निकायको अभाव; अन्तर निकाय समन्वय सहकार्य एवं सूचना आदान प्रदान कार्यको अभाव।
- साइबर सुरक्षासँग सम्बन्धित कार्यको अनुगमन गर्न संरचनागतरूपमा निकाय/संयन्त्रलाई सशक्त बनाउन नसकिएको।
- सूचना प्रविधिको प्रयोग गरेर हुन अपराधको न्यायिक निरूपण गर्न ट्राइब्यूनल अझैसम्म पनि गठन हुन नसकेको।
- सीमापार साइबर अपराधलाई कानूनी दायरामा ल्याउन द्विपक्षीय कानूनी सहयोग सन्धि/सम्झौताहरू हुन नसकेको।
- नेपाल बाहिरबाट सञ्चालन हुने सामाजिक नेटवर्किङ्ग साइटहरू, मोबाइल एप्लिकेशन, इमेल सेवा प्रदायक लगायतका विद्युतीय प्लेटफर्मका आधिकारिक निकायसँग द्विपक्षीय सम्झौता नभएकोले त्यस्ता माध्यमबाट हुने अपराध नियन्त्रणमा समस्या देखिएको।
- इन्टरनेट सेवा प्रदायक (Internet Service Provider -ISP) जस्तैः MAC Address/IMEI of the device needed for Internet Browsing, IP Address that is being used, Social Networking Sites Log, Mobile App Logs आदि उपलब्ध नगराउँदा अपराध अनुसन्धानमा कठिनाइ हुने गरेको। ISPs ले Network Address Translation (NAT) को Log Content नराख्नु।

- नेपालमा रहेका केही इन्टरनेट सेवा प्रदायक संस्थाहरूले डाटाहरूलाई उचित रूपमा भण्डारण गर्न नसक्नु वा त्यस्ता प्रविधिहरूको प्रयोग नगर्नु ।
- नियमित सुरक्षा परीक्षण नहुनु। सरकारी निकायहरूका अनलाइन प्रणालीको नियमित सुरक्षण परीक्षण गर्न आवश्यक पर्ने प्रविधि र जनशक्तिको कमी।
- आवश्यक जनशक्ति तथा दक्ष जनशक्ति को अभाव, साइबर सुरक्षा क्षेत्रमा काम गर्ने दक्ष जनशक्तिको न्यून उपलब्धता तथा साइबर सुरक्षा जस्तो महत्वपूर्ण र संवेदनशील क्षेत्रमा कार्यरत जनशक्तिहरूको सरुवा प्रणालीबाट सिर्जित समस्याहरू।
- क्षमता विकास नहुनु, कार्यरत जनशक्तिको क्षमता अभिवृद्धि कार्यक्रमको अभाव हुनुका साथै मनोबल बढाउन उत्प्रेरणामुलक कार्यको अभाव।
- सर्भर, नेटवर्क उपकरण, सफ्टवेयर, हार्डवेयरको न्यूनत्तम मापदण्ड तोक्न नसकिएको र प्रयोग अघि Bug free छ/छैन (Sandboxing) यकिन गर्ने कुनै प्रकारको संयन्त्र नभएको ।
- डिजिटल साक्षरतामा विद्यमान रहेको खाडल; जनचेतनाको अभाव हुनु; इन्टरनेट तथा सो सँग सम्बन्धित सेवाहरूको उचित प्रयोगमा आम जनताको ज्ञानको अभाव ।
- नीति निर्देशनलाई पूर्ण अनुपालनमा देखिएका समस्याहरू।
- समस्या समाधानका व्यवहारिक ज्ञान र अनुभवको कमी।
- उपलब्ध साइबर सुरक्षाका उपकरणहरूको पूर्ण रूपमा प्रयोग नहुनु।
- आचार संहिता र नैतिकताको अभाव।
- विभिन्न सूचना प्रणाली सूचना गरी ई-सेवा प्रदान गर्ने सङ्घ संस्थाहरूले सुरक्षाका आधारभुत मापदण्ड पुरा नगर्नु, आदि।

५.२. चुनौतीहरू

माथि उल्लेखित विभिन्न समस्याहरूले साइबर अपराध अनुसन्धानमा चुनौती सिर्जना गरेका छन्। जस्तैः

- व्यक्तिको व्यवहारमा परिवर्तन ल्याउने चुनौती।
- सीमित स्रोत र साधन बाट गम्भीर तथा जटिल किसिमको काम कारबाही गर्नुपर्ने चुनौती।
- नयाँ प्रविधिहरूको विकास र प्रयोग (जस्तै: 5G, Block chain and cryptocurrency) सँगै प्रविधिको फड्को (Technology Leapfrogging) समात्ने चुनौती।
- Internet of things (IoT) उपकरणहरूको व्यापक प्रयोगलाई नियमन गर्ने चुनौती।
- Phishing Scams

- अनाधिकृत (Pirated) सफ्टवेयरको प्रयोग नियन्त्रण
- सामाजिक सञ्जाल (Facebook, Twitter, Instagram, YouTube, TikTok WhatsApp) आदिलाई दर्ता प्रकृयामा ल्याउने चुनौती।
- आन्तरिक एवं वाह्य सुरक्षा जोखिमलाई कम गर्न नसक्नु।
- नवीनत्तम प्रविधिहरू जस्तैः Blockchain, Cryptocurrency को प्रयोगबाट सिर्जित चुनौतीहरू।
- सरकारी संयन्त्रमा कार्यरत सबै जनशक्तिसँग सूचना प्रविधि सम्बन्धित आधारभूत तालिम लगायतबाट डिजिटल साक्षरता वृद्धि गर्ने चुनौती।
- सार्वजनिक सेवामा साइवर सुरक्षा विषयका विज्ञ कर्मचारीहरू लगायत सूचना प्रविधि क्षेत्रमा लागेका जनशक्तिसँग विषयवस्तु सम्बन्धित दक्षता वृद्धि र टिकाइराख्ने चुनौती।
- स्रोत व्यवस्थापनका चुनौतीहरू।
- विद्यमान नीति कार्यान्वयन तथा नयाँ नीतिको आवश्यकता बुझाउन सक्ने व्यवस्थापन तहको जनशक्तिको अभाव।
- सरकारी तथा निजी क्षेत्रबाट डिजिटल माध्यमको प्रयोग गरी दिइने सेवामा साइबर सुरक्षाको चुनौती।
- विभिन्न संस्थाहरूले दिएका सेवाहरू र सो सेवा दिन प्रदान गर्न प्रयोग भएका प्रणालीहरू साथै प्रयोग भएका प्रकृयाहरूमा संस्थागत अनुपालन संयन्त्र तथा प्रणाली लेखापरीक्षण गराउने निकायको क्षमता विकासको चुनौती।
- संस्थाका कर्मचारीहरू नै साइबर अपराधमा संलग्न हुनसक्ने अवस्थालाई नियन्त्रण गर्दै cyber hygiene लाई चुस्त दुरुस्त राख्ने चुनौती।
- संस्थाभित्र व्यक्तिगत gadget को प्रयोगबाट हुन सक्ने सूचनाको चोरी नियन्त्रण गर्ने चुनौती।
- विभिन्न निकायलाई cybersecurity capability maturity model को विभिन्न तहमा राखेर संस्थालाई दिएको सेवाहरूलाई त्यो model को निस्चित तहसम्म पार नगरी सेवा प्रवाह भए नभएको नियमन गर्ने चुनौती।
- विभिन्न निकायमा pirated software हरूको व्यापक प्रयोगमा परिवर्तन ल्याउने चुनौती।
- सञ्चार तथा सूचना प्रविधि पुर्वाधारको स्थापना एवं विस्तारका चुनौती।
- बढ्दो Digitalization तथा e-governance को कार्यान्वयनका चुनौतीहरू।
- सञ्चार तथा सूचना प्रविधिमा निर्भरता एवं द्रुत विकासलाई पच्छ्याउने चुनौती।
- Data, Information को स्वामित्व एवं उत्तरदायित्व यकिन गर्ने गराउने चुनौती।
- अव्यवस्थित र असुरक्षित राष्ट्रिय साईवरस्पेशलाई सुरक्षित र व्यवस्थित बनाउने चुनौती।
- साइबर स्पेसको स्तरीकरण नियन्त्रण प्रणाली र कानूनी कार्यढाँचा तयार गर्ने चुनौती।

- Digitally Locked अवस्थाबाट मुक्त हुन Nepal Internet to the sea लाई छिटो कार्यान्वयन गरी आत्मनिर्भर हुदै जाने र वाह्य विश्वसँग सञ्चार तथा सूचना प्रविधि प्रणालीहरूलाई जोडिराख्ने चुनौती।
- तदर्थ रूपमा वितरण भैरहेको Internet bandwidth प्रणालीबाट सिर्जित सुरक्षा चुनौती सामना गर्न ब्यान्डविथलाई राष्ट्रिय ग्रिडमा ल्याई वितरण प्रणाली लागु गर्ने र National Gateway नियमन प्रणाली कार्यान्वयन गर्ने चुनौती।
- वृहत रूपमा प्रयोग हुने बाह्य राष्ट्रबाट सञ्चालित एप्लिकेशनहरू (Facebook, tiktok, etc)को माध्यमबाट हुने अपराध नियन्त्रण गर्न Digital evidences हासिल गर्ने चुनौती , आदि।

परिच्छेद ६- आगामी कार्यदिशा (Way Forward)

विश्वव्यापी रूपमा विस्तार भईरहेको साइबर स्पेसलाई हरेक राष्ट्र, संस्था, क्षेत्र तथा व्यक्तिले आत्मसाथ गर्दै अधिकतम उपलब्धि हासिल गरिरहेको परिप्रेक्षमा हाम्रो सन्दर्भमा पनि यसका अवसरहरूको सदुपयोग गरि राष्ट्रिय, सामाजिक, तथा नागरिक तहसम्म पहुँच कायम गरि विकास र समृद्धिका लक्षहरू हासिल गर्ने चुनौती एकातिर छ भने साइबर स्पेशको प्रयोग गरी हुने गरेका आन्तरिक र वाह्य सुरक्षा चुनौतीहरूको सामना गर्न उपयुक्त रणनीति कार्यनीति तथा कार्यक्रमहरू यकिन गरी सोको कार्यान्वयनको जिम्मेवारी प्रष्ट पार्ने र ती जिम्मेवारीहरू वहन गर्न सक्ने संस्थागत संयन्त्रको विकास र समन्वय गर्ने चुनौती अर्कातिर छ।

६.१. साइबर सुरक्षाका लागि रणनीतिक कार्यहरू

१. **साइबर सुरक्षित एवं उत्थानशील राष्ट्र, नेपालको कार्यान्वयन**

- ☞ साइबर सुरक्षा best practices को अवलम्वन, standards र Guidelines को कार्यान्वयन।
- ☞ Risk assessment and Risk management processes, Business continuity management and cyber crisis management को योजना तर्जुमा एवं कार्यान्वयन।
- ☞ संवेदनशील तथा महत्वपुर्ण ICT पुर्वाधारको पहिचान र सुरक्षाको प्रत्याभुति ।
- ☞ साइबर अडिट सम्वन्धी व्यवस्था र नियमन ।
- ☞ Regulatory frameworkको निर्माण तथा सुदृढिकरण ।

२. साइबर **संप्रभुता**

- ☞ राष्ट्रको साइबर स्पेसको सही उपयोग, राष्ट्रिय स्वार्थ अनुसारको प्रयोग, राष्ट्र तथा नागरिकको हितको लागि साइबरस्पेसको सुरक्षित प्रयोग।
- ☞ अन्य राष्ट्र र निकायहरू बिरुद्ध कुनै पनि प्रकारको साइबर कार्य / हमला हुन नदिने।
- ☞ Cyber Territorial Integrity लगायत का विविध विषयहरू सम्वोधन हुने गरी नीति तर्जुमा गर्दा उपयुक्त हुने।

३. महत्वपुर्ण ICT पुर्वाधारहरूको सुरक्षा

- ☞ देशमा रहेका महत्वपुर्ण सूचना तथा सञ्चार प्रविधि सम्बन्धी पूर्वाधारहरूको पहिचान गर्ने।
- ☞ नयाँ निर्माण हुने पूर्वाधारहरूको पहिचान र सो को सुरक्षा।

- ☞ सम्भावित थ्रेट/असुरक्षाका तत्वहरूको पहिचान गरी सोही अनुसार सुरक्षा प्रणाली-संयन्त्र-योजना निर्माण।
- ☞ २४X७ मनिटरिंग, Quick Action लिन सक्ने संयन्त्रको विकास र परिचालन।
- ☞ Response को तयारी लगायतका विविध क्षेत्रहरूको पहिचान तथा व्यवस्था।

४. राष्ट्रिय, आर्थिक, रक्षा लगायतका सम्पुर्ण क्षेत्रहरूको साइबर सुरक्षा

- ☞ विभिन्न सेक्टरहरूको अवधारणा अनुसारको सुरक्षा योजनाः सम्वन्धित सेक्टरहरू भित्रका निकाय - सरकारी, गैर-सरकारी, private, public सङ्गठनहरूबीचको समन्वय र सहकार्यको व्यवस्था तथा सेक्टरहरूबिचको समन्वय, सूचना साझेदारी, सहकार्यको व्यवस्था ।
- ☞ First Responder Entity को व्यवस्था,
- ☞ सूचना विश्लेषण, अनुसन्धान लगायतका कार्यहरू।

५. साइबर क्षमताको सुदृढीकरण

राष्ट्र विकास र समृद्धिका अनेकौ अवसरहरूको सृजना गर्न, कायम गर्न र सञ्चार तथा सूचना प्रविधिको विकास सँगै यसका सुरक्षा चुनौतीको अनवरत रूपमा सम्वोधन हुन जरुरी छ। साइबर सुरक्षा संवेदनशील क्षेत्र भएको हुनाले साइबर सुरक्षाको क्षमता अभिवृद्धि गर्नका लागि ठोस आधारहरू निर्धारण गरी कार्ययोजना तयार गरी राष्ट्रिय रूपमा नै आत्मनिर्भर हुनु अत्यावश्यक छ। विद्यालय तहबाटै साइबर सुरक्षा सम्बन्धी पाठ्यक्रम निर्धारण गर्ने, व्यवसायिक क्षमता अभिवृद्धि गर्न आकर्षित गर्ने योजनाहरूको कार्यान्वयन र विश्वविद्यालय तहका कार्यक्रमहरूमा जोड दिने, विभिन्न कार्यक्रमहरूको माध्यमबाट विश्वस्तरीय साइबर क्षमताको सुदृढीकरण गर्दै समयसिमाहरू निर्धारण गरी व्यावसायिक क्षमताका जनशक्तिहरूको विकास गर्नुका साथै राष्ट्रिय विभिन्न सुरक्षा, सरकारी निकायहरूलाई साधन स्रोत र प्रविधिले सुसज्जन गरी साइबर क्षमता अभिवृद्धि गर्नु आवश्यक देखिन्छ।

६. सञ्चार तथा सूचना प्रविधि सम्वन्धि सेवा प्रवाह गर्ने तथा सम्वन्धित निकायहरू सम्वन्धी नीति

सञ्चार तथा सूचना प्रविधि क्षेत्रमा कार्य गर्ने निकायहरूको साइबर सुरक्षा सम्वन्धी अझ बढी जिम्मेवारी तथा उत्तरदायित्व रहन्छ। आ-आफ्नो क्षेत्रमा राष्ट्र तथा सेवाग्राही समेतलाई साईवर सुरक्षा प्रत्याभूति गर्ने किसिमको योजना तर्जुमा गरी कार्यान्वयनमा ल्याउनु जरुरी देखिन्छ।

७. कानुनी तथा नियामक फ्रेमवर्कको निर्माण

साइबर सुरक्षाका विविध पक्षहरूको सम्वोधन गर्न कानुनी तथा नियामक फ्रेमवर्क निर्माण गर्नु अत्यावश्यक देखिएको छ। व्यक्तिगत, सामाजिक र राष्ट्रिय तहमा मात्र नभई Trans-Border तहमै अधिकतम वृद्धि

भइरहेको साइबर अपराध, साइबर घटना तथा आक्रमणहरूलाई कानुनी दायरामा ल्याउन, न्यूनीकरण गर्न र साइबरस्पेसमा रहेका Digital Evidences को प्राप्ति, संरक्षण र उपयोगका लागि कानुनी तथा नियामक फ्रेमवर्कको निर्माण गर्न जरुरी छ।

८. प्रविधि, प्रक्रिया, प्रणालीको मानकीकरण

राष्ट्रिय साइबर स्पेसमा अनियन्त्रित रूपमा असुरक्षित प्रविधि, Obsolete र Unpatched प्रणाली तथा Wide Range का Commercial, Smart उपकरणहरूको प्रयोगमा वृद्धि भईरहेको, भविष्यमा IOTको वृहत प्रयोग बढ्दा जोखिमहरू पनि बढ्ने हुनाले राष्ट्रको साइबरस्पेसमा प्रयोग हुने सञ्चार तथा सूचना प्रविधिका उपकरण, प्रविधि, प्रणाली र प्रक्रियाहरूको Standardization कायम गरी हरेक क्षेत्र, निकायहरूमा त्यसको कडाईका साथ कार्यान्वयन गर्न अत्यावश्यक रहेको छ।

९. साइबर सुरक्षा सम्वन्धी अनुसन्धान तथा विकास

साइबर सुरक्षा जस्तो संवेदनशील क्षेत्रमा क्रमश: आत्मनिर्भर हुदै जानु अत्यावश्यक छ। साइबर क्षमताको अभिवृद्धि गर्दै साइबर सुरक्षा सम्वन्धी अनुसन्धान तथा विकासका लागि कार्ययोजनाहरू तयार गर्नु पर्दछ।

१०.सार्वजनिक-निजी-सरकारी साझेदारी

राष्ट्रिय साइबर सुरक्षा नीतिले राष्ट्रिय तहदेखि विभिन्न निकाय, सङ्गठन तथा नागरिक तहसम्म नै साइबर सुरक्षा सम्वन्धी सचेतना अभिवृद्धि गर्दै प्रत्येक नागरिकहरूमा राष्ट्रिय साइबर सुरक्षा सम्वन्धी जिम्मेवारी बोध गराउने खालका कार्यक्रमहरू सञ्चालन गर्न साझेदारी गर्नु पर्दछ।

११.अन्तर्राष्ट्रिय समन्वय, सहयोग र साझेदारी

साइबर सुरक्षा सम्वन्धी अनुसन्धान, साइबर अपराध र आतङ्कवाद विरुद्ध सहकार्य, साइबर सुरक्षित र उत्थानशील समाज / विश्वको निर्माणका लागि अन्तर्राष्ट्रिय समन्वय, सहकार्य र साझेदारी गर्ने उपयुक्त संयन्त्रको विकास गर्न आवश्यक नीतिगत र कानुनी व्यवस्था गरी उपयुक्त वातावरण निर्माण गर्नु पर्दछ।

१२.साइबर सुरक्षा चुनौती, पूर्व चेतावनी संयन्त्र, जोखिम व्यवस्थापन तथा सुरक्षा जोखिम प्रतिकार्य

- ☞ राष्ट्रियस्तरको प्रणाली, प्रक्रिया, संरचना र संयन्त्रहरूको विकास गरी हरेक क्षेत्रका सामाजिक, सरकारी, गैर-सरकारी लगायतका निकाय, संस्थाहरूलाई परिस्थितिजन्य सचेतना वृद्धि गरी वर्तमान र सम्भावित सुरक्षा चुनौतीबारे जानकारी गराई प्राक्-सक्रिय (proactive), निवारणात्मक (preventive) र संरक्षणात्मक (protective) कदम चाल्न सक्ने बनाउने।

- ☞ राष्ट्रिय तहमा साइबर सुरक्षा आपतकालीन प्रतिकार्य, विपद् प्रतिकार्य र सङ्कट व्यवस्थापनका लागि २४ X ७ परिचालित रहने गरी प्रणाली-संयन्त्र-योजनाको व्यवस्था गर्नु पर्दछ।यस्तो प्रकारको योजनामा घटना वर्गीकरण गरी सो अनुसारको प्रतिकार्यको लागि तयारी हालतमा रहनु पर्दछ। विभिन्न प्रकारका साइवर घटना व्यवस्थापन र प्रतिकार्य गर्दा त्यसको प्रभाव अनुसारको कार्यढाँचाको व्यवस्था गर्नु पर्दछ। सामाजिक तथा व्यक्तिगत साइबर सुरक्षाको सम्वोधनको एक प्रकारले हुने गर्छ भने राष्ट्रिय तहमै प्रभाव पार्ने, राष्ट्रिय सुरक्षामा प्रभाव पार्ने खालको चुनौतीलाई राष्ट्रिय तहमा सम्वन्धित सबै निकायहरूको समन्वय र बहुआयामिक (multi-disciplinary approach) तवरबाट गर्ने व्यवस्था हुनु पर्दछ। यसरी विभिन्न पक्षहरूको व्यवस्थापन हुने गरी सम्वन्धित निकायहरूको भुमिका एवं जिम्मेवारी यथोचित तवरले परिभाषित गर्नुपर्ने हुन्छ।

१३. राष्ट्रिय तहमा सूचना आदानप्रदानको व्यवस्था

राष्ट्रिय साइबर सुरक्षा सम्बन्धी समन्वयकारी भुमिका निर्वाह गर्ने राष्ट्रिय प्रणाली-संयन्त्र-योजना बनाउने र स्पष्ट काम, कर्तव्य र जिम्मेवारी परिभाषित गर्ने तथा राष्ट्रिय तहमा सूचना आदानप्रदान संयन्त्रको व्यवस्था गर्नु उत्तिकै आवश्यक देखिन्छ।

६.२. रणनीतिक कार्यान्वयन योजना म्याट्रिक्स

राष्ट्रिय सुरक्षाको अभिन्न अङ्गको रूपमा रहेको साइबर सुरक्षाका विभिन्न आयामहरूमा माथिका परिच्छेदहरूबाट विवेचित परिदृश्यहरूको मूल्याङ्कन गरी विद्युतीय प्लेटफर्मको प्रयोगबाट सिर्जित जोखिमहरूलाई घटाउँदै राष्ट्रिय सुरक्षाको सुदृढीकरणका लागि निम्नबमोजिमका क्रियाकलापहरूको कार्यान्वयन गर्न आवश्यक कानूनी, संरचनागत एवं संस्थागत व्यवस्था गरी संलग्न कार्यान्वयन म्याट्रिक्स बमोजिम गर्न यस अध्ययन समितिले सिफारिस गरेको छः

रणनीतिक कार्यान्वयन योजना म्याट्रिक्स

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
१. नीतिगत आधारशीला तयार गर्ने।							
१.१ सुरक्षित र उत्थानशील साइबर स्पेशको लागि नीतिगत खाका (framework) को विकास	१.१.१	राष्ट्रिय साइबर सुरक्षा नीति तयार गर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, रक्षा मन्त्रालय, अर्थ मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय लगायतका सरोकारवाला मन्त्रालयहरू, नेपाल दूरसञ्चार प्राधिकरण	आ.व. २०७८/७९	मस्यौदा तयार भई स्वीकृतिको चरणमा रहेको।	राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ८ को (ग) र सूचना तथा सञ्चार प्रविधि नीति, २०७२ को दफा ११.२१ सँग सम्बन्धित विषय
	१.१.२	सूचना प्रविधिको प्रयोग र नियमनका सम्बन्धमा कानूनी व्यवस्था हुनु पर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, रक्षा मन्त्रालय, अर्थ मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय लगायतका सरोकारवाला मन्त्रालयहरू, नेपाल दूरसञ्चार प्राधिकरण	आ.व. २०७८/७९	विद्येयक तयार भई संसदमा विचाराधीन रहेको।	प्रतिनिधि सभामा दर्ता मितिः २०७५।११।२ प्रस्तुत : २०७५।११।८ सामान्य छलफल: २०७५।११।१० समितिमा दफावार छलफल: २०७५।११।१४
	१.१.३	साइवर सुरक्षा विधेयकको मस्यौदा तयार गर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, अर्थ मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय, रक्षा मन्त्रालय नेपाल दूरसञ्चार प्राधिकरण	आ.व. २०७९/ ८०	अध्ययन चरणमा रहेको	नेपाल दूरसञ्चार प्राधिकरणबाट अध्ययन सुरु गरिएको (राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ८ को (ग) सँग सम्बन्धित विषय)

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	१.१.४	राष्ट्रिय साइबर सुरक्षाको रोडम्याप (National Cyber Security Road Map) तयार गरी जारी गर्ने	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, अर्थ मन्त्रालय, कानुन, न्याय तथा संसदीय मामिला मन्त्रालय, रक्षा मन्त्रालय नेपाल दूरसञ्चार प्राधिकरण	आ.व. २०७९/ ८०		नेपाल दूरसञ्चार प्राधिकरणबाट यस सम्बन्धी कार्य अघि बढाईएको
	१.१.५	राष्ट्रिय स्तरबाट साइबर सुरक्षा तथा साइबर अपराध क्षेत्रलाई विशेष प्राथमिकतामा राखी योजना तर्जुमा गर्ने।	राष्ट्रिय योजना आयोग	सबै सरोकारवाला निकाय	आ.व. २०७९/ ८०		
	१.१.६	गुणस्तरीय सफ्टवेयर निर्माण तथा आयात एवम् हार्डवेयर एवम् नेटवर्क उपकरण प्रयोगका लागि आवश्यक पर्ने न्यूनत्तम मापदण्ड तयार गर्ने	सञ्चार तथा सूचना प्रविधि मन्त्रालय	सरोकारवाला निकाय तथा यस विषयसँग सम्बन्धित विज्ञहरू	आ.व. २०७९/ ८०		
	१.१.७	साइवर सुरक्षा तथा अपराध नियन्त्रणका लागि विभिन्न मुलुकसँग पारस्परिक कानूनी सहायता सन्धी (Mutual Legal Assistance Treaty (MLAT)) गर्ने।	कानून, न्याय तथा संसदीय मामिला मन्त्रालय	सञ्चार तथा सूचना प्रविधि मन्त्रालय, गृह मन्त्रालय, परराष्ट्र मन्त्रालय	आ.व. २०७९/ ८०	सम्झौताका लागि का. न्या. तथा सं. व्य. मं.मा पत्राचार भएको	राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.७ सँग सम्बन्धित विषय

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	१.१.८	निजी तथा सार्वजनिक निकायहरूले राष्ट्रिय सूचना सञ्चार प्रविधि नीति २०७२ सँग तादाम्यता हुने गरी अनिवार्य रूपमा आफ्नो निकायको लागि ICT Security सम्बन्धी Guidelines/ Standards/ Policy तयार गरी लागू गर्ने व्यवस्था मिलाउने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	सरोकारवाला निकाय तथा यस विषयसँग सम्बन्धित विज्ञहरू	आ.व. २०७८/ ७९		नियामक निकाय नतोकिएकोले कार्यान्वयनमा चुनौती रहेको हुँदा नियामक निकाय तोक्नुपर्ने।
	१.१.९	सूचना प्रविधि प्रयोग गरी सेवा प्रदान गरिरहेका सार्वजनिक तथा निजी संस्थाहरूले अनिवार्य रुपमा साइबर सुरक्षा अडिट गराउनुपर्ने कानुनी व्यवस्था गर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय, सम्बन्धित नियामक निकाय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, अर्थ मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय	आ.व. २०७८/ ७९		अभ्यासमा नरहेको। बाध्यकारी व्यवस्था गर्नुपर्ने।
१.२ प्रभावकारी साइबर अपराध अनुसन्धानका लागि कानूनी व्यवस्था	१.२.१	नेपाल बाहिरबाट सञ्चालित सामाजिक सञ्जाल लगायत मेसेन्जर, इमेल प्रणालीसँग सम्बन्धित डाटा प्राप्त गर्नका लागि Mutual Legal Assistance Treaty (MLAT) को व्यवस्था गर्ने।	कानून, न्याय तथा संसदीय मामिला मन्त्रालय	सञ्चार तथा सूचना प्रविधि मन्त्रालय, गृह मन्त्रालय, परराष्ट्र मन्त्रालय	आ.व. २०७९/ ८०		अनुसन्धानका क्रममा डाटा प्राप्त नहुने कारण कठिनाई आउने गरेको। (राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.७ को विषय)

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	१.२.२	अनुसन्धानका कार्यलाई प्रभावकारी बनाउन सञ्चार तथा सूचना प्रविधि सम्बन्धी सेवा प्रदान गर्ने, सम्वेदनशील व्यक्तिगत तथा संस्थागत विवरणहरू भण्डारण गर्ने निजी तथा सरकारी संस्थाहरूलाई Log राख्न लगाउने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय सम्बन्धित नियमनकारी निकाय	नेपाल प्रहरी	आ.व. २०७८/ ७९		यस सम्बन्धी पूर्वाधार विकास तथा व्यवस्थापन गर्न बाध्यकारी गर्ने व्यवस्था गराउन आवश्यक रहेको।(राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.१ को विषय)
	१.२.३	साइबर अपराध अनुसन्धानको हद म्याद ३५ दिन बाट ९० दिन गर्नु पर्ने	गृह मन्त्रालय, कानून तथा संसदीय व्यवस्था मन्त्रालय	नेपाल प्रहरी	आ.व. २०७८/ ७९		अन्तराष्ट्रिय अभ्यास अनुसार पनि ३५ दिनको हद म्याद अव्यवहारिक रहेको; अनुसन्धानको प्रभावकारिता बढाउनका लागि आवश्यक रहेको।
२. संस्थागत सुदृढीकरण एवं नवीन व्यवस्था गर्ने।							
२.१ सुरक्षित साइबर स्पेशको लागि सुदृढ संस्थागत संरचना तयार गर्ने।	२.१.१	राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूहको क्षमता अभिवृद्धि गर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, अर्थ मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय	निरन्तर		राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूहको गठन भई कार्य गरिरहेको भएता पनि पूर्ण समर्पित भई कार्य गर्न समस्या रहेको; र सो समूहको क्षमता अभिवृद्धि

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
							गरी साइबर सुरक्षा जोखिमको पहिचान, त्यसबाट हुने असरको न्यूनीकरण र आकस्मिक साइबर सुरक्षा प्रदान गर्न दक्ष जनशक्ति बनाउन आवश्यक रहेको।
	२.१.२	क्षेत्रगत सूचना प्रविधि आकस्मिक सहायता समूहको गठन गर्ने।	सूचना प्रविधि आकस्मिक सहायता समुहको निर्देशक समिति	सञ्चार तथा सूचना प्रविधि मन्त्रालय र अन्य सरोकारवाला निकाय	आव २०७९/८०	नेपाल दूरसञ्चार प्राधिकरणले Cyber Security Task Force (NTACERT) गठन गरेको।	सूचना प्रविधि आकस्मिक सहायता समूह सञ्चालन तथा व्यवस्थापन निर्देशिका, २०७५ मा क्षेत्रगत सूचना प्रविधि आकस्मिक सहायता समुह गठन गर्न सकिने व्यवस्था रहेको।
	२.१.३	राष्ट्रिय साइबर सुरक्षा अनुगमन केन्द्रको स्तरोन्नति गर्ने तथा विभिन्न निकायहरूको प्रणालीलाई आवद्ध गर्ने।	सूचना प्रविधि आकस्मिक सहायता समुहको निर्देशक समिति	सञ्चार तथा सूचना प्रविधि मन्त्रालय, अन्य सरोकारवाला निकायहरू	आ.व. २०७९/ ८०	राष्ट्रिय साइबर सुरक्षा अनुगमन केन्द्रको	न्यून संख्यामा मात्र सरकारी सूचना प्रविधि प्रणालीहरू आवद्ध भएको, थप प्रणालीहरू आवद्ध गराई निरन्तर अनुगमन गर्नुपर्ने

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
						स्थापना भई केही सरकारी सूचना प्रविधि प्रणालीहरू को अनुगमन भइरहेको।	अवस्था रहेको, सोका लागि जनशक्तिको अभाव रहेको, स्रोत साधनको व्यवस्था गरी स्तरोन्नति गर्न तथा विभिन्न निकायहरूको प्रणालीलाई आवद्ध गर्न आवश्यक रहेको।
	२.१.४	प्रमाणीकरण नियन्त्रकको कार्यालयको साइबर फरेन्सिक ल्याबको स्तरोन्नती/क्षमता अभिवृद्धि गर्ने।	प्रमाणीकरण नियन्त्रकको कार्यालय	सञ्चार तथा सूचना प्रविधि मन्त्रालय	आ.व. २०७९/ ८०	साइबर फरेन्सिक ल्याब संचालनमा रहेको	साइबर फरेन्सिक ल्याबलाई सक्रिय रुपमा कार्य गर्न सक्ने गरी स्रोतसाधनको व्यवस्था, जनशक्तिको व्यवस्था गर्नुपर्ने।
	२.१.५	राष्ट्रिय महत्वका सूचना प्रणालीको कार्य निरन्तरता तथा विपद् पश्चातको पुनर्लाभ (business continuity and disaster recovery)को लागि आवश्यक संस्थागत संरचना तथा योजना विकास गर्ने।	सरोकारवाला निकायहरू	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, अर्थ मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय, राष्ट्रिय विपद् जोखिम न्यूनीकरण तथा व्यवस्थापन प्राधिकरण	आ.व. २०७९/ ८०		विपद् जोखिमका लागि वित्तीय व्यवस्थापन राष्ट्रिय रणनीति, २०७८ को बजारमा आधारित वित्तीय साधन सहितको दीर्घकालीन कार्यान्वयन कार्ययोजनासँग सम्बन्धित

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	२.१.६	नागरिकका वैयक्तिक विवरण (नाम, ठेगाना, इमेल, मोबाइल नम्बर, नागरिकता, पासपोर्ट जस्ता विवरण) सङ्कलन तथा सञ्चय/ भण्डारण गर्ने सरकारी तथा निजी संघसंस्थाहरुले जुन प्रयोजनका लागि विवरण संकलन भण्डारण गरेको हो सो प्रयोजन वा कानूनले व्यवस्था गरेबमोजिम बाहेक अन्य प्रयोजनका लागि प्रयोग नगर्ने सुनिश्चितताको लागि नियमनकारी निकाय तोक्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	सञ्चार तथा सूचना प्रविधि मन्त्रालय, सूचना प्रविधि विभाग	आ.व. २०७९/ ८०		संवेदनशील व्यक्तिगत विवरण; Personally identifiable Information (PII) तोकिनुपर्ने।
		(क) यस्ता संघसंस्थाहरुले डाटा सङ्कलन तथा सञ्चय/ भण्डार, प्रोसेस व सञ्चार गर्दा अपनाउनु पर्ने न्यूनतम सुरक्षा मापदण्ड (Security Standard) तय गरी लागू गर्ने।	सम्बन्धित नियमनकारी निकाय	सञ्चार तथा सूचना प्रविधि मन्त्रालय, सूचना प्रविधि विभाग लगायतका सरोकारवाला निकाय	आ.व. २०७९/ ८०		
		(ख) न्यूनतम सुरक्षा मापदण्ड (Security Standard) लागू	सम्बन्धित नियमनकारी निकाय	सञ्चार तथा सूचना प्रविधि मन्त्रालय, सूचना प्रविधि विभाग लगायतका सरोकारवाला निकाय	आ.व. २०७९/ ८०		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
		गर्ने सम्बन्धमा नियमित अनुगमन गर्ने,					
	२.१.७	नेपाल दूरसञ्चार प्राधिकरण, सूचना प्रविधि विभाग, नेपाल प्रहरी साइबर ब्यूरो लगायतका जिम्मेवार निकायहरूको संगठनात्मक संरचना एवम् कार्यदक्षता अभिवृद्धि गर्ने सोको लागि आवश्यक जनशक्ति व्यवस्थापन गर्न संगठन तथा व्यवस्थापन सर्वेक्षण गर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, अर्थ मन्त्रालय	आ.व. २०७९/ ८०		क्षमता विकास गर्न तथा विद्यमान जनशक्तिलाई समेत टिकाइराख्न नसकिएको हुँदा विभिन्न क्षेत्रमा साइबर सुरक्षा सम्बन्धी जनशक्तिको प्राप्ति र विकास सम्बन्धी विशेष रणनीति आवश्यक रहेको।
	२.१.८	राष्ट्रिय साइबर सुरक्षा केन्द्र स्थापना गर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय		आ. व. २०७९।८०		साइवर सुरक्षाको विषयमा अनुसन्धान तथा विकास, साइबर सुरक्षा प्रवर्द्धन, जनचेतना अभिवृद्धि, साइबर सुरक्षा सम्बन्धी तयारी, रोकथाम, पहिचान, प्रतिक्रिया तथा पुनर्लाभ गर्न, २४/७ सम्पर्क निकायको रुपमा कार्य गर्न तथा डिजिटल फोरेन्सिक अनुसन्धान गर्नका लागि ।

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	२.१.९	सूचना प्रविधि प्राधिकरणको स्थापना गर्ने	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानमन्त्रि तथा मन्त्रिपरिषद्को कार्यालय, अर्थ मन्त्रालय, संघीय मामिला तथा सामान्य प्रशासन मन्त्रालय	आ.व. २०७९/ ८० आ.व. २०८०/ ८१		सरकारी निकायका सूचना प्रविधिको निर्माण, सफ्टवेयरहरू -को निर्माण, मर्मत संभार अनुगमन गर्नका लागि सूचना प्रविधि प्राधिकरणको स्थापना गर्न आवश्यक देखिन्छ।
	२.१.१०	सूचना प्रविधि अन्वेषण (R&D) तथा प्रशिक्षण केन्द्रको स्थापना गर्ने	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानमन्त्रि तथा मन्त्रिपरिषद्को कार्यालय, अर्थ मन्त्रालय, संघीय मामिला तथा सामान्य प्रशासन मन्त्रालय	आ.व. २०७९/ ८० आ.व. २०८०/ ८१		
	२.१.१०	विभिन्न ICT सेवा प्रदायक संस्थाहरूको वर्गीकरण गरी तिनीहरूको अनुपालन संयन्त्र रहे नरहेको यकिन गर्न अनुगमन तथा नियमन गर्ने नियामक निकायहरू तोक्ने तथा तोकिएका नियामक निकायको स्तरोन्नति गरिनु पर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	नेपाल दुरसञ्चार प्राधिकरण, सूचना प्रविधि विभाग	निरन्तर		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	२.१.११	साइबर सुरक्षासँग सम्बन्धित निजी क्षेत्र एवं अन्तर्राष्ट्रिय क्षेत्रका संघसंस्थाहरूसँग समन्वय तथा सहकार्य गर्न निकायगत व्यवस्था।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	कानून, न्याय तथा संसदीय मामिला मन्त्रालय, परराष्ट्र मन्त्रालय	आ.व. २०७९/ ८०		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.७ सँग सम्बन्धित विषय
२.२ प्रभावकारी साइबर अपराध अनुसन्धानका लागि सुदृढ संस्थागत/ संरचनागत व्यवस्था गर्ने।	२.२.१	साइबर सुरक्षा तथा साइबर अपराध सम्बन्धी विषयमा अन्तर्राष्ट्रिय सहकार्यका लागि सम्पर्क बिन्दू (points of Contact) तोक्ने	गृह मन्त्रालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय	परराष्ट्र मन्त्रालय	आ.व. २०७९/ ८०		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.७ सँग सम्बन्धित विषय
	२.२.२	नेपाल बाहिरबाट सञ्चालित सामाजिक सञ्जाल, ईमेल सेवा प्रदायक, लगायतका विभिन्न सेवा प्रदायक संस्थाको Local Contact Office को स्थापना गर्न नीतिगत व्यवस्था गर्ने।	सूचना तथा सञ्चार प्रविधि मन्त्रालय	कानून, न्याय तथा संसदीय मामिला मन्त्रालय, परराष्ट्र मन्त्रालय	आ.व. २०७९/ ८०		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.३.२ सँग सम्बन्धित विषय
	२.२.३	सुरक्षा निकायहरुमा सूचना संकलन, विश्लेष्ण, संभावित साइबर खतराको मूल्याङ्कन, अनुसन्धान र विकासका लागि आधुनिक प्रविधिको प्रयोग गर्ने।	रक्षा मन्त्रालय, गृह मन्त्रालय	प्रधानन्त्री तथा मन्त्री परिषदको कार्यालय	निरन्तर		(राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.१ र २.८.१०.१.३.२ सँग सम्बन्धित विषय)

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	२.२.४	सुरक्षा निकायलाई साइबर सुरक्षा तथा साईबर अनुसन्धान सम्बन्धमा क्षमता अभिवृद्धि गरी समयानुकूल सबलीकरण गर्ने।	रक्षा मन्त्रालय, गृह मन्त्रालय	प्रधानन्त्री तथा मन्त्री परिषदको कार्यालय	निरन्तर		(राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.३.२ सँग सम्बन्धित विषय)
	२.२.५	नेपाल प्रहरीमा प्रदेशगत तथा जिल्लागत साइबर सेल गठन गर्ने।	गृह मन्त्रालय	नेपाल प्रहरी	आ.व. २०७९/ ८० - २०८४/८५		सूचना प्रविधि विधेयकमा उल्लेख गरिएको
३. रणनीतिक पूर्वाधारहरू तयार गर्ने।							
	३.१.१	राष्ट्रिय संवेदनशील सूचना तथा सञ्चार प्रविधि पूर्वाधारहरूको नियमनका लागि सम्बन्धित नियमनकारी निकाय तोक्ने।	रक्षा मन्त्रालयको प्रस्तावमा राष्ट्रिय सुरक्षा परिषद	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय, गृह मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय मन्त्रालय लगायतका सरोकारवाला निकायहरू			राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.३.२ र २.८.१०.१.४ तथा राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ६ को (५) सँग सम्बन्धित विषय
३.१ राष्ट्रिय रूपमा संवेदनशील सूचना तथा सञ्चार प्रविधि	३.१.२	संवेदनशील सूचना तथा सञ्चार प्रविधि पूर्वाधारहरू पहिचान गर्ने मापदण्ड तयार गर्ने।	तोकिएको निकाय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय, गृह मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय, रक्षा	आ.व. २०७९/ ८०		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.३.२ र २.८.१०.१.४ तथा राष्ट्रिय सुरक्षा नीति, २०७५ को

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
पूर्वाधारहरू पहिचान, सुरक्षाको उचित प्रबन्ध तथा नियमन गर्ने।				मन्त्रालय लगायतका सरोकारवाला निकायहरू			भाग ६ को (५) सँग सम्बन्धित विषय
	३.१.३	संवेदनशील सूचना तथा सञ्चार प्रविधि पूर्वाधारहरू पहिचान गरी वर्गिकरण गर्ने।	तोकिएको निकाय	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय, गृह मन्त्रालय, रक्षा मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय, रक्षा मन्त्रालय लगायतका सरोकारवाला निकायहरू	आ.व. २०७९/ ८०		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.३.२ र २.८.१०.१.४ तथा राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ६ को (५) सँग सम्बन्धित विषय
	३.१.४	संवेदनशील सूचना तथा सञ्चार प्रविधि पूर्वाधारहरूको न्यूनतम सुरक्षा मापदण्ड (Minimum Security Standard) तय गरी लागू गर्ने ।	संवेदनशील सूचना तथा सञ्चार प्रविधि पूर्वाधारहरू सम्बन्धी नियमनकारी निकाय	सञ्चार तथा सूचना प्रविधि मन्त्रालय, नेपाल दूरसञ्चार प्राधिकरण, नेपाल राष्ट्र बैंक लगायत अन्य सरोकारवाला निकायहरू	आ.व. २०७९/ ८०		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.३.२ र २.८.१०.१.४ तथा राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ६ को (५) सँग सम्बन्धित विषय
३.२ सुदृढ एवम् उत्थानशील सूचना सञ्चार	३.२.१	साइबर हमलाबारे अद्यावधिक सूचना आदानप्रदान गर्न डिजिटल पूर्वाधार (Digital Infrastructure) को विकास गर्ने।	N-ITERT	सरोकारवाला निकायहरू	आ.व. २०७९/ ८०		राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ६ को (५) सँग सम्बन्धित विषय

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
प्रविधि पूर्वाधार विकास गर्ने।	३.२.२	विद्युतीय भुक्तानी प्रणालीलाई भरपर्दो र सुरक्षित बनाउन जारी गरिएका मार्गदर्शन अध्यावधिक गरी प्रभावकारी बनाउने	नेपाल राष्ट्र बैंक	अर्थ मन्त्रालय	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.८.१.४ सँग सम्बन्धित
	३.२.३	राष्ट्रिय सूचना महामार्ग लगायतका दूरसञ्चार तथा सूचना प्रणाली सञ्जाललाई थप सुरक्षित र उत्थानशील बनाउने।	नेपाल दूरसञ्चार प्राधिकरण	सञ्चार तथा सूचना प्रविधि मन्त्रालय	निरन्तर		
	३.२.४	सार्वजनिक निजी साझेदारी [Public–private partnership- (PPP)] को अवधारणा अनुरुप संयन्त्र निर्माण गरी पूर्वाधारहरूको विकास गर्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय		आ.व. २०७९/ ८०		
४. जनशक्ति व्यवस्थापन र क्षमता विकास गर्ने।							
४.१ साइबर सुरक्षाको क्षेत्रमा दक्ष जनशक्ति विकास गर्ने।	४.१.१	सरकारी निकायहरूमा रहेका सूचना प्रविधि क्षेत्रका दरबन्दीहरूको पुनरावलोकन गरी आवश्यक दरबन्दीको व्यवस्था गर्ने।	सम्बन्धित निकायहरू	सङ्घीय मामिला तथा सामान्य प्रशासन मन्त्रालय, गृह मन्त्रालय, अर्थ मन्त्रालय	आ.व. २०७९/ ८०		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	४.१.२	सूचना प्रविधि सम्बन्धी जनशक्तिको सेवा सञ्चालन तथा व्यवस्थापन गर्ने निकाय हाल सङ्घीय मामिला तथा सामान्य प्रशासन मन्त्रालय भएकोमा सञ्चार तथा सूचना प्रविधि मन्त्रालयलाई तोक्ने।	सङ्घीय मामिला तथा सामान्य प्रशासन मन्त्रालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय	अर्थ मन्त्रालय, कानून न्याय तथा संसदीय मामिला मन्त्रालय	आ.व. २०७९/ ८०		
	४.१.३	सरकारी निकायहरूमा रहेका सूचना प्रविधि क्षेत्रका कर्मचारीहरूका लागी उत्प्रेरणा, वृत्ति विकासको अवसर प्रदान गरी टिकाइराख्ने (Retention Policy) वातावरणको सिर्जना गर्ने।	सङ्घीय मामिला तथा सामान्य प्रशासन मन्त्रालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय				सूचना प्रविधि क्षेत्रका दक्ष जनशक्ति सरकारी सेवामा आउन नचाहने, भएका दरबन्दी खाली रहने; अत्याधिक कार्यबोझ र न्यून वृत्ति विकासको अवसरका कारण छोडेर जाने प्रवृत्ति रहेको।
	४.१.४	निजामती सेवामा सूचना प्रविधि सम्बन्धी छुट्टै सेवा गठन गरी सो अन्तर्गत साइवर सुरक्षा समूह गठन गर्ने।	सङ्घीय मामिला तथा सामान्य प्रशासन मन्त्रालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय	अर्थ मन्त्रालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय	आ.व. २०७९/ ८०		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	४.१.५	सार्वजनिक निकायहरूका सूचना प्रविधि सम्बन्धी जनशक्तिलाई साइबर सुरक्षा सम्बन्धी विशिष्टिकृत तालिम तथा स्थलगत अवलोकनको व्यवस्था गरी क्षमता अभिवृद्धि गर्ने।	सूचना प्रविधि विभाग, सेवा संचालक निकाय	अर्थ मन्त्रालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ७ को (८) सँग सम्बन्धित विषय
	४.१.६	साइबर सुरक्षा सम्बन्धी विशिष्ट जनशक्ति निर्माण गर्न विश्वविद्यालयहरूसँग सहकार्य गर्ने।	शिक्षा मन्त्रालय	अर्थ मन्त्रालय, सञ्चार तथा सूचना प्रविधि मन्त्रालय	आ.व. २०७९/ ८०		
	४.१.७	सरकारी, सुरक्षा निकाय तथा निजी क्षेत्रहरुमा सूचना सुरक्षा सम्बन्धि कार्य गरिरहेका जनशक्तिको (Resource Pool) विवरण अद्यावधिक गरी राख्ने।	सञ्चार तथा सूचना प्रविधि मन्त्रालय	प्रधानन्त्री तथा मन्त्री परिषदको कार्यालय, रक्षा मन्त्रालय, गृह मन्त्रालय	निरन्तर		
५. नवप्रवर्तनशील अभ्यास तथा प्रविधिको प्रयोग गर्ने।							
५.१ विद्युतीय अभिलेखको सृजना, उत्पादन, प्रशोधन, सञ्चय, प्रवाह तथा	५.१.१	सार्वजनिक तथा निजी क्षेत्रका महत्वपूर्ण प्रणालीहरूमा डिजिटल हस्ताक्षर प्रयोगमा ल्याउने ।	प्रमाणीकरण नियन्त्रककको कार्यालय (OCC), सञ्चार	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, अर्थ मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय	निरन्तर		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
सम्प्रेषण प्रणालीको मान्यता, सत्यता, अखण्डता र विश्वसनीयतालाई प्रमाणीकरण गर्ने तथा अनधिकृत प्रयोग वा परिवर्तन गर्ने कार्यलाई नियन्त्रण गर्ने।			तथा सूचना प्रविधि मन्त्रालय				
५.२ विभिन्न निकायमा pirated software हरूको व्यापक प्रयोगमा परिवर्तन ल्याउने।	५.२.१	सरकारी तथा सार्वजनिक निकायहरूले Genuine/Licensed Software हरू मात्र प्रयोग गर्ने।	सबै सरकारी तथा सार्वजनिक निकायहरू	सञ्चार तथा सूचना प्रविधि मन्त्रालय	निरन्तर		अधिकांश निकायहरूले pirated windows and office package प्रयोग गरिरहेको हुँदा पछिल्लो Window patch को crack version अद्यावधिक हुन नसकी ह्याकरको निशानामा सजिलै पर्ने गरेको।
५.३ साइबर सुरक्षा प्रणालिको	५.३.१	Government Enterprises Architecture को प्रभावकारी कार्यान्वयन गर्ने।	सरोकारवाला सबै निकाय	सञ्चार तथा सूचना प्रविधि मन्त्रालय	आ.व. २०७८/ ७९		लागतप्रभावकारिताका हिसाबले समेत उपयुक्त रहेको।

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
ecosystem मा सुचना आदान प्रदानमा सुरक्षा प्रत्याभूति प्रदान गर्ने।	५.३.२	सार्वजनिक निकायहरुले डाटा संवेदनशिलतालाई मध्यनजर गर्दै सूचना वर्गीकरण गर्ने तथा आवश्यकतानुसार सूचनाहरुको गोपनियाता कायम राख्ने	सरोकारवाला सबै निकाय	सञ्चार तथा सूचना प्रविधि मन्त्रालय	निरन्तर		
	५.३.३	निकायगत सुरक्षा संवेदनशीलतालाई मध्यनजर गर्दै कार्यालयहरूमा व्यक्तिगत उपकरणको प्रयोग सम्बन्धमा (Bring Your Own Device) BYOD नीति निर्माण गरी लागू गर्ने।	सबै सरकारी तथा सार्वजनिक निकायहरू		निरन्तर		सरकारी निकायका प्राङ्गणमा निजी Devices प्रयोग नियन्त्रण गर्ने नीति आवश्यक पर्ने।
	५.३.४	साईवर सुरक्षाका (Capability Maturity Model Integration) CMMI मा रहेका तहहरू मध्य कम्तिमा तेस्रो तह (defined) पार गर्नु पर्ने।	सूचना प्रविधि विभाग	सबै सरकारी तथा गैरसरकारी निकायहरू	निरन्तर		प्रकृयागत सुधारका लागि नीति प्रविधि र जनशक्तितहको सुरक्षा सुनिश्चित गर्नुपर्ने।
	५.३.५	निकायहरूले साइबर सुरक्षा जोखिम मूल्याङ्कन गरी risk threat तथा vulnerability matrix अद्यावधिक गर्नु पर्ने।	प्रयोगकर्ता निकाय	सूचना प्रविधि विभाग	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ६ को (५) सँग सम्बन्धित विषय (उक्त

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
							प्रयोजनका लागि दक्ष जनशक्तिको अभाव रहेको।)
	५.३.६	निकायहरूले साइबर सुरक्षा जोखिम पहिचान, रोकथाम, प्रतिक्रिया, तथा पुनर्लाभ (Preparedness, Protection, Detection, Response and Recovery) सम्बन्धि योजना तयार गरी कार्यान्वयन गर्ने।	प्रयोगकर्ता निकाय	सूचना प्रविधि विभाग	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ८ को (ग) सँग सम्बन्धित विषय (उक्त प्रयोजनका लागि दक्ष जनशक्तिको अभाव रहेको।)
	५.३.७	निकायहरुमा Security Information and Event Management (SIEM) उपकरण/सिस्टम प्रयोगमा जोड दिइनुपर्ने।	प्रयोगकर्ता निकाय	सूचना प्रविधि विभाग	निरन्तर		तथा राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ७ को (८) सँग सम्बन्धित विषय
	५.३.८	कार्यालयबाट निर्माण गरिने सूचना प्रविधिसँग सम्बन्धित प्रणाली तथा वेबसाइट निर्माण गर्दा सुरक्षा चुनौतीलाई (किप्टो माइनिङ, डाटाको चोरी आदि) Security Audit गरेर मात्र Launch/ प्रयोगमा ल्याउने	प्रयोगकर्ता निकाय	सूचना प्रविधि विभाग	निरन्तर		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	५.३.९	Ransomware बाट हुनसक्ने आर्थिक क्षति तथा प्रणालीमा हुने खराबी (System Crash) बाट हुनसक्ने क्षतीलाई न्यूनीकरण गर्न नियमितरुपमा डाटा ब्याकअप गरीरहने, हरेक कार्यालयको डाटा ब्याकअप गर्नका लागि ब्याकअप सिस्टम (DR, SAN/NAS Storage, हार्ड डिस्क लगायत) को व्यवस्था गर्ने	प्रयोगकर्ता निकाय	सूचना प्रविधि विभाग	निरन्तर		
	५.३.१०	कर्मचारीहरुको सरुवा/बढुवा तथा शाखा परिवर्तन हुँदा बरबुझारथको क्रममा उक्त व्यक्तीको सूचना प्रविधिसँग सम्बन्धित प्रणालीमा भएको Access (Username, password) निश्क्रिय गरी गोपनियता कायम गर्नु पर्ने	प्रयोगकर्ता निकाय	सूचना प्रविधि विभाग	निरन्तर		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	५.३.११	फिसिंग इमेलको पहिचान हुनासाथ सो सम्बन्धमा सचेत हुनका लागि सम्पूर्ण कार्यालयका कर्मचारीलाई ब्रोडकास्ट इमेल पठाउने	प्रयोगकर्ता निकाय	सूचना प्रविधि विभाग	निरन्तर		
	५.३.१२	सोसल इन्जिनियरिंगको हमलाबाट वच्न कस्ता व्यक्तिहरुसँग कुन तहको निकटता कायम गर्ने भन्ने विषयमा कर्मचारीहरुलाई नियमित सचेत गराउने	प्रयोगकर्ता निकाय	सूचना प्रविधि विभाग	निरन्तर		
	५.३.१३	सार्वजनिक निकायहरुमा पेन ड्राइभको प्रयोगमा नियन्त्रण गर्ने	सरोकारवाला निकाय		निरन्तर		Pen Drive Data Transfer मा धेरै प्रयोगहुने साधन भएकोले महत्वपूर्ण डाटा चोरी, भाइरस सार्ने, system corrupt हुन सक्ने भएकोले
५.४ प्रभावकारी साइबर अपराध अनुसन्धान	५.४.१	अनुसन्धानका क्रममा आन्तरिक सूचना सङ्कलन गर्ने	साइबर व्यूरो, केन्द्रीय अनुसन्धान व्यूरो	Internet Service Providers, नेपाल दूरसञ्चार प्राधिकरण लगायत अन्य सबै सम्बन्धित निकायहरू	निरन्तर		(राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.३.२ र २.८.१०.१.१२ सँग सम्बन्धित विषय)

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	५.४.२	प्रविधिमा आधारित अपराध अनुसन्धानको क्रममा प्रयोग हुने Tools and Technologies समन्वयात्मक तथा नियन्त्रणात्मक प्रयोग सुनिश्चित गर्ने	अपराध अनुसन्धान गर्ने सहयोगी निकायहरू	अन्तर सम्बन्धित निकायहरू	निरन्तर		एकल सम्पर्क बिन्दु तोकिनु पर्ने। स्रोतको दोहोरोपन र कमसल प्रयोग रोक्नुपर्ने।
	५.४.३	साइबर अपराध अनुसन्धानको कार्यान्वयन	साइबर व्यूरो	नेपाल प्रहरी, गृह मन्त्रालय	निरन्तर		
६. अनुगमन तथा मूल्याङ्कनलाई प्रभावकारी बनाउने।							
६.१ सूचना प्रविधि प्रणाली र पूर्वाधारहरूको सुरक्षण परीक्षण तथा प्रभावकारी अनुगमन/ मूल्याङ्कन गर्ने	६.१.१	अनलाइन प्रणालीहरूको नियमित सुरक्षण परीक्षण (Security Audit) गर्ने/गराउने।	सूचना प्रविधि विभाग, सम्बन्धित नियामक निकाय	सम्बन्धित प्रणाली सञ्चालक निकाय	निरन्तर		सूचना प्रविधि विभागबाट केही सरकारी अनलाइन प्रणालीहरूको Security Audit भएको।
	६.१.२	सूचना प्रविधि सेवा प्रदायक निकाय तथा संस्थाहरूको वर्गीकरण गरी अनुपालन (compliance) कायम गरे नगरेको यकिन गर्न अनुगमन तथा नियमन गर्ने।	सरोकारवाला तोकिएको निकाय	सञ्चार तथा सूचना प्रविधि मन्त्रालय			System, network र process audit गरी compliancy test र report generation लागि IT विज्ञहरूका लागि hands-on training प्रदान गर्नुपर्ने।

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	६.१.३	सूचना प्रविधि प्रणाली र पूर्वाधारहरूको स्तर नियमित जाँच गराउने, पछिल्लो मापदण्ड अनुरूप भए नभएको परीक्षण गरी अनुपालन सुनिश्चित गर्ने।	सूचना प्रविधि विभाग-(सञ्चार तथा सूचना प्रविधि मन्त्रालय)	प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, गृह मन्त्रालय, अर्थ मन्त्रालय, कानून, न्याय तथा संसदीय मामिला मन्त्रालय	आ.व. २०७९/ ८०		सरकारी निकायहरूले CCMMI प्राप्त गर्ने कार्य चुनौतीपूर्ण रहेको।
	६.१.४	संवेदनशील सूचना प्रविधि प्रणालीहरूको प्रभावकारी अनुगमन गर्ने।	राष्ट्रिय साइवर सुरक्षा अनुगमन केन्द्र	सम्बन्धित प्रणाली सञ्चालक निकाय	निरन्तर		क्षमता विकास आवश्यक (राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं. २.८.१०.१.३.२ र २.८.१०.१.४ तथा राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ६ को (५) सँग सम्बन्धित विषय।
	६.१.५	कर्मचारीहरूको cyber hygiene को अवस्था मुल्याङ्कन गर्ने	सरोकारवाला निकाय	सञ्चार तथा सूचना प्रविधि मन्त्रालय	निरन्तर		
	६.१.६	सूचना प्रविधि क्षेत्रमा क्रियाशील निजी क्षेत्रका संघसस्थाहरूको स्वनियमन तथा अनुपालनामा जोड दिने।	सरोकारवाला निकाय	सञ्चार तथा सूचना प्रविधि मन्त्रालय	निरन्तर		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
६.२ साइबर स्पेशको प्रभावकारी अनुगमन तथा नियमन गर्ने	६.२.१	इन्टरनेट तथा सामाजिक सञ्जालको प्रयोग गरी झुठ्ठा खबर (Fake News) सम्प्रषेण गर्ने कार्यको नियन्त्रण गर्ने।	प्रेस काउन्सिल नेपाल	नेपाल दूरसञ्चार प्राधिकरण, नेपाल प्रहरी	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं २.८.१०.१.१६ र २.८.१०.१.१७ सँग सम्बन्धित
	६.२.२	राष्ट्रिय प्रतिष्ठामा आँच पुऱ्याउने, घृणा द्वेष फैलाउने, अनलाइन उत्पीडन (Online harassment) र साइबर बुलिङ्ग गर्ने, विभिन्न जातजाति र समुदायबीच खलल पुऱ्याउने किसिमको डिजिटल सामाग्रीको सम्प्रषेणमा नियमन तथा नियन्त्रण गर्ने।	साइबर ब्यूरो, नेपाल प्रहरी	राष्ट्रिय अनुसन्धान विभाग, प्रेस काउन्सिल नेपाल,	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं २.८.१०.१.११ र २.८.१०.१.१७ तथा राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ६ को (५) सँग सम्बन्धित विषय
	६.२.३	बालबालिका मैत्री विषयवस्तु , कानूनले वर्जित गरेका आपत्तिजनक विषयबस्तुहरु रहे नरहेको नियमन गरी अनुपयुक्त अनलाइन सेवाहरूमा पहुँच निषेध गर्ने।	नेपाल दूरसञ्चार प्राधिकरण	महिला बालबालिका तथा जेष्ठ नागरिक मन्त्रालय, नेपाल प्रहरी	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं २.८.१०.१.१७ सँग सम्बन्धित
७. साइबर चेतना अभिवृद्धि गर्ने।							

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
७.१ साइबर सुरक्षाको विषयमा जनचेतना अभिवृद्धि गर्ने।	७.१.१	प्रत्येक निकायमा काम गर्ने कर्मचारीहरूलाई साइबर सुरक्षासम्बन्धी जानकारीमूलक कार्यक्रम सञ्चालन गर्ने।	सबै निकायहरू	राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह, सञ्चार तथा सूचना प्रविधि मन्त्रालय, गृह मन्त्रालय, नेपाल दूरसञ्चार प्राधिकरण, नेपाली सेना, नेपाल राष्ट्र बैंक	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७५ को भाग ७ को (८) सँग सम्बन्धित विषय
	७.१.२	साइबर स्पेशमा समसायमिक विषयहरू सम्बन्धमा विषय, घटना, सुरक्षित प्रयोग बारे नागरिकलाई सुसुचित गर्न आवश्यकता अनुसार परामर्श (Advisory) जारी गर्ने।	राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह - NITERT	सञ्चार तथा सूचना प्रविधि मन्त्रालय, गृह मन्त्रालय, नेपाल दूरसञ्चार प्राधिकरण, नेपाली सेना, नेपाल राष्ट्र बैंक, Computer Emergency Response Team (CERT) Community,	निरन्तर		(National Information Technology Emergency Response Team - NITERT)
	७.१.३	ज्येष्ठ नागरिक, बालबालिका, विशेष आवश्यकता भएका व्यक्तिहरूलाई लक्षित गरी कार्यक्रमहरू सञ्चालन गर्ने।	महिला बालबालिका तथा जेष्ठ नागरिक मन्त्रालय	नेपाल प्रहरी, सञ्चार तथा सूचना प्रविधि मन्त्रालय, दूर सञ्चार सेवा प्रदायकहरू, Corporate Social Responsibility (CSR)	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं २.८.१०.१.११ र २.८.१०.१.१७ सँग सम्बन्धित
	७.१.४	विद्यालयस्तरको पाठ्यक्रममा साइबर सुरक्षा सम्बन्धी विषय समावेश गर्ने।	शिक्षा मन्त्रालय	सञ्चार तथा सूचना प्रविधि मन्त्रालय	आ.व. २०७९।८०		

रणनीतिक उद्देश्य	क्रियाकलापहरू		जिम्मेवार निकाय		समयावधि	विद्यमान अवस्था	कैफियत
			मुख्य निकाय	सहयोगी निकाय			
	७.१.५	साइबर सुरक्षा सम्बन्धी जनचेतनामूलक सामाग्रिहरू निर्माण (अडियो भिडियो, ब्रोसर, सहयोगी पुस्तिका, सामाजिक सञ्जालमा पोस्ट आदि) गरी वितरण गर्ने	नेपाल दुरसञ्चार प्राधिकरण, साइबर ब्यूरो, सूचना प्रविधि विभाग	नेपाल प्रहरी, सञ्चार तथा सूचना प्रविधि मन्त्रालय, दूर सञ्चार सेवा प्रदायकहरू, Corporate Social Responsibility (CSR)	निरन्तर		राष्ट्रिय सुरक्षा नीति, २०७३ को कार्यनीति नं २.८.१०.१.११ र २.८.१०.१.१७ सँग सम्बन्धित

अनुसुची १: प्रचलित साइबर/कम्प्यूटर जोखिमका प्राविधिक शव्दाबलीहरू

- Malware: कम्प्युटर, नेटवर्क, सर्भर लगायत ICT (Information and Communication Technology) उपकरण तथा प्रणालीलाई हानि पुऱ्याउने उद्देश्यले सिर्जना गरिएको कुनै प्रोग्राम वा कोडलाई Malware वा Malicious Software (हानिकारक सफ्टवेयर) भनिन्छ। Malware अन्तर्गत viruses, worms, ransomware, trojans, spyware, keyloggers, botnet, cryptojacking, लगायत हानिकारक तरिकाले प्रयोग गरिने सबै प्रकारका सफ्टवेयरहरू पर्दछन्।
- Virus: अरु कम्प्युटर प्रोग्रामहरूलाई परिवर्तन गरी ती प्रोग्राममा आफ्नो हानिकारक कोड संलग्न गर्ने कम्प्युटर प्रोग्रामलाई Virus भनिनछ। परिवर्तन भएको प्रोग्राम सूचना हुँदा Virus पनि सूचना भई अरु प्रोग्रामलाई समेत परिवर्तन गर्दै कम्प्युटरको विभिन्न भागमा आफ्नो प्रतिलिपि बनाउँदै फैलिन्छ र कम्प्युटरको विभिन्न डाटा परिवर्तन गर्छ वा मेटाउँछ।
- Worms: आफ्नो धेरै प्रतिलिपि बनाउँदै एउटा कम्प्युटरबाट अर्को कम्प्युटरमा संक्रमण फैलाउन सक्ने क्षमता भएको हानिकारक कम्प्युटर प्रोग्रामलाई Worm भनिन्छ। Worm लाई सुचारु हुन Virus लाई जस्तो अरु कम्प्युटर प्रोग्राम नचाहिने हुँदा यो अरु Malware भन्दा बढी संक्रामक हुन्छ र यो प्राय कम्प्युटर नेटवर्कबाट सर्दछ।
- Trojan: आवश्यक पर्ने सफ्टवेयरभित्र हानिकारक कोड राखी प्रयोगकर्ताहरूलाई झुक्याइ ICT उपकरणहरूमा सो सफ्टवेयर सूचना गराउने प्रकारको Malware लाई Trojan वा Trojan Horse भनिन्छ। प्रयोगकर्ताले उक्त सफ्टवेयर सूचना गर्दा भित्र रहेको हानिकारक कोड समेत सूचना हुन्छ र यसले ह्याकरलाई प्रयोगकर्ताको गतिविधि तथा संवेदनशील सूचनामा पहुँच प्रदान गर्दछ।
- Spyware: कुनै व्यक्ति वा संस्थाको ICT उपकरणमा प्रयोगकर्तालाई थाहा नै नदिई Install हुने र प्रयोगकर्ताको अनलाइन गतिविधि, संवेदनशील सूचना लगायतका विभिन्न जानकारी सङ्कलन गरी सोको विवरण सम्बन्धित ह्याकरलाई पठाउने सफ्टवेयरलाई Spyware भनिन्छ।
- Ransomware: आधिकारिक प्रयोगकर्ताहरूलाई आफ्नो ICT उपकरण तथा प्रणालीमा पहुँच निषेधित गराई पहुँच पुन: प्राप्त गर्न भुक्तानी वा फिरौती माग्ने Malware लाई Ransomware भनिन्छ। Ransomware बाट कुनै उपकरण वा प्रणाली संक्रमित भएमा यसले हार्ड ड्राइभमा प्रयोगकर्ताको पहुँच पूर्ण रूपमा रोक्छ वा फाइलहरू Encrypt गर्दछ। Ransomware हमलामा प्राय ह्याकरहरूले सजिलै पत्ता लगाउन नसकिने Cryptocurrency मार्फत फिरौतीको माग गर्छन्।

- Ransomware as a Service (RaaS): RaaS मोडेलमा, ह्याकरहरूलाई तेस्रो-पक्षको तर्फबाट Ransomware आक्रमणहरू सञ्चालन गर्न भाडामा लिइन्छ। यस मोडेलबाट जो कोहीले पनि प्राविधिक सीप वा अनुभवबिना साइबर आक्रमण सूचना गर्न सक्दछन्।
- Zero-day Exploit: कुनै पनि ICT उपकरण, प्रणाली वा सेवामा देखिएको नयाँ सुरक्षा जोखिमको Patch जारी गर्नु अघि वा Patch कार्यान्वयन गर्नु अघि नै उक्त सुरक्षा जोखिम मार्फत गरिने साइबर आक्रमणलाई Zero-day Exploit भनिन्छ। कुनै सुरक्षा जोखिम खुलासा हुने बित्तिकै त्यसको समाधान वा निवारक उपायहरू लागू नहुन्जेलको छोटो समायावधिमा Zero-day आक्रमणकारीहरू उक्त सुरक्षा जोखिमको माध्यमबाट विभिन्न साइबर हमलाहरू सूचना गर्न प्रयत्नशील रहन्छन्।
- Keylogger: कम्प्युटरमा प्रयोगकर्ताले किबोर्डमा टाइप गरेको हरेक अक्षरको रेकर्ड राख्ने सफ्टवेयरलाई Keylogger भनिन्छ। ह्याकरहरूले यस प्रकारको सफ्टवेयर लक्षित व्यक्ति वा संस्थाको कम्प्युटरर उपकरणमा प्रयोगकर्तालाई थाहै नदिई Install गर्छन् र प्रयोगकर्ताको कम्प्युटरमा गतिविधि निगरानी तथा पासवर्ड चोरी जस्ता कार्यहरू गर्दछन्।
- Brute Force Attack: ह्याकरहरूले विशेष प्रकारको सफ्टवेयरबाट स्वचालित रूपमा निरन्तर पासवर्डको सम्भावित सबै मिश्रण परीक्षण गरी पासवर्ड पत्ता लगाउन प्रयोग गर्ने विधिलाई Brute Force Attack भनिन्छ। यो विधि प्रयोग गर्दा पासवर्ड जति लामो हुन्छ, परीक्षण गर्न समय त्यति नै बढी समय लाग्छ। पछिल्लो समयमा निर्माण गरिएका आधुनिक कम्प्युटरहरूले ८ वर्णको पासवर्ड Brute Force विधिबाट छिटोमा दुई घण्टाभित्र पत्ता लगाउन सक्छन्।
- Dictionary Attack: ह्याकरहरूले Dictionary मा भएका सम्पूर्ण शब्दहरू तथा ती शब्दहरूसँग प्रचलित मिश्रणहरू (@123, @098, 123#, 2022$, आदि) वा लक्षित व्यक्तिको नाम, जन्म मिति, फोन नं. जस्ता व्यक्तिगत विवरणहरू प्रयोग गरी विशेष प्रकारको सफ्टवेयरबाट स्वचालित रूपमा पासवर्ड अनुमान लगाउने विधिलाई Dictionary Attack भनिन्छ। अरुले अनुमान लगाउन सक्ने विवरण तथा Dictionary मा भएका शब्दहरू भएको पासवर्डलाई ह्याकरहरूले यस विधिबाट सजिलै पत्ता लगाउन सक्छन्।
- Credential Stuffing: विभिन्न समयमा भएका डाटा Breach, Phishing Campaign लगायतका सूचना चुहावटमा सङ्कलन गरिएका करोडौं पासवर्डहरू प्रयोग गरी ह्याकरहरूले विशेष प्रकारको सफ्टवेयरबाट स्वचालित रूपमा पासवर्ड अनुमान लगाउने विधिलाई Credential Stuffing भनिन्छ। अहिले सम्म पासवर्ड Breach भएका विभिन्न कम्पनीका प्रयोगकर्ताले अझै पुरानो पासवर्ड सोही अकाउन्ट वा अन्य अकाउन्टमा प्रयोग गरेमा ती प्रयोगकर्ताहरू यस प्रकारको साइबर हमलाको शिकार हुन सक्छन्।
- Cryptojacking: साइबर अपराधीले गोप्य रूपमा प्रयोगकर्ताहरूको ICT उपकरणमा Crypto currency उत्पादन गर्ने सफ्टवेयर राखी सो Cryptocurrency आफूले आर्जन गर्ने प्रक्रियालाई Cryptojacking

भनिन्छ। यसरी Cryptocurrency उत्पादन गर्दा प्रयोगकर्ताको उपकरणको Processing शक्तिको प्रयोग हुन्छ र Cryptocurrency निषेधित राष्ट्रहरूमा प्रयोगकर्ता कानूनको दायरमा समेत पर्न सक्दछन्।

- Spam: ठूलो संख्यामा सामाजिक सञ्जाल समूह वा प्रयोगकर्ताहरूलाई इन्टरनेट मार्फत पठाइएका अप्रासंगिक वा अनुपयुक्त मेसेजहरूलाई Spam भनिन्छ। यस्ता मेसेजहरूको उद्देश्य प्राय विज्ञापन गर्न, भ्रामक समाचार फैलाउन, जातीय अफवाह फैलाउन, धर्म परिवर्तनका लागि प्रचार गर्न, ठगी गर्न, आदि रहेको हुन्छ।
- Denial of Service (DoS): ICT सेवा वा प्रणाली सञ्चालनमा बाधा पुऱ्याउन झूटा अनुरोधहरू सिर्जना गरि सम्बन्धित नेटवर्कलाई आफ्नो क्षमता भन्दा अधिक भार दिने लक्षित हमलालाई DoS भनिन्छ। DoS हमला सफल भएको अवस्थामा आधकारिक प्रयोगकर्ताहरू इमेल, वेबसाईट, अनलाइन खाता जस्ता नियमित तथा आवश्यक कार्यहरू प्रयोग गर्नबाट बञ्चित हुन्छन्।
- Distributed Denial of Service (DDoS): DoS र DDoS आक्रमणहरू बीचको मुख्य भिन्नता यस आक्रमणको उत्पत्तिसँग सम्बन्धित रहेको हुन्छ। DoS आक्रमण कुनै एक कम्प्युटर उपकरण वा प्रणालीबाट उत्पन्न भएको हुन्छ भने DDoS आक्रमण धेरै कम्प्युटर उपकरण वा प्रणालीहरूबाट सुरु हुन्छ। एकैपटक धेरै उपकरण वा प्रणालीबाट उत्पन्न हुने र सबै उपकरण/प्रणाली पहिचान गर्नुपर्ने हुँदा DDoS आक्रमण DOS आक्रमण भन्दा ब्लक गर्न कठिन हुन्छ।
- Botnet: Botnet वा Bot Network भन्नाले ह्याकरहरूले विभिन्न माध्यमबाट संक्रमण गरी आफ्नो अधीनमा राखेका ICT उपकरणहरूको सञ्जाल बुझिन्छ। ह्याकरहरूले यी कम्प्युटरहरू इन्टरनेटमा जडान भएको अवस्थामा टाढाबाट भौतिक पहुँच बिना नै नियन्त्रण गर्न सक्छन् र यसको माध्यमबाट DDoS हमला गर्न, Spam इमेल पठाउन, अरु साइबर अपराधीलाई भाडामा प्रयोग दिन जस्ता कार्यहरूको लागि प्रयोग गर्न सक्छन्।
- Phishing: आधिकारिक व्यक्ति वा संस्थाको नक्कल पारी इमेल, SMS, Messages, भ्रामक वेबसाइट, विज्ञापन लगायत अन्य विभिन्न आकर्षक लिङ्कहरू मार्फत प्रयोगकर्तालाई झुक्याई वा प्रलोभनमा पारी युजरनेम, पासवर्ड, बैकिंग विवरण, डेबिट/क्रेडिट कार्ड विवरण लगायत अन्य व्यक्तिगत तथा अति संवेदनशील गोप्य जानकारीहरूको चोरी गर्ने प्रयासलाई Phishing भनिन्छ।
- Man in The Middle (MITM) Atttack: ह्याकरले दुर्भावनापूर्ण उद्देश्यले प्रयोगकर्ता र Web Application बिच भइरहेको संवाद पत्ता लगाउने हमलालाई MITM भनिन्छ। MITM आक्रमणको मुख्य लक्ष्य गोप्य रूपमा प्रयोगकर्ताको व्यक्तिगत विवरण, पासवर्ड, बैकिंग विवरण लगायत जानकारी सङ्कलन गर्नु हो। साथै, ह्याकरले उक्त संवादमा Web Application को नक्कल पारी प्रयोगकर्ताबाट थप सूचना हासिल गर्ने वा प्रयोगकर्ताको नक्कल पारी Web Application मा पासवर्ड परिवर्तन गरिदिने, आर्थिक कारोबार गरिदिने, झुटो सूचना फैलाउने जस्ता कार्यहरू पनि गर्न सक्दछन्।

- Cross-Site Scripting (XSS): ह्याकरले कुनै वैध वेबसाइट भित्र हानिकारक कोड राखिदिएर सो वेबसाइट प्रयोगकर्तालाई लक्षित गरी गरिने हमलालाई XSS भनिन्छ। XSS सफल भएको वेबसाइट प्रयोग गर्दा उक्त कोड प्रयोगकर्ताको Web Browser मा हानिकारक Script को रूपमा सुरु हुन्छ र ह्याकरले यसको माध्यमबाट संवेदनशील जानकारी चोरी गर्न, प्रयोगकर्ताको नक्कल गर्न लगायत अन्य विभिन्न दुर्भावनापूर्ण कार्य गर्न सक्दछन्। प्रयोगकर्ताहरूलाई आफ्नो सामग्री पोस्ट गर्न अनुमति दिने Web Forums, Message Boards, Blogs जस्ता वेबसाइटहरू XSS आक्रमणको लागि सबैभन्दा बढि संवेदनशील हुन्छन्।
- SQL (Structured Query Language) Injection: डाटाबेस व्यवस्थापन गर्न प्रयोग गरिने SQL को विभिन्न कमाण्डहरूको प्रयोग गरी ह्याकरले सुरक्षा दृष्टिकोणले कमजोर रहेका वैध वेबसाइटहरूको डाटाबेसमा पहुँच पुर्याउनुलाई SQL Injection भनिन्छ। ह्याकरले वेबसाइटको डाटाबेसमा भण्डारण भएका डाटा परिवर्तन गर्न, चोर्न वा मेटाउन SQL Injection को प्रयोग गर्दछन्। XSS र SQL Injection आक्रमणहरू बीचको मुख्य भिन्नता आक्रमण कसलाई लक्षित गरेर गरिएको हो भन्ने कुरासँग सम्बन्धित रहेको हुन्छ। XSS वेबसाइटको अरु प्रयोगकर्ताहरूलाई लक्षित गरि गरिन्छ भने SQL Injection वेबसाइटको डाटाबेसलाई लक्षित गरी गरिन्छ।
- DNS (Domain Name System) Attack. साइबर अपराधीहरूले DNS मा रहेका सुरक्षा कमजोरीहरू मार्फत गरिने आक्रमणलाई DNS Attack भनिन्छ। DNS को मुख्य कार्य प्रयोगकर्ताहरूले अनुरोध गरेको Website इन्टरनेटबाट खोजी सम्बन्धित प्रयोगकर्तालाई प्रदान गर्नु रहेको हुन्छ। साइबर अपराधीहरूले DNS को सुरक्षा कमजोरीहरू मार्फत भण्डारण गरिएको रेकर्ड फेरबदल गरी प्रयोगकर्ताले कुनै Website अनुरोध गर्दा सोको बदलामा अन्य हानिकारक Website खोलिदिन्छन् र त्यस मार्फत प्रयोगकर्ताको संवेदनशील सूचना सङ्कलन गर्छन्।
- Backdoor: कुनै Virus, Trojan, Rootkit लगायतका Malware को माध्यमबाट ICT उपकरण वा प्रणालीमा प्रयोगकर्ताको जानकारी बिना अनाधिकृत रूपमा निरन्तर पहुँच पुऱ्याउन स्थापना गरिएको प्रवेशद्वारलाई Backdoor भनिन्छ।
- Rootkit: वैध सफ्टवेयरभित्र हानिकारक कोड राखी प्रयोगकर्ताहरूलाई झुक्याइ ICT उपकरणहरूमा डाउनलोड गराउने प्रकारको Malware लाई Rootkit भनिन्छ। प्रयोगकर्ताले उक्त सफ्टवेयर सूचना गर्दा भित्र रहेको हानिकारक कोड समेत सूचना हुन्छ र यसले ह्याकरलाई उक्त उपकरणमा Administrative स्तरको पहुँच प्रदान गर्दछन्।
- Social Engineering: ह्याकरहरूले आधिकारिक निकायको रूपमा प्रस्तुत भई हामीलाई झुक्याई हाम्रो संवदेनशील सूचना हासिल गर्ने अभ्यसालाई Social Engineering भनिन्छ। यस प्रकारको हमला कम्प्युटरबाट मात्र नभई फोन, मेसेज, सामाजिक सञ्जाल र प्रत्यक्ष रुपमै व्यक्तिबाट समेत हुन सक्छ। फोन मार्फत

बैंकको कर्मचारी को नक्कल पारी व्यक्तिगत विवरण अद्यावधिक गर्नुपर्ने भनि संवेदनशील सूचना मागेर हासिल गर्ने, कार्यालय प्रमुखको नक्कल गरी इमेल पठाई कार्यालयको सूचना चुहावट गर्ने, इन्टरनेट मर्मत गर्न आएको नक्कल पारी घर तथा कार्यालयको नेटवर्क उपकरणमा पहुँच पुर्याउने जस्ता उदाहरण केहि प्रचलित Social Engineering अभ्यास हुन्।

- Advanced Persistent Threat (APT): ह्याकर वा ह्याकरहरूको समूह (प्राय: राष्ट्र प्रायोजित) ले ठूला उद्योग, सुरक्षा निकाय तथा सरकारी कार्यालय जस्ता उच्च श्रेणीका अति संवेदनशील निकायहरूको सम्बन्धित ICT उपकरण, नेटवर्क, प्रणाली वा सेवामा दीर्घकालीन उपस्थिति स्थापना गरी गोप्य सूचना हासिल गर्न अज्ञात रूपमा निरन्तर पहुँच कायम राखिने आक्रमण अभियानलाई APT भनिन्छ। प्राय: यस प्रकारको आक्रमण अभियान निकै अनुभवी ह्याकरहरूको समूहले पर्याप्त आर्थिक लगानी मार्फत धेरै सावधानीपूर्वक छानिएका तथा अनुसन्धान गरिएका निकायहरूलाई लक्षित गरी गर्ने गर्छन्। साथै, केही APT हमलाहरू साइबर वारफेयरको निम्ति प्रयोग गरिन्छ र सम्बन्धित राष्ट्रले नै यसलाई आर्थिक सहायता प्रदान गरेको हुन्छ।