मानवअधिकार मैत्री

राष्ट्रिय साइबर सुरक्षा रणनीति

FREEDOM FORUM

मानवअधिकार (सम्मान, संरक्षण र प्रवर्द्धन) मैत्री

राष्ट्रिय साइबर सुरक्षा रणनीति

फ्रिडम फोरम
थापाथली, काठमाडौं, नेपाल
पोष्ट बक्स: २४२९२
फोन: ४१०२०३०/४१०२०२२
इमेल: info@freedomforum.org.np
www.freedomforum.org.np

भदौ, २०७८

साजसज्जा तथा मुद्रण: स्पन्दन डिजाइन कम्युनिकेशन, फोन: ५४३५८८४

भूमिका

सूचना तथा सञ्चार प्रविधि (आइसिटी) मानव सभ्यताको बहुआयामिक विकासको अभिन्न अंग भइसकेको छ । आइसिटीको विकासले मानव जीवनका हरेक क्षेत्रमा प्रभाव पारेको छ । श्रम, शिक्षा, सूचना र मनोरञ्जनका क्षेत्रमात्र नभई सामरिक सुरक्षालगायतका संवेदनशील पक्षमा समेत आइसिटीको भूमिका बढ्दो छ । आइसिटीको विकासले आविस्कार गरेको इन्टरनेट हाम्रो परिवारको एक सदस्य जस्तै भइसकेको छ । त्यसैले इन्टरनेटलाई मानिसको प्रत्येक कृयाकलापसँग जोडिने आधारभूत विषयका रुपमा बुझ्ने गरिन्छ । इन्टरनेटमा पहुँच अब सुविधाको विषयमात्र रहेन । यो अधिकारको पक्ष भएको छ ।

विश्वभरी नै मानवअधिकारको सम्मान, रक्षा र प्रवर्द्धनमा इन्टरनेटको भूमिकाबारे सघन बहस भइरहेका छन् । विश्वव्यापी र बहुआयामिक विशेषता भएको इन्टरनेटको भूमिकाबारे नेपालमा पनि यस्तै बहसको खाँचो छ । स्वतन्त्र, सुरक्षित र खुला इन्टरनेटमा पहुँच हाम्रो वकालतको विषय हो । यसको सदुपयोगबाट मानवअधिकारको रक्षा र प्रवर्द्धन गर्नुपर्ने गम्भीर र विचारणीय पक्षहरु छन् । यसतर्फ गर्नुपर्ने सुधारको काम नेपाली नीति निर्माता, राजनीतिक दलहरु, कर्मचारीतन्त्र, सूचनाप्रविधिका प्राविधिक, नीजिक्षेत्र, कानूनका ज्ञाता र नागरिक समाज सबैको साझा दायित्व पनि हो ।

नेपालमा स्मार्ट फोनको प्रयोगमा बढोत्तरीसँगै इन्टरनेटको पहुँचमा संख्यात्मक वृद्धि भएको छ । नेपाल दूरसञ्चार प्राधिकरणको पछिल्लो रेकर्डअनुसार, नेपालमा इन्टरनेटको विस्तार ९० प्रतिशत पुगेको छ । यो विस्तारसँगै इन्टरनेटका माध्यमहरुबाट सार्वजनिक सरोकारका विषयमाथि दिनहुँ आममानिसका विचार व्यक्त हुने र आपसी संवाद हुने मात्र होइन सरकारले ल्याएका नीति कार्यक्रम र राज्यको कानूनमा समेत डिजिटल स्पेसमा व्यापक छलफल हुन थालेका छन् ।

नेपालमा इन्टरनेटको प्रयोग हुन थालेको २६ वर्ष भएपनि आम मानिसका लागि इन्टरनेट/साइबरस्पेसमा आफ्नो अधिकार कसरी सुरक्षित हुन्छ भन्ने ज्ञानको अभाव छ । कतिपय नागरिक अज्ञानताकै कारणले पनि साइबर अपराधकबाट पीडित हुने गरेका छन् भने इन्टरनेट तथा साइबर स्पेसमा नागरिकका अधिकार कसरी सुरक्षित गर्न सकिन्छ भन्ने ज्ञान कानून तथा नीति निर्माण तहमा पनि कम छ । समाजमा इन्टरनेटको प्रयोग यति धेरै बढिसक्दा पनि सुरक्षित इन्टरनेट निर्माण गर्न केही नीतिगत तथा कानूनी व्यवस्थाहरु गरिएका भए पनि ती प्रबन्धहरु उपयुक्त र पर्याप्त दुवै छैनन् । तसर्थ साइबर सुरक्षाको उचित व्यवस्थापनका लागि बहूपक्षीय पहलमार्फत् नीतिगत तथा कानूनी प्रयास गर्न अब ढिला गर्न हुँदैन ।

एकातिर इन्टरनेट, साइबर सुरक्षाका क्षेत्रमा भएका केही प्रयासहरु छन् र अर्कोतिर डिजिटलस्पेस, इन्टरनेटमा नेपाली नागरिकको बढ्दो पहुँच र उपस्थितिले साइबर सुरक्षा र यसका लागि तय गरिने नीति नियमको मानवअधिकारसँगको अन्तरसम्बन्ध बारेमा पनि बृहत्त छलफल हुनु जरुरी भएको छ। साइबर सुरक्षा तथा इन्टरनेटको क्षेत्र व्यापक भएपनि विशेष गरी नागरिकको अभिव्यक्ति स्वतन्त्रता र गोपनीयताको हक कुण्ठित नहोस् भन्ने कुरा बढी महत्वपूर्ण हुन्छ। राष्ट्रिय साइबर सुरक्षा नीति नियम बनाउने क्रममा राज्यको सुरक्षामा बढी जोड दिँदा नागरिक अधिकार खुम्चिने डर उत्तिकै हुन्छ। एक प्रजातान्त्रिक मुलुकमा जनताका अधिकार कुनै पनि माध्यममा कुण्ठित हुनु हुँदैन -चाहे त्यो अनलाइन होस् वा अफलाइन। त्यसैले समग्र राज्यको सुरक्षा अपनाउँदा तथा सूचना तथा सञ्चारप्रविधि उपकरण र इन्टरनेटको माध्यमबाट हुने अपराध नियन्त्रण गर्दा चालिने कदम कति वैधानिक छन् भन्ने कुराले उत्तिकै महत्व राख्छ। साइबर अपराध नियन्त्रण तथा निर्मूल गर्न चालिने राज्यका कदमले नागरिकको अभिव्यक्ति स्वतन्त्रता तथा गोपनीयतामा कुनै आँच आउनु हुँदैन।

सूचना प्रविधि र इन्टरनेटको सुरक्षा तथा सुरक्षित इन्टरनेटको सहज प्रयोगको अवस्था यी दुवै आयाम साइबर सुरक्षाका पक्षहरु हुन्। अहिले विश्वभरी नै इन्टरनेटको क्षेत्रसँग मानवअधिकारको विश्वव्यापी मान्यता र संवेदनशीलतालाई कसरी स्थापित गर्ने भन्नेबारे अवधारणाहरु र मान्यताहरुमा छलफल चलिरहेको छ। डिजिटलस्पेसमा वा डिजिटल वातावरणमा मानवअधिकारको सम्मान, संरक्षण र प्रवर्द्धनलाई सचेततापूर्वक ध्यान दिनु आवश्यक छ। सूचना प्रविधिका पूर्वाधारहरु संरक्षण एउटा महत्वपूर्ण पाटो हो भनें यसैसँग जोडिने अर्को पाटो इन्टरनेटका माध्यमहरुमा गरिने अभिव्यक्ति, संवाद र सूचना प्रवाहको सुरक्षा हो। राष्ट्रिय साइबर सुरक्षा रणनीतिले सम्बोधन गर्नुपर्ने यिनै दुई पक्षमा यस पुस्तिकामा प्रस्तुत सन्दर्भ सामाग्रीले थप छलफल र बहसलाई दिशाबोध गर्नेछ। मानवअधिकारका अन्तर्राष्ट्रिय सिद्धान्त र संयन्त्रहरुमा व्यक्त प्रतिवद्धता र मान्यताहरुलाई सूचना प्रविधिको विकास र नियमनमा अलग्याउन सकिदैन।

यही सेरोफेरोमा डिजिटल अधिकारको क्षेत्रमा काम गर्ने बेलायती संस्था ग्लोबल पार्टनर्स डिजिटल (Global Partners Digital) ले तयार गरेको मानवअधिकार मैत्री राष्ट्रिय साइबर सुरक्षा रणनीतिसम्बन्धी एक श्रोत सामाग्री हाम्रो सन्दर्भमा निकै उपयोगी हुने देखिएकाले हामीले सो सामाग्रीलाई श्रोत पुस्तिकाको रुपमा प्रकाशन गरेको छौं। यो GPD ले तयार गरेको "Developing National Cybersecurity Strategies which Respect, Protect and Promote Human Rights" शीर्षकको नीतिपत्रको नेपाली अनुवाद हो। यस पुस्तिकामा मानवअधिकार मैत्री (सम्मान, संरक्षण र प्रवर्द्धन) राष्ट्रिय साइबर सुरक्षा राणनीति तयार गर्दा अवलम्बन गर्नुपर्ने उपायका बारेमा विस्तृत चर्चा गरिएको छ। अस्ट्रेलिया, स्वीडेन, युके, डेनमार्क आयरल्याण्ड, संयुक्त राज्य अमेरिकाजस्ता प्रजातान्त्रिक देश तथा विभिन्न विकासोन्मुख र अल्पविकसित देशहरुका राष्ट्रिय साइबर सुरक्षा

रणनीतिले उल्लेख गरेका प्रावधानहरुको प्रसङ्ग खिच्दै र तुलना गर्दै अब निर्माण गरिने साइबर सुरक्षा रणनीति मानवअधिकार मैत्री कसरी बनाउन सकिन्छ भनी यस सामाग्रीले मापदण्ड प्रस्तुत गरेको छ । साइबर सुरक्षा रणनीतिमा हुनुपर्ने अन्तर्वस्तुको साथै रणनीति निर्माणमा के कस्ता सरोकारवालाको सहभागिता हुनुपर्छ र यसमा कुन कुन विषयमा कसरी अन्तर्राष्ट्रिय सहयोग र सहकार्य गर्न सकिन्छ भन्ने पक्ष पनि यहाँ उल्लेख छ ।

नेपालमा साइबर सुरक्षा रणनीतिको मस्यौदा तथा यस क्षेत्रका लागि विभिन्न कानूनहरुका विधेयकहरु छलफलमा आइरहेका बेला यस विषयमा सही रणनीति तयार गर्नका लागि यस पुस्तिकाले निकै मद्दत पुग्ने आशा गरिएको छ । साथै, साइबरस्पेसलाई सुरक्षित र मानवअधिकार मैत्री बनाउन जनस्तरमा बहस अगाडि बढाउन र नीति निर्माण तहका व्यक्तिहरु तथा सांसदहरुलाई पनि नीति तर्जुमा गर्न यसले महत्वपूर्ण ज्ञान प्रदान गर्छ भन्ने फ्रिडम फोरमले ठानेको छ । फ्रिडम फोरम अनलाइन/साइबरस्पेसमा मावनअधिकारमा व्यवधानरहित अभ्यासका पक्षमा छ । यसका लागि यो श्रोत सामाग्री निकै महत्वपूर्ण हुने हामो विश्वास छ ।

यस श्रोत सामाग्रीलाई अनुवाद गरेर मनोज कार्कीले पुऱ्याउनु भएको सहयोगका लागि हार्दिक धन्यवाद छ । साथै यसको अनुवाद गर्न र प्रकाशन एवं वितरणका गर्न अनुमति दिने Global Partners Digital र सो संस्थाका मित्रहरु डोन्जा घोबाडी र डानिला निड्रिग प्रति विशेष आभार व्यक्त गर्दछु । यो प्रकाशनमा साइबर सुरक्षा रणनीति बारेका नेपाली सन्दर्भहरु समेत यसमा प्रस्तुत गर्न र आवश्यक संयोजन गर्नुहुने फ्रिडम फोरमका कार्यक्रम संयोजक सहकर्मी नारायण घिमिरेसहित सहकर्मी आदित्य दाहाल र मञ्जु दाहाल ओझालाई पनि धन्यवाद ज्ञापन गर्दछु ।

तारानाथ दाहाल
प्रमुख कार्यकारी,
फ्रिडम फोरम

विषय प्रवेश:
नेपालमा साइबर सुरक्षा नीति

राष्ट्रिय साइबर सुरक्षा नीतिको मस्यौदा, २०७८

प्रविधि क्षेत्रमा नेपाल ढिलो प्रवेश गरे पनि सूचना तथा सञ्चार क्षेत्रले दुई दशकयता फड्को मारेको छ। यसको विकाससँगै सरकारले विभिन्न समयमा आइसिटीसम्बन्धी नीति, कानून ल्याएको पनि छ। सूचना तथा सञ्चारको नियमनका लागि नीति र कानून धेरै अगाडि देखि ल्याइए पनि विशेषगरी इन्टरनेट र डिजिटल युगका क्रियाकलापसँग प्रत्यक्ष सरोकार राख्ने विषय साइबर सुरक्षासँग सम्बन्धित भएर राष्ट्रिय साइबर सुरक्षा नीतिको मस्यौदा २०७८ असार महिना मात्र सार्वजनिक गरिएको छ । नीतिको मस्यौदामाथि विभिन्न सरोकारवालाहरुको सुझावका लागि मन्त्रालयले आह्वान पनि गरेको छ। यस नीतिको मस्यौदामा १६ परिच्छेद छन् । यसको पृष्ठभूमीमै लेखिएको छ, **"सूचना प्रविधि प्रणालीमा साइबर आक्रमणबाट हुन सक्ने क्षतिलाई रोक्न, न्युनिकरण गर्न र भविष्यमा हुन सक्ने यस्ता आक्रमणबाट सुरक्षित रहन साइबर सुरक्षासम्बन्धी राष्ट्रिय नीति पहिलो पटक तर्जुमा गरिएको छ।"**

नीतिको दीर्घकालीन सोच यसप्रकार छ: "साइबर जोखिमलाई सम्बोधन गर्दै व्यक्ति, व्यवसाय एवं सरकारका लागि भरपर्दो, सुरक्षित एवं लचिलो साइबर स्पेस (resilient cyber space) निर्माण गर्ने।" यस मस्यौदामा चारवटा लक्ष्य निर्धारण गरिएको छ भनें उद्देश्य पनि चार वटै छन् । परिच्छेद ९ मा उल्लेख गरेका चारवटा उद्देश्य यसप्रकार छन्:

- सुरक्षित, भरपर्दो र लचिलो साइबरस्पेस बनाउन एवं यस क्षेत्रमा अन्तराष्ट्रिय मापदण्ड /स्तर कायम गर्न कानूनी तथा नीतिगत व्यवस्थालाई सशक्त बनाउनु। (९.१)
- सूचना एवं सूचना प्रविधि प्रणालीको सुरक्षाको लागि संस्थागत र संगठनात्मक सरचनाहरु निर्माण गर्नु। (९.२)
- साइबरस्पेसलाई सशक्त र सुदृढ बनाउन सुरक्षाका विषयमा जनचेतना बढाउने तथा साइबर सुरक्षा क्षेत्रमा जनशक्ति उत्पादन एवम् कार्यरत जनशक्तिको क्षमता अभिवृद्धि गर्नु। (९.३)
- साइबर सुरक्षा सम्बन्धी विश्वव्यापी जोखिमलाई मध्यनजर गरी त्यस्ता जोखिमहरुका विरुद्ध द्विपक्षीय, क्षेत्रीय तथा अन्तर्राष्ट्रिय मुलुक एवम् संगठनहरुसँग सहकार्य गर्नु। (९.४)

त्यसैगरी परिच्छेद ११ मा कार्यनीतिको व्यवस्था गरिएको छ। यस सम्बन्धी केही सान्दर्भिक बूँदाहरु यसप्रकार छन् ।

- विद्यमान कानूनलाई साइबर सुरक्षा अनुकूल हुने गरी संशोधन, परिमार्जन र पुनरावलोकन गरी समय सान्दर्भिक बनाइने । (११.१)
- साइबर अपराध (cybercrime) एवं सूचना तथा सञ्चार प्रविधिको अपराधिक दुरुपयोग विरुद्ध एवं साइबर सुरक्षा सबलिकरणको लागि कानून निर्माण गरिने । (११.२)
- साइबर सुरक्षा सम्बन्धी अन्तर्राष्ट्रिय अभ्यास समेतका आधारमा न्यूनतम प्राविधिक मापदण्ड (Minimum Technical Standard) निर्माण गरिने । (११.७)
- नेपाली नागरिकका गोपनीयताको हक, सूचनाको हक एवं स्वतन्त्रताको संरक्षण गर्न व्यक्तिगत एवं सामूहिक साइबर सुरक्षाका उपायहरु निर्धारण गरिने । (११.१०)
- व्यक्तिगत वा संस्थागत तथ्यांकहरु संकलन, प्रशोधन, प्रयोग एवं भण्डारण गर्ने निकायहरुमा भएका साइबर आक्रमण तथा प्रयोगकर्ताका डाटा हानी, नोक्सानी, तथा चोरी सम्बन्धी सूचना सार्वजनिक गर्नुपर्ने व्यवस्था गरिने । (११.११)

त्यसैगरी परिच्छेद १० मा उल्लेख गरिएको साइबर सुरक्षा रणनीतिमा निम्न आठ बूँदा उल्लेख गरिएको छ:

- सुरक्षित, भरपर्दो र लचिलो साइबरस्पेस बनाउन आवश्यक कानून एवं मापदण्डहरु निर्माण गरिने, (१०.१)
- सूचना एवं सूचना प्रविधि प्रणाली सुरक्षा गर्न अन्तर्राष्ट्रिय प्रचलन समेतको आधारमा संस्थागत एवं संगठनात्मक संरचनाहरु निर्माण एवम् सुदृढिकरण गरिने, (१०.२)
- साइबर सुरक्षालाई सुदृढ गर्न सवल एवं सुरक्षित प्रविधि, पूर्वाधार र प्रकृयाको व्यवस्था गरिने, (१०.३)
- साइबर सुरक्षा सम्बन्धी दक्ष जनशक्ति उत्पादन गरिने, (१०.४)
- साइबर सुरक्षाको विषयमा जनचेतना अभिवृद्धि गरिने, (१०.५)
- सुरक्षित साइबरस्पेस निर्माणका लागि सार्वजनिक निकाय तथा नीजि क्षेत्रसँग समन्वय एवम् सहकार्य गरिने, (१०.६)
- साइबर सुरक्षालाई सुदृढ गर्न अन्य मुलुक तथा अन्तर्राष्ट्रिय संघ-संगठनहरुसँग समन्वय एवं सहकार्य गरिने, (१०.७)
- सुरक्षित अनलाइन स्पेस निर्माण गरिने । (१०.८)

सूचना तथा सञ्चार प्रविधि नीति, २०७२

यसअघि २०७२ मा नेपाल सरकारले सूचना तथा सञ्चाार प्रविधि नीति ल्याएको थियो, जुन नीति हाल कार्यान्वयनमा नै छ । उक्त नीतिमा पनि साइबर सुरक्षासम्बन्धी विषयहरु उल्लेख गरिएको छ ।

यस नीतिको आवश्यकता किन पऱ्यो भनी औचित्य खिच्दै लेखिएको छ , **"सूचना तथा सञ्चार प्रविधि क्षेत्रमा निरन्तर भइरहेका विकासको यथोचित लाभ लिन वर्तमान नीतिगत र संस्थागत व्यवस्था अपरिहार्य छ । साइबर सुरक्षा, कन्भरजेन्सलगायतका अवधारणको नीतिगत सम्बोधन गर्न**

सकिएको छैन ।...” त्यसैगरी यस नीतिको भावी सोच (vision) मा लेखेको छ, “सूचना तथा सञ्चार प्रविधिको प्रयोगबाट नेपाललाई सूचना तथा ज्ञानमा आधारित समाजमा रुपान्तरण गर्ने” ।

यस नीतिका आठ वटा लक्ष्य छन् भने साइबर सुरक्षाको आवश्यकता बढ्दै गएको उल्लेख गरेको छ ।

त्यसैगरी, नीतिको दफ ११.६.६ मा यस्तो उल्लेख छ, “वौद्धिक सम्पत्तिको अधिकार, गोपनीयता तथा सूचना संरक्षणको क्षेत्रमा विद्यमान समस्या निराकरणका लागि विशेष नियामक व्यवस्था लागू गरिनेछ ।”

यस नीतिको दफा ११.२१ (सूचना तथा सञ्चार प्रविधि प्रयोगमा सुरक्षा र विश्वसनीयता प्रत्याभूती) ले प्रस्तुत गरेका विषय अझ महत्वपूर्ण छन् । ती हुन्:

- नागरिकको सूचनाको गोपनीयता तथा वैचारिक स्वतन्त्रतालगायत अन्य मूल्यहरु प्रवर्धन गर्न समयानूकुल साइबर सुरक्षा, नीति, निर्देशिका निमार्ण गरी लागू गिरनेछ । ११.२१.१.
- सूचना तथा सञ्चार प्रविधिको अवाञ्छित प्रयोगका साथै अनपेक्षित सूचना प्रवाह (Unsolicited Content) निरुत्साहित गर्न दूरसञ्चार कम्पनी तथा इन्टरनेट सेवा प्रदायकहरुलाई प्रशासनिक, प्राविधिक तथा अन्य उपाय अवलम्वन गर्नु पर्ने बाध्यकारी व्यवस्था गरिनेछ । ११.२१.२.
- साइवर अपराधको अनुसन्धान तथा अभियोजन (Prosecution) व्यवस्थामा यथोचित परिमार्जन गर्दै विद्युतीय कारोबार ऐनको पूर्ण कायान्वयन सुनिश्चित गरिनेछ । ११.२१.३.

अर्को दफा १२.२१.४ मा यस नीतिले उपयुक्त सरकारी संयन्त्रको मातहतमा एक साइबर सुरक्षा निकाय (Cyber Security Cell) स्थापना गर्दै साइबर आक्रमण पहिचान, रोकथाम, प्रतिरक्षा लगायतका आयामहरुको प्रभावकारी सम्बोधन हुने व्यवस्था मिलाइने कुरा उल्लेख गरेको छ । यसै सन्दर्भमा सूचना तथा सञ्चार मन्त्रालयमा आपतकालीन कम्प्युटर उद्धार समूह (Computer Emergency Response Team) स्थापना गरी साइबर सुरक्षासम्बन्धी चुनौतीहरुको शीघ्र सम्बोधन हुने व्यवस्था मिलाइने छ भनिएको छ ।

यस सन्दर्भमा सबैभन्दा महत्व राख्ने कानून तर्जुमा प्रक्रियामा पनि छ । त्यो हो सघीय व्यवस्थापिकाको तल्लो सदनमा विचाराधीन रहेको **सूचना प्रविधिको सम्बन्धमा व्यवस्था गर्न बनेको विधेयक, २०७५** । यसले सूचनाप्रविधि क्षेत्रका अनेक आयामलाई एउटै छाता ऐनबाट नियमनको उद्देश्य लिएको छ । विधेयकमा साइबर सुरक्षालगायत विषयमा विभिन्न प्रावधानहरु प्रस्ताव उल्लेख गरको छ ।

सूचना प्रविधिको सम्बन्धमा व्यवस्था गर्न बनेको विधेयक, २०७५

सूचना प्रविधिको सम्बन्धमा व्यवस्था गर्न बनेको विधेयक, २०७५ को प्रस्तावनामै **“साइबर सुरक्षाको समुचित व्यवस्था गरी साइबर अपराधलाई नियन्त्रण गरी सर्वसाधारणको हित कायम गर्न र सामाजिक**

सञ्जालको प्रयोगलाई व्यवस्थित र मर्यादित बनाउने सम्बन्धमा आवश्यक कानूनी व्यवस्था गर्न प्रचलित कानूनलाई संशोधन र एकीकरण गर्न वाञ्छनीय भएकाले" उल्लेख गरिएको छ ।

त्यसैगरी विधेयकको परिभाषा खण्डमा (२.भ.) "साइबर सुरक्षा" भन्नाले– कुनै पनि सूचनाप्रविधिमा आधारित प्रणाली, नेटवर्क र प्रोग्रामलाई डिजिटल आक्रमबाट सुरक्षा भन्ने अभ्यास सम्झनुपर्छ –लेखेको छ ।

यस्तै परिभाषा खण्डको (ल) मा "सूचना" भन्नाले सरकारी निकाय, सार्वजनिक संस्था वा कुनै व्यक्ति तथा संस्थाबाट सम्पादन हुने वा भएको महत्वपूर्ण काम, कारबाही र वा निर्णयसँग सम्बन्धित कुनै तथ्यांक सम्झनु पर्छ ।

यस विधेयकको परिच्छेद १२ मा साइबर सुरक्षासम्बन्धी विशेष व्यवस्था उल्लेख गरेको छ । सो परिच्छेदको दफा ७९ मा संवेदनशील पूर्वाधार तोक्न सक्ने उल्लेख छ । यसअन्तर्गत लेखिएको छ :

नेपाल सरकारले कुनै पनि राष्ट्रिय सुरक्षा, अर्थव्यवस्था, अत्यावश्यक सेवा, आकस्मिक सेवा, स्वास्थ्य वा सार्वजनिक सुरक्षा समेतमा गम्भीर असर पुऱ्याउन सक्ने सूचना तथा सञ्चार पूर्वाधारहरुलाई नेपाल राजपत्रमा सूचना प्रकाशन गरी संवेदनशील पूर्वाधार तोक्न सक्नेछ । (१)

उपदफा १ बमोजिमको संवेदनशील पूर्वाधार सम्बन्धी सुरक्षाको जिम्मेवार निकाय र अन्य व्यवस्था तोकिए बमोजिम हुनेछ । (२)

उक्त विधेयकको परिच्छेद ११ का विभिन्न दफामा सूचना सुरक्षा तथा गोपनीयतासम्बन्धी व्यवस्था प्रस्ताव गरेको छ । यसअन्तर्गत दफा ६७ देखि ७८ गरी ११ वटा दफाहरु छन्, जस्तै वैयक्तिक विवरणको संकलन गर्न नहुने, सूचनाको सुरक्षाको प्रत्याभूति गर्नुपर्ने, तथ्यांक केन्द्र तथा क्लाउड सेवा सञ्चालनसम्बन्धी व्यवस्था, तथ्यांक केन्द्र तथा क्लाउड कम्प्युटर प्रणाली राख्नुपर्ने, विद्युतीय स्वरुपको सूचनालाई क्षति पुऱ्याउने, चोरी गर्न नहुने, विद्युतीय प्रणालीमा रहेको सूचनाको चोरी गर्न नहुनेलगायत प्रावधान छन् ।

त्यसैगरी, विधेयकको परिच्छेद १४ मा सामाजिक सञ्जाल नियमनसम्बन्धी व्यवस्था गरिएको छ, जसमा सामाजिक सञ्जाल दर्ता र नियमन, निर्देशन दिन सक्ने, सामाजिक सञ्जालको प्रयोग, सामाजिक सञ्जालमा सम्प्रेषण गर्न नहुने प्रावधान उल्लेख छन् ।

लामो सययदेखि नागरिक तथा पत्रकारको अभिव्यक्ति र प्रेस स्वतन्त्रता अभ्यसमा नकारात्मक प्रभाव पारिरहेको विद्युतीय कारोबार ऐनको दफा ४७ उल्लेख गर्नु उत्तिकै सान्दर्भिक छ ।

विद्युतीय कारोबार ऐन, २०६३

विद्युतीय स्वरुपमा गैरकानूनी कुरा प्रकाशन गर्नेः (१) कम्प्युटर, इन्टरनेट लगायतका विद्युतीय सञ्चार माध्यमहरुमा प्रचलित कानूनले प्रकाशन तथा प्रदर्शन गर्न नहुने भनी रोक लगाएका सामग्रीहरु वा सार्वजनिक नैतिकता, शिष्टाचार विरुद्धका सामग्री वा कसैप्रति घृणा वा द्वेष फैलाउने वा विभिन्न जात जाति र सम्प्रदायबीचको सुमधुर सम्बन्धलाई खलल पार्ने किसिमका सामग्रीहरु प्रकाशन वा प्रदर्शन गर्ने वा गर्न लगाउने व्यक्तिलाई एक लाख रुपैयाँसम्म जरिबाना वा पाँच वर्षसम्म कैद वा दुवै सजाय हुनेछ। ४७.

(२) कुनै व्यक्तिले उपदफा (१) बमोजिमको कसूर पटक पटक गरेमा त्यस्तो कसूर वापत अघिल्लो पटक भएको सजायको डेढी सजाय हुनेछ।

त्यसैगरी यस ऐनको दफा ४८ मा गोपनीयता सम्बन्धी यस्तो लेखिएको छ, "गोपनीयता भङ्ग गर्नेः यो ऐन वा यस ऐनअन्तर्गत बनेका नियमहरु वा प्रचलित कानूनमा अन्यथा व्यवस्था भएकोमा बाहेक यो ऐन वा यस ऐन अन्तर्गत बनेका नियमहरु अन्तर्गत प्रदान गरिएको कुनै अधिकारबमोजिम कुनै विद्युतीय अभिलेख, किताब, रजिष्टर, पत्रव्यवहार, सूचना, कागजात वा अन्य सामग्रीहरुमा पहुँच प्राप्त गरेको कुनै व्यक्तिले कुनै अनधिकृत व्यक्तिलाई त्यस्तो अभिलेख, किताब, रजिष्टर, पत्र व्यवहार, सूचना, कागजात वा सामग्रीको गोपनीयता भङ्ग गरेमा वा भङ्ग गर्न लगाएमा निजलाई कसूरको मात्रा हेरी एक लाख रुपैयाँसम्म जरिबाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ।"

अन्य

नीतिगत तथा कानूनी व्यवस्थाहरु बाहेक मुलुकको संविधान पछिको प्रमुख कानून मानिने देवानी र फौजदारी संहितामा पनि डिजिटल स्पेसमा हुने कृयाकलाप नियमनका विषय छन्। त्यहाँ रहेका कतिपय प्रावधानहरु अभिव्यक्ति स्वतन्त्रता र गोपनीयताको अधिकार कुण्ठित गर्ने खालका छन्। खासगरी गाली बेइज्जती, सार्वजनिक सुरक्षा र राजद्रोह तथा अपराध दुरुत्साहनसम्बन्धी कसूरमा डिजिटल माध्यमहरुलाई फरक र कडा नियमनका प्रावधानहरु छन्। जसको असर आधारभूत मानवअधिकारमा परेको छ।

नेपालमा साइबरसम्बन्धी नियमनका नियमहरु तर्जुमा गर्दा र साइबर सुरक्षा रणनीति तर्जुमा गर्दा मानवअधिकारको पक्षमा पर्याप्त ध्यान नदिएको माथिका नीति तथा कानूनका उदाहरणहरुले पुष्टी गर्दछ। विद्यमान अवस्थाको विश्लेषण गर्न र थप सुधार गर्न यससम्बन्धी बहस/छलफललाई यस पुस्तिकामा अब प्रस्तुत गरिएको अनुवाद सामाग्रीले सही दिशाबोध गर्न सक्ने आशा गरिएको छ। विभिन्न देशले अवलम्बन गरेका मान्यता र गरिरहेका अभ्यासहरु हाम्रो नीति तर्जुमा प्रकृया र सुधारको अभियानका लागि उपयोगी सन्दर्भ सामाग्री हुनेछन्।

अध्याय १:
परिचय

हरेक राज्यले अन्तर्राष्ट्रिय मानवअधिकार कानूनको पालना गर्दै मानवअधिकारको सम्मान, संरक्षण र प्रवर्द्धन गर्छन् । मानवअधिकारका दायित्वलाई विभिन्न क्षेत्रीय र राष्ट्रिय मानवअधिकारका नीति र कानूनले पनि उल्लेख गर्छन्, महत्व दिन्छन् । यिनीहरूले मानवअधिकारको लागि परिपूरक रुपमा काम गर्दछन् । त्यसैले सरकार तथा राज्यका विभिन्न निकायले विशेष गरी नीति निर्माण गर्दा मानवअधिकारका आयामलाई ध्यान दिनु जरुरी छ । यो कुराले साइबर सुरक्षाका विषयमा बनाईने सार्वजनिक नीतिका सन्दर्भमा पनि उत्तिकै महत्व राख्छ ।

वास्तवमा साइबर सुरक्षा सबल बनाउन राज्य र अन्य निकायले अपनाउने कृयाकलाप र साइबर चुनौतीको सामनासम्बन्धी विषयले मानवअधिकारका विविध पक्षसँग गहिरो र विविधतापूर्ण सम्बन्ध छ । साइबर सुरक्षा सुदृढ गर्नका लागि लिइने उचित कदमले जोकोहीको मानवअधिकारका रक्षामा र साइबर आक्रमणबाट विशेष गरी गोपनीयता र अभिव्यक्ति स्वतन्त्रताको उल्लंघन न्यूनिकरणमा महत्वपूर्ण भूमिका खेल्दछ । तर, अनुचित तरिका जस्तै स्वच्छाचारी निगरानी, सञ्चार दक्खल पुऱ्याउने (intercept) अत्याधिक र अनियन्त्रित अधिकार, साइबर अपराधका अस्पष्ट र व्यापक परिभाषा साइबर सुरक्षाका क्षेत्रभित्र राखिनु पनि मानवअधिकारको गम्भीर उल्लंघन सरह मानिन्छ ।

साइबर सुरक्षा नीतिमा मानवअधिकारको सुनिश्चितताको महत्वको विषयहरुले विषेशगरी उच्चस्तरीय साइबर सुरक्षा प्रक्रियाका रुपमा मान्यता पाएका छन् । अन्तर्राष्ट्रिय सुरक्षाको सन्दर्भमा सूचना तथा दूरसञ्चारका क्षेत्रमा भएका विकास- २०१३, सम्बन्धी यूएन् सरकारी विज्ञ समूहको प्रतिवेदनले उल्लेख गरेको छ, "सूचना तथा सञ्चारप्रविधिको सुरक्षाका लागि राज्यले चाल्ने कदम र मानवअधिकारसम्बन्धी विश्वव्यापी घोषणापत्रमा उल्लेख भएका मानवअधिकार तथा मौलिक स्वतन्त्रताको सम्मान अनिवार्यरुपमा सँगसँगै लैजानुपर्दछ ।"[१] त्यसैगरी साइबरस्पेससम्बन्धी विश्व सम्मेलन- २०१५ समापनपश्चात् जारी भएको अध्यक्षको वक्तव्यमा, "सबै सरोकारवालाहरूले

[१] संयुक्त राष्ट्रसंघ महासभा, अन्तर्राष्ट्रिय सुरक्षाको सन्दर्भमा सूचना तथा दूरसञ्चार क्षेत्रको विकासका लागि सरकारी विशेषज्ञरुको समूह, राष्ट्रसंघीय दस्तावेज ए/६८/९८, २४ जुन २०१३, अनुच्छेद २१

साइबर सुरक्षा नीति निर्माण गर्दा स्वतस्फूर्ततरुपमा शुरुदेखि नै नीतिमा समावेश गरिने विषयवस्तुहरु अधिकारको संरक्षण गर्ने खालका छन् छैनन् र अन्तर्राष्ट्रिय कानून र अन्तर्राष्ट्रिय मानवअधिकारका संयन्त्रसँग मेल खाएका छन् छैनन् सुनिश्चित गर्नुपर्दछ ।"

साइबर चुनौती/जोखिमसम्बन्धी उचित नीतिगत प्रक्रिया अपनाउँदा मानवअधिकारका विभिन्न पक्षमाथि हुने असरबारे ध्यानपूर्वक सोचविचार गर्नु जरुरी छ, जसले गर्दा मानवअधिकारमा हुने जोखिम कम गर्ने मात्र होइन कि मानवअधिकारको प्रवर्द्धन र अभिवृद्धि गर्दछ । यस प्रक्रियामा एउटा जटिल अवस्था भने राष्ट्रिय साइबर सुरक्षा रणनीति निर्माणको दौरानमा देखापर्छ । साइबर जोखिमका विरुद्ध बृहद, समन्वयकारी र प्रभावकारी प्रतिकार्यको सुनिश्चिततामा राष्ट्रिय साइबर सुरक्षा रणनीति निर्माणले महत्व राख्दछ । सन् २०१९ अगष्ट सम्ममा ८० भन्दा बढी राज्यले यस्तो रणनीति निर्माण गरिसकेका छन् ।[२] राष्ट्रिय साइबर सुरक्षा रणनीति निर्माणका लागि विभिन्न सहयोगी सामाग्री उत्पादन भएका छन् । अतः यस रणनीतिले मानवअधिकारको सम्मान, संरक्षण, र प्रबर्द्धन गर्नुपर्ने कुरालाई विशेष महत्व दिइएको पाइन्छ ।अन्तर्राष्ट्रिय दूरसञ्चार युनियन, विश्व बैक, कमनवेल्थ सचिवालय, कमनवेल्थ दूरसञ्चार संगठन र नेटो कोअपरेटिभ साइबर डिफेन्स सेन्टर अफ एक्सेलेन्सले संयुक्तरुपमा तयार पारेको 'साइबर सुरक्षा रणनीति निर्माणको लागि निर्देशिका'[३] ले विशेषरुपमा उदाहरण दिएको छ -

"रणनीतिले मानिसका अफ्लाइनमा रहेका अधिकार अनलाइनमा पनि अनिवार्यरुपमा संरक्षण गर्नुपर्ने तथ्यलाई स्वीकार गर्नुपर्दछ । यसले विश्वव्यापी मानवअधिकार घोषणापत्र, नागरिक तथा राजनीतिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय अभिसन्धी र अन्य सान्दर्भिक बहूपक्षीय र क्षेत्रीय कानूनी दस्तावेजका साथै विश्वव्यापीरुपमा स्वीकृत आधारभूत अधिकारहरूको सम्मान गर्नुपर्दछ ।"

अभिव्यक्ति स्वतन्त्रता, सञ्चारसम्बन्धी गोपनीयता र व्यक्तिगत तथ्यांक संरक्षणमा पनि उक्तिकै ध्यान दिनु जरुरी छ । विशेषगरी साइबर सुरक्षा रणनीतिले स्वेच्छाचारी, अप्रमाणित र गैह्रकानूनी निगरानी, सञ्चार र व्यक्तिगत तथ्यांकमा अवरोध (interception) गर्न मद्दत पुऱ्याउने खालको प्रावधान राख्नुहुदैन ।

व्यक्ति र राज्यका आवश्यकतावीच सन्तुलन कायम गर्दा, निगरानी, सञ्चारमा अवरोध (interception) र व्यक्तिगत तथ्यांक संकलन गर्दा विशेष अनुशन्धान अथवा कानूनी मुद्दामा

---

२ उदाहरणको लागि आइटियूको राष्ट्रिय साइबर सुरक्षा रणनीति भण्डारमा हेर्नुहोस् यहाँ उपलब्ध छ: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

३ राष्ट्रिय साइबर सुरक्षा रणनीति तयारिका लागि गाइडका केही हरफहरुका अतिरिक्त, आइटियूको राष्ट्रिय साइबर सुरक्षा रणनीति गाइड, २०१२, दफा ७.४, एनिशा, साइबर सुरक्षा रणनीतिको मूल्यांकन ढाँचा, २०१४, दफा ३.१.१ र ३.१.५, कमनवेल्थ दूरसञ्चार युनियन, राष्ट्रिय साइबर सुरक्षा रणनीति निर्माणका लागि कमनवेल्थ दृष्टिकोण, २०१५, सिद्धान्त ४ र दफा ४.३, र विश्वव्यापी साइबर सुरक्षा सक्षमता केन्द्र, राष्ट्रका लागि साइबर सुरक्षा क्षमता परिपक्वता मोडेल, २०१६, आयाम ४.१

मात्रै रणनीतिले सुनिश्चित गर्नुपर्छ । जुन कुरा सम्बन्धित अधिकारसम्पन्न राष्ट्रिय निकायबाट र सार्वजनिक, सटीक, बृहद् र विभेदरहित कानूनी संरचनाको आधारमा गरिन्छ । त्यसैगरी ती कार्यको निरीक्षण, प्रक्रियागत सुरक्षा र कानूनी उपचार सुदृढ हुनु जरुरी छ ।

यी आम भनाइका अलावा राष्ट्रिय साइबर सुरक्षा रणनीति (रासासुर) ले मानवअधिकारको सम्मान, संरक्षण र प्रवर्द्धन कसरी गर्ने भन्नेबारे अझै पनि मार्गदर्शनको अभाव छ । यो प्रतिवेदनको उद्देश्य अहिले भइरहेका विभिन्न देशका रणनीतिहरुमा रहेका असल अभ्यास प्रस्तुत गर्दै, रासासुरका संवेदनशील विषयवस्तु अध्ययन गर्दै यस सम्बन्धी मार्गदर्शनमा देखिएको अभावलाई सम्बोधन गर्ने हो, जसले गर्दा यस्तो रणनीतिका अन्तरवस्तुले मानवअधिकारको सम्मान, संरक्षण र प्रवर्द्धन गर्न सहयोग पुग्दछ । यस प्रतिवेदनले रासासुरका विषयलाई जोड दिइरहँदा, यसमा प्रयोग गरिने भाषा रासासुरको प्रभावकारी कार्यान्यवनका लागि चालिने कदम र व्यवहारिक पक्षसँग मेल खानु आवश्यक छ । यो निर्देशिकाले राष्ट्रिय साइबर सुरक्षा रणनीतिले मानवअधिकारको कसरी सम्मान, संरक्षण र प्रवर्द्धन गर्नसक्छ भन्ने कुरामा जोड दिन्छ । यो निर्देशिकामा प्रयोग भएका भाषा र प्रतिवद्धताहरु मानवअधिकारलाई चुनौती दिने खालका छैनन् । कानून र रणनीति कार्यान्वयनसम्बन्धी अधिकारमा प्रयोग हुने भाषा र प्रतिवद्धताले विशेष महत्व राख्छ जस्तै, फौजदारी अपराध, सुरक्षा निकाय र कानून कार्यान्वयन गर्ने निकायको शक्ति (अधिकार) अथवा नीजि क्षेत्रका दायित्वहरू ।

यो निर्देशिकाले साइबर सुरक्षाको क्षेत्रमा ग्लोबल पार्टनर्स डिजिटल (Global Partners Digital) को गहन अनुभव र विशेषगरी रासासुर निर्माणको विषयमा यहाँहरूको ध्यान खिच्छ । यो प्रतिवेदन मुख्यगरी रासासुर निर्माणमा सरकारहरूलाई सहयोग गर्न बनाइए पनि रासासुर निर्माणका प्रक्रियामा सरकारसँग संलग्न हुने विभिन्न जागरुक सरोकारवालाहरूलाई पनि यसबारे वकालत गर्ने उपयोगी मार्गदर्शन हुनेछ ।

अध्याय २:
निर्देशिकाको दृष्टिकोण

(१) राष्ट्रिय साइबर सुरक्षा रणनीतिका अन्तरवस्तु

यस्तो रणनीतिको कुनै एउटा मात्र विशिष्ठ संरचना छैन, नत यसको संरचना अन्तर्गत राखिनु पर्ने विषयवस्तुका बृहद् सूची नै छन् । पछिल्लो परिच्छेदमा रासासुरको ढाँचा तयार गर्न अत्यन्त धेरै प्रयोगमा आएका निम्न छ वटा मार्गदर्शक दस्तावेजहरूलाई हामीले समीक्षा गरेका छौं:

१) राष्ट्रिय साइबर सुरक्षा रणनीति निर्माणका लागि गाइड[४]
२) आइटीयू राष्ट्रिय साइबर सुरक्षा रणनीतिका लागि गाइड[५]
३) एनिसाको राष्ट्रिय साइबर सुरक्षा रणनीति असल अभ्यास गाइड[६]
४) राष्ट्रिय साइब र सुरक्षा रणनीति निर्माणमा कमनवेल्थको दृष्टिकोण (कमनवेल्थ दूरसञ्चार संगठन)[७]
५) विश्व साइबर सुरक्षा क्षमता केन्द्रको साइब र सुरक्षा क्षमता परिपक्वता मोडल[८]
६) माइक्रोसफ्टको राष्ट्रिय साइबर सुरक्षा रणनीति निर्माण[९]

यी माथिका दस्तावेजहरूको समीक्षा पश्चात्, हामीले तीनले रासासुरका लागि सिफारिस गरेका ढाँचाबाट छ वटा महत्वपूर्ण साझा अन्तरवस्तु फेला पार्यौं । यी अन्तरवस्तु भनें यस निर्देशिकामा उल्लेखित संरचनासँग मेल नखान सक्छन् । केही अन्तरवस्तु यस निर्देशिकामा फरक किसिमका शब्दवालीमा छन् अथवा फराकिलो शीर्षक अन्तर्गत राखिएको छ, अथवा अझ स्पस्ट खण्डमा

---

४ अन्तर्राष्ट्रिय दूरसञ्चार युनियन, विश्व बैंक, कमनवेल्थ सचिवालय, कमनवेल्थ दूरसञ्चार संगठन, र नेटो कोअपरेटिभ साइबर डिफेन्स अफ एक्सेलेन्स, राष्ट्रिय साइबर सुरक्षा रणनीति निर्माणका लागि गाइड, २०१८ यहाँ उपलब्ध छ: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

५ आइटीयू राष्ट्रिय साइबर सुरक्षा रणनीतिका लागि गाइड, २०१२, यहाँ उपलब्ध छ: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

६ एनिसाको राष्ट्रिय साइबर सुरक्षा रणनीति असल अभ्यास गाइड, नोभेम्बर २०१६ यहाँ उपलब्ध छ:https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

७ राष्ट्रिय साइबर सुरक्षा रणनीति निर्माणमा कमनवेल्थको दृष्टिकोण (कमनवेल्थ दूरसञ्चार संगठन), २०१५ यहाँ उपलब्ध छ: : https://cto.int/media/fo-th/cyb-sec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf.

८ विश्वव्यापी साइबर सुरक्षा क्षमता केन्द्रको साइबर सुरक्षा क्षमता परिपक्वता मोडल, २०१६ यहाँ उपलब्ध छ:https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf.

९ माइक्रोसफ्टको राष्ट्रिय साइबर सुरक्षा रणनीति निर्माण, २०१३ यहाँ उपलब्ध छ: http://download.microsoft.com/download/b/f/0/bf05da49-7127-4c05-bfe8-0063dab88f72/developing_a_national_strategy_for_cybersecurity.pdf.

विभाजित छन् । जे होस्, विभिन्न निर्देशिकाले सिफारिस गरेका रासासुरका सबै तत्व सम्मिलित छन् । यस प्रतिवेदनको अनुसूचीमा विभिन्न निर्देशिकाले सिफारिस गरेका संरचना र तत्वहरूको समीक्षा गरिएको छ । र, छ मुख्य अन्तरवस्तुसँग तिनीहरूको सम्बन्ध देखाइएको छ ।

सारांशमा छ अन्तरवस्तु यस प्रकार छन्:

१. ढाँचा, दृष्टिकोण, उद्देश्य र परिभाषा (Framing, vision, objectives and definitions):
यस भागमा साइबर सुरक्षासम्बन्धी सरकारको समग्र दृष्टिकोण, साइबर सुरक्षा रणनीतिको उद्देश्य र लक्ष्य अथवा सिद्धान्त र 'साइबर सुरक्षा'जस्ता महत्वपूर्ण शब्दावलीको परिभाषा छन् ।

२. भूमिका र उत्तरदायित्व (Roles and responsibilities):
यस भागमा साइबर सुरक्षा क्षेत्रका विभिन्न निकायको भूमिका र उत्तरदायित्व पर्दछन् । यस भागले त्यस्ता निकायको बारेमा उल्लेख गर्दछ जसको उत्तरदायित्व रणनीति वा राष्ट्रिय साइबर सुरक्षा नीतिको कार्यान्वयन हुन्छ । कार्यान्वयन भने विशेष साइबर सुरक्षा प्राधिकरण मार्फत हुन्छ । त्यसैगरी, यसमा सरकारले सहयोग गर्ने वा मिलेर काम गर्ने निकाय जस्तो कि सार्वजनिक-नीजि सहकार्य मार्फत् नीजि क्षेत्र पनि पर्दछ ।

३.साइबर लचकता (Cyber resilience)
यस भागमा साइबर आक्रमण र साइबर चुनौतीका पूर्वाधार, नेटवर्क, सिस्टम, सूचना तथा प्रयोगकर्ताको सुरक्षाका निम्ति सरकारले चाल्ने कदमबारे विवरण छन् । सरकारका कदम भन्नाले थुप्रै खालका कृयाकलाप पर्दछन् जस्तै, संवेदनशील राष्ट्रिय पूर्वाधारको सुरक्षा, प्राविधिक सुरक्षा उपायहरूको निर्माण तथा सम्बर्द्धन, स्वतस्फूर्त र निरोधात्मक कार्यमा जोड दिने कम्प्यूटरजन्य घटनाको प्रतिकृया समूह (CIRT)को स्थापना र श्रोत व्यवस्था, साइबर सुरक्षा अभ्यास, साइबर सुरक्षाको क्षेत्रमा हुने अनुसन्धान र विकासमा सहयोग र व्यापारी तथा आम मानिसमा साइबर सुरक्षासम्बन्धी सीप र सचेतनाको विकास पर्दछन् ।

४. साइबर घटना प्रतिकार्य (Cyber incident response)
यसले साइबर आक्रमण हुँदा सरकारले लिने कदमलाई यस भागमा राखिएको छ । र, यसमा प्राय सरकारले लिन सक्ने धेरै किसिमका कार्य पर्दछन् जस्तै, आकस्मिक योजनाको निर्माण, स्वतस्फूर्त र निरोधात्मक कार्यमा जोड दिने कम्प्यूटरजन्य घटनाको प्रतिकार्य समूह (CIRT)को स्थापना र श्रोत व्यवस्था, कानून कार्यान्वयन गर्ने निकायलाई साधन र श्रोतको व्यवस्थापन, र साइबर आक्रमणमा परेका आम मानिस र व्यपारीहरूलाई सहयोग जस्ता विषय छन् ।

५. साइबर अपराध (Cybercrime):
यस विषयअन्तर्गत सरकारले साइबर अपराधलाई कसरी सामना गर्छ भन्ने कुरामा जोड दिइन्छ । यसले मुख्यत: साइबर अपराधसम्बन्धी कानूनको निर्माण र कार्यान्वयन तथा सम्बन्धित निकायलाई कानून कार्यान्वयनमा सहयोग गर्ने विषयहरु छन् ।

६. अन्तर्राष्ट्रिय सहयोग (International Cooperation):

यस खण्डले साइबर सुरक्षाका विषयमा सरकारले अन्य सरकारहरू तथा अन्तर्राष्ट्रिय र क्षेत्रीय संगठनहरूसँग कसरी काम गर्छ भन्ने कुरामा प्रकाश पार्दछ । यसमा प्रायजसो साझा साइबर चुनौती सामना गर्न सरकारहरूबीच सहकार्यको विषय छन् । साथै साइबर सुरक्षासम्बन्धी बहस हुने अन्तर्राष्ट्रिय र क्षेत्रीय मञ्चमा सरकारका निश्चित मूल्य र विदेश नीतिका प्राथमिकताको प्रवर्द्धन पनि पर्न सक्छन् ।

यी माथि उल्लेखित सबै विषयवस्तु मानवअधिकारसँग सम्बन्धित भए पनि, हरेक घटकभित्रका प्रत्येक विषय चाहिं सम्बन्धित छन् भन्ने होइन । रासासुरका केही भाग मानवअधिकारको दृष्टिकोणमा धेरै महत्वपूर्ण हुनेछन् भने अन्य केहीको भने केही वा सान्दर्भिकता नै छैन (विशेषगरी सरकारहरूले गर्ने प्रशासनिक व्यवस्था जस्तै विभागहरूबीच आन्तरिक समन्वय) । त्यसकारण, अध्याय ३ मा उल्लेख गरिएका सिफारिसहरूले राज्यका रासासुरका सम्पूर्ण पक्षहरूलाई होइन कि मानवअधिकारसँग स्पष्ट र मजबुत सम्बन्ध भएका पक्ष चाहिं समेट्छन् ।

(२) मानवअधिकारको विश्लेषण

हामीले गरेका विश्लेषण र सिफारिसहरूको आधार हुन्- अन्तर्राष्ट्रिय मानवअधिकार कानून र मापदण्ड, विशेषगरी विश्वव्यापी मानवअधिकार घोषणपत्र (यूडिएच्आर), नागरिक र राजनीतिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय अभिसन्धी (आईसिसिपिआर) र राष्ट्र संघीय सन्धी सम्बन्धी निकायले गरेको यिनीहरूको व्याख्या ।[१०] योग्य अधिकारको हस्पक्षेप वा प्रतिबन्ध गर्न सक्ने उपायहरू नियाल्दा, कानूनी आधारका आवश्यकता प्रयोग गर्ने पूर्ण स्थापित उपागमलाई यहाँ अवलम्बन गरिएको छ । त्यसैगरी राष्ट्र संघीय मानवअधिकार समितिका टिप्पणी नं १६ र ३४ मा उल्लेख गरिए जस्तै वैध उद्देश्य र समानुपातिकतालाई ध्यानमा राखिएको छ ।[११]

(३) असल अभ्यासका उदाहरण समावेश गर्ने क्षेत्र र औचित्य

रासासुरले मानवअधिकारको सम्मान, रक्षा र प्रवर्द्धन कसरी गर्न सक्छ भन्ने मापदण्ड निर्धारण गर्नुका साथै अध्याय ३ मा प्रत्येक मापदण्डका यतिखेर चल्तीमा रहेका असल अभ्यासका उदाहरण पनि समावेश गरेका छौं। कुन उदाहरण समावेश गर्ने भनी निर्धारण गर्न हामीले झण्डै मौजुदा ७० वटा राष्ट्रिय साइबर सुरक्षा रणनीतिमा मापदण्ड प्रयोग गरी हेर्यौं। रासासुरको मापदण्ड पूरा गर्ने उदाहरणको सूचीबाट क्षेत्रीय र राष्ट्रिय सन्दर्भ खिच्दै सबैभन्दा धेरै मापदण्ड पूरा गर्ने उदाहरण छनौट गरिएको छ । तसर्थ यस निर्देशिकामा असल अभ्यासका त्यस्ता सबै उदाहरणमा प्रकाश पारिएका छैन, र यहाँ समावेश गरिएका उदाहरण मात्रै सम्पूर्ण होइनन् ।

---

[१०] यस गाइडको दृष्टिकोण अन्तर्राष्ट्रिय मानवअधिकार कानून र मापदण्डमा आधारित छ भनें अरु क्षेत्रीय मानव अधिकार प्रणालीले अझ बढी मात्रामा संरक्षण गर्न सक्छन् । क्षेत्रीय मानव अधिकार प्रणालीको सदस्य भएका राज्यमा सरकारले राष्ट्रिय साइबर सुरक्षा रणनीति तयार गर्दा राष्ट्रिय साइबर सुरक्षा रणनीतिले ती क्षेत्रीय मापदण्डसँग मेल खाउन् र प्रतिबिम्बत गरुन् भनी सोच्न सक्छ ।

[११] हेर्नुहोस्, विशेष गरी, राष्ट्रसंघीय मानवअधिकार समितिको जेनेरल कमेन्ट नं १६ (१९८८) को अनुच्छेद ३ र ४, र राष्ट्रसंघीय मानवअधिकार समितिको जेनेरल कमेन्ट नं ३४ (२०११) को अनुच्छेद २२

अध्याय ३:
रासासुरमार्फत् मानवअधिकारको सम्मान, संरक्षण र प्रवर्द्धन

(१)ढाँचा, दृष्टिकोण, उद्देश्य र परिभाषाः

मापदण्ड १. क. यो परिच्छेदमा साइबर सुरक्षाको ढाँचा वा साइबर सुरक्षाप्रति सरकारको दृष्टिकोण के हुने जसले साइबर सुरक्षाले मानवअधिकारको संरक्षणमा खेल्ने भूमिकालाई मान्यता दिनुपर्दछ भन्ने कुरा उल्लेख गरिएको छ ।

धेरैजसो रासासुर रणनीतिको ढाँचा र निश्चित क्षेत्राधिकारभित्र सरकारको साइबर सुरक्षाप्रतिको दृष्टिकोणबाट शुरु हुन्छन् । रासासुरको अन्तरवस्तु सिर्जना नगरे पनि साइबर सुरक्षाको ढाँचा निर्माण भनें मानवअधिकारको कोणबाट अत्यन्त महत्वपूर्ण छ । साइबर सुरक्षाको ढाँचा विभिन्न तवरले गर्न सकिन्छ जस्तै राष्ट्रिय सुरक्षा रक्षा गर्न, वा डिजिटल अर्थतन्त्रको प्रर्वद्धनका लागि । यद्यपि मानवअधिकारबारे राज्यको बुझाइ स्पष्ट नभएसम्म र यो साइबर सुरक्षाको अभिन्न अंग नबनेसम्म, यस पछिल्ला सारवान परिच्छेद मानवअधिकारको सम्मान, रक्षा र सम्बर्द्धनमा फितला प्रयास हुनसक्छन् । साइबर सुरक्षाको ढाँचा निर्माण गर्ने, सरकारको दृष्टिकोण तयार गर्ने (वा दुवै) रासासुरको परिच्छेदले साइबर सुरक्षाले व्यक्तिको मानव अधिकारको संरक्षण गर्नु पर्ने भूमिकालाई स्पष्टरुपमा मान्यता दिइनुपर्छ ।

युरोपेली युनियन : युरोपेली युनियनको साइबर सुरक्षा रणनीति (२०१३) को सिद्धान्तमा निम्न कुरा उल्लेख गरिएको छः
"मौलिक अधिकार, अभिव्यक्ति स्तवन्त्रता, व्यक्तिगत तथ्याङ्क र गोपनीयताको संरक्षण"
साइबर सुरक्षा यदि युरोपेली युनियनको आधारभूत अधिकारको वडापत्र र इयूको मूल मूल्यमा उल्लेखित आधारभूत अधिकार र स्वतन्त्रतामा आधारित हुन्छ भने त्यो भरपर्दो र प्रभावकारी हुन्छ । पारस्परिकरुपमा, सुरक्षित नेटवर्क र प्रणाली बिना व्यक्तिका अधिकार सुरक्षित हुनसक्दैनन् । (पेज ४)

ग्रीसः ग्रीक रासासुर (२०१८) को परिचयमा यस्तो उल्लेख छः
"खुला र स्वतन्त्र इन्टरनेटमा पहूँच, गोपनीयता, अक्षुण्णता, उपलब्धता र सूचना तथा सञ्चार प्रविधि, सम्बृद्धि र राष्ट्रिय सुरक्षाका मात्र होइन आधारभूत अधिकार र स्वतन्त्रताका पनि आधार हुन् ।" (पेज ४)

स्विडेनः स्विडेनको रासासुर (२०१७) मा लेखिएको छः
"खुला प्रजातान्त्रिक समाज सूचनाको व्यवस्थापनमा अपेक्षित गोपनीयता, प्रामाणिकता र उपलब्धता कायम गर्नसक्ने क्षमतामा आधारित हुन्छ । यसको अर्थ सूचनाको भण्डार र स्थानान्तर गर्दा सूचना र प्रणाली दुवै अनिवार्य सुरक्षित हुनुपर्छ । अन्ततः साइबर सुरक्षा भनेको आधारभूत मूल्य र उद्देश्य, जस्तै- प्रजातन्त्र, मानवअधिकार र स्वतन्त्रता, स्विडेनको स्वतन्त्रता, सुरक्षा र स्वायत्तताको अधिकार, आर्थिक बृद्धि र आर्थिक स्थायित्वको जगेर्ना गर्नु नै हो ।" (पेज ५)

मापदण्ड १. ख. साइबर सुरक्षाको उद्देश्य मध्ये एक वा सिद्धान्तमध्ये एक जसले सम्बन्धित राज्यको क्षेत्रकाधिकार संविधानको अधीनमा रही मानवअधिकारको सम्मान, संरक्षण र प्रम्वर्द्धन गर्न आधार तय गर्छ ।

धेरै राष्ट्रिय साइबर सुरक्षा रणनीतिले तिनका विभिन्न उच्चस्तरीय उद्देश्यसम्बन्धी एउटा परिच्छेद समावेश गर्छन् । मानवअधिकार संरक्षणमा साइबर सुरक्षाको भूमिकाको स्पष्ट मान्यता मानवअधिकारका संरक्षण सुनिश्चित गर्ने निश्चित उद्देश्यसँग पूरक हुनुपर्दछ । यस किसिमको उद्देश्यले रासासुर कार्यान्वयनको जिम्मेवार व्यक्ति/निकायलाई मानवअधिकारका सबै किसिमका कार्य र गतिविधिमा पर्ने प्रभाव विचार गर्न मद्दत गर्छ र साथै रासासुरको सफलता मापन गर्न मानवअधिकारमा पर्ने असर सुदृढ बनाउँछ । अन्य केही रणनीतिहरुले पनि विभिन्न सिद्धान्तको उल्लेख गरेका छन् । जसले उपयुक्त रासासुरलाई टेवा पुऱ्याउँछन् । साइबर सुरक्षा रणनीतिमा एउटा सिद्धान्त यो पनि हुनुपर्छ जसले राज्यको अन्तर्राष्ट्रिय, क्षेत्रीय वा राष्ट्रिय मानवअधिकारका दायित्वहरु पनि मेल खानुपर्दछ ।

मापदण्ड १. ग. मानवअधिकारले र अन्तर्राष्ट्रिय असल अभ्याससँग मेल खाने साइबर सुरक्षाको परिभाषा रणनीतिमा समावेश गर्नुपर्छ ।

चिली: चिलीको रासासुर (२०१७) मा मानवअधिकारसम्बन्धी नीति उद्देश्यमा नै छ:
"मौलिक अधिकारको सम्मान तथा सम्वर्द्धन
नीतिका सबै उपायहरुमा तिनीहरूको मौलिक प्रकृति, अविभाज्यता, साइबरस्पेस र भौतिक अवस्थामा मानिसका अधिकार एकै किसिमका हुन्छन् भन्ने आधारलाई जोड दिई रणनीति तर्जुमा र कार्यान्वयन हुनुपर्दछ।" (पेज १९)

अस्ट्रिया: अष्ट्रियन रासासुर (२०१३) को सिद्धान्तहरु मध्येको एक सिद्धान्तमा लेखिएको छ:
"कानूनको शासन: साइबर सुरक्षाका क्षेत्रको गभर्नेन्सले कानूनको शासनको उच्च मापदण्ड पूरा गर्नैपर्छ र मानवअधिकारसँग मेल खानु पर्दछ- विशेषगरी गोपनीयता र तथ्यांक संरक्षण तथा अभिव्यक्ति स्वतन्त्रता र सूचनाको हकका सम्बन्धमा।" (पेज ७)

मानवअधिकार राष्ट्रिय साइवर सुरक्षा रणनीतिको ढाँचा र उद्देश्यको एक भाग हुनुको साथै साइबर सुरक्षाका कुनै पनि परिभाषा (र, यदि सही भए साइबर अपराध) सान्दर्भिक अन्तर्राष्ट्रिय असल अभ्याससँग मेल खानु पर्छ। (जस्तो कि, फ्रिडम अनलाइन कोएलिसन (Freedom Online Coalition) को वर्किङ ग्रुप १ को साइबर सुरक्षाको परिभाषा।) [१२]

(२) भूमिका र उत्तरदायित्व

मापदण्ड २ क. रासासुरको कार्यान्वयन गर्दा निजी क्षेत्र, प्राविधिक समुदाय र नागरिक समाजलगायत सबै सरोकारवाला समूहका प्रतिनिधि सम्मिलित हुनुपर्छ।

प्रचलित कुनै पनि साइबर सुरक्षा रणनीतिले मानवअधिकार र अन्तर्राष्ट्रिय असल अभ्याससँग पूर्णरुपले मेल खानेगरी साइबर सुरक्षाको परिभाषा गरेका छैनन्। अत: यहाँ उल्लेख गरिएको उदाहरण रासासुरबाट लिइएको होइन तर फ्रिडम अनलाइन कोएलिसन को वर्किङ् ग्रुप १ ले निर्माण गरेको हो।

"साइबर सुरक्षा भनेको नीति, प्रविधि र शिक्षाको माध्यमबाट सूचना प्रविधि र यसका अन्तर्निहित पूर्वाधारको उपलब्धता, गोप्यता र अक्षुण्णताको संरक्षण हो जसले मानिसको अनलाईन र अफलाइन सुरक्षा सबल बनाउँछ।"

[१२] हेर्नुहोस्, फ्रि एण्ड सेक्युयर, अनलाइन उपलब्ध छ: https://freeandsecure.online/definition/.

साइवर सुरक्षा भनेको कुनै एक पक्षको मात्र बचाउ होइन । कुनै राज्यमा साइबर सुरक्षा सुनिश्चित गर्न सरकारले महत्वपूर्ण भूमिका खेले पनि नीजि क्षेत्र, प्राविधिक समुदाय र नागरिक समाजको पनि यसमा विशेष भूमिका हुन्छ ।

मानवअधिकारको दृष्टिकोणबाट नागरिक समाजको भूमिका विशेषगरी महत्वपूर्ण हुन्छ । अन्तर्राष्ट्रिय मानवअधिकार कानूनअन्तर्गत आफ्नो कार्यक्षेत्रभित्र मानवअधिकारको सम्मान, संरक्षण र प्रवर्द्धन गर्नु राज्यको दायित्व हो । यद्यपि, नागरिक समाजमा मानवअधिकारको विशेसज्ञता हुन्छ र राज्यका साइबर सुरक्षासम्बन्धी गतिविधिमा हुने यसको संलग्नताले मानवअधिकारको सम्मान, रक्षा र सम्वर्द्धनको परिणाम ल्याउने सम्भावना धेरै हुन्छ । अतः रासासुरको तर्जुमामा यी विभिन्न सरोकारवालाहरुको सहभागिताको बावजुद पनि राणनीतिको कार्यान्वयनमा पनि नागरिक समाज लगायतका सरोकारवाला निकायहरूको संलग्नता हुनुपर्दछ ।

माल्टा: माल्टाको रासासुर (२०१६)को निर्देशक सिद्धान्तमा यस्तो उल्लेख गरेको छ:

"साइबरस्पेसको व्यापक प्रकृतिले अनिवार्यरुपमा राष्ट्रिय स्तरमा र माल्टा बाहिर पनि सुरक्षाप्रति बहूसरोकारवाला दृष्टिकोणको आवश्यकता औंल्याउँछ । तसर्थ, राष्ट्रियस्तरमा, सार्वजनिक, नीजि क्षेत्र, शैक्षिक जगत र नागरिक समाजलगायतका विभिन्न निकायहरूको सहयोग र सहकार्य आवश्यक छ ।" (पेज १२)

यो रासासुरले यसको कार्यान्वयनसम्बन्धी परिच्छेदमा लेख्छ:

"रणनीतिको कार्यान्वयनमा सार्वजनिक र नीजि क्षेत्रका बहुसरोकारवालाहरूको संलग्नता र नागरिक समाजसँग सहकार्य र समन्वय अपेक्षा गरिएको छ ।" (पेज ३१)

(३) साइबर लचकता

मापदण्ड ३. क. साइबर लचकता प्रबर्द्धन गर्ने उपाय अवलम्बन गर्दा वैधानिकताको सिद्धान्तप्रति सुस्पष्ट प्रतिवद्धता हुनुपर्दछ ।

मापदण्ड ३. ख. साइबर लचकता प्रबर्द्धन गर्ने उपाय अवलम्बन गर्दा समानुपातिकताको सिद्धान्तप्रति सुस्पष्ट प्रतिवद्धता हुनुपर्दछ ।

साइवर लचकता प्रत्याभूति गर्ने जिम्मेवारी रहेका राज्यका निकायका पदाधिकारीहरुको मानवअधिकारको संरक्षणमा अहम् भूमिका हुन्छ । सरकारमा निहित व्यापक निगरानी अधिकार जस्तो कि कानून कार्यान्वयनका निकायलाई इन्स्क्रिप्सन (encryption) को प्रयोगमा प्रतिवन्धको

अनुमतिले सुरक्षा र व्यक्तिको सञ्चारको अनुगमन गर्न र साइबर असुरक्षा रोक्न सजिलो हुन्छ। तर, यस्तो जिम्मेवारीले व्यक्तिको मानवअधिकार विशेषगरी अनलाइन दुनियामा गोपनीयता र अभिव्यक्ति स्वतन्त्रताको अभ्यासमा अत्यन्त खराब असर पर्दछ।

यद्यपि, राज्यले साइबर असुरक्षाको चुनौतीप्रति लचकता बृद्धि गर्न संभाव्य विभिन्न उपायहरू अवलम्बन गर्न सक्छ र यी राज्यपिच्छे फरक-फरक हुनसक्छन्। साइबर असुरक्षाप्रति लचकता बृद्धि गर्न बनाइने रणनीतिले अन्तर्राष्ट्रिय मानवअधिकारको सिद्धान्त विशेष गरी वैधताको सिद्धान्त (जस्तै, ती उपायहरू राष्ट्रिय कानूनले अधिकार दिएको क्षेत्रमा मात्रै) र समानुपातिकता (जस्तै, मानवअधिकारमा नकारात्मक असर पार्ने उपायहरू जो वैधानिक उद्देश्यको अनुपातमा हुनेछन् जुन ती उपायहरूको पुस्ट्याइमा प्रयोग हुनेछन्।) सँग मेल खानुपर्छ।[१३]

माल्टा: माल्टाको रासासुर (२०१६) को निर्देशक सिद्धान्तका रुपमा लेखिएको छ -

"युरोपेली युनियनको साइबर सुरक्षा दृष्टिकोण राष्ट्रिय विधानमा उल्लेखित मौलिक अधिकार र स्वतन्त्रताको सम्मान र प्रबर्द्धन गर्नेछ। सम्पूर्ण प्रक्रियाहरूले आवश्यकता, समानुपातिकता र वैधताको सिद्धान्तसँग मेल खाने छ, जहाँ जबाफदेहीता र समाधान सुनिश्चित गर्ने उचित रक्षक हुनुपर्छ।" (पेज १२)

पारागुए: पारागुएली रासासुर (२०१७)ले सिद्धान्तका रुपमा उल्लेख गर्छ:

"समानुपातिकता: अवलम्वन गरिने उपाय/प्रक्रिया प्रर्याप्त, आवश्यक र समानुपातिक हुनुपर्छ जसले मौलिक अधिकार विशेषगरी आत्मियता, गोपनीयताको अधिकार, अभिव्यक्ति स्वतन्त्रता र संगठनको स्वतन्त्रताको सम्मान गर्छ, र यी राज्यका उच्चतम प्राथमिकता हुन्।" (पेज २२)

मापदण्ड ३. ग.सरकारले बनाउने साइबर सुरक्षा रणनीतिले काउन्सिल अफ् युरोप कन्भेन्सन १०८, गोपनीयताका लागि ओइसिडि (OECD)को निर्देशिका र अन्य अन्तर्राष्ट्रिय असल अभ्यासँग मेल खाने गरी सरकारलाई उचित, समानुपातिक र प्रभावकारी तथ्यांक संरक्षण सम्बन्धी कानून निर्माण गर्न प्रतिवद्ध गराउनुपर्छ।

[१३] गोपनीयताको हक र अभिव्यक्ति स्वतन्त्रताको हकको सम्बन्धमा नागरिक तथा राजनीतिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय अनुबन्धको व्याख्याका लागि राष्ट्रसंघीय मानवअधिकार समितिले विकास गरेको वैधानिकता र अनुपातिकताको सिद्धान्त हेर्नुहोस् जेनेरल कमेन्ट नं. ३४, दफा १९: विचार तथा अभिव्यक्ति स्वतन्त्रताको अधिकार राष्ट्रसंघीय दस्तावेज. हेर्नुहोस् –सीसीपीआर/सी/जीसी/३४, १२ सेप्टेम्बर २०११, अनुच्छेद २२

मापदण्ड ३. घ. बढी जोखिममा रहेको समूह जस्तै बालबालिका, वृद्धबृद्धा र अशक्त व्यक्तिहरूको सुरक्षामा विशेष जोड दिदै आवश्यकताअनुसार डिजिटल साक्षरता र जनताको सुरक्षा अभिबृद्धि गर्ने स्पष्ट प्रतिबद्धता हुनुपर्दछ ।

त्यतिमात्र होइन, राज्यको साइबर लचकता बृद्दि गर्न दुईवटा निश्चित उपायहरू अवलम्बन गर्नुपर्दछ जसले विषेशगरी व्यक्तिको मानवअधिकारमा सकारात्मक प्रभाव पार्दछन्: पहिलो, यदि यस अघि छैन भने, काउन्सिल अफ् युरोप कन्भेन्सन १०८ र ओइसिडीको गोपनीयताको संरक्षण र व्यक्तिगत तथ्यांकको सीमापार प्रवाहसम्बन्धी निर्देशिका र अन्तर्राष्ट्रिय असल अभ्यासका आधारमा

ग्याटेमाला: ग्वाटेमालाको रासासुर (२०१८) मा उल्लेख छ:

"मानवअधिकारका अन्तर्राष्ट्रिय महासन्धीअनुसार गोपनीयता र तथ्यांक संरक्षणसम्बन्धी कानून निर्माण गर्न, अनुमोदन गर्न र कार्यान्वयन गर्न" (पेज ३६)

अस्ट्रेलिया: अस्ट्रेलियन रासासुर (२०१६) को जनतामा साइबर सुरक्षा सीप निर्माण गर्ने भन्ने दफामा उल्लेख छ:

सरकार सम्पूर्ण अष्ट्रेलियाली जनताको सुरक्षित अनलाइनका लागि दीगो, राष्ट्रिय सचेतना निर्माण अभियानका विभिन्न गतिविधि गर्ने उद्योगी, अनुशन्धाता र नागरिक समूहसँग सहकार्य गर्नेछ । यस कार्यक्रमले अष्ट्रेलियाली जनतालाई साइबर चुनौतीमा पर्ने वास्तविक असर र यसले कसरी हाम्रो वर्तमान र भविष्यको सम्बृद्धिमा असर पार्छ भन्ने शिक्षा दिनेछ ।" (५५)

डेनमार्क: डेनिस रासासुर (२०१८) ले निम्न प्रतिवद्धता र पहलहरू उल्लेख गरेको छ -

"बालबालिका र युवाहरूमा डिजिटल न्याय र डिजिटल सीप ।

शैक्षिक प्रणालीमा बालबालिका, युवा र शिक्षकहरूमा सुरक्षा चुनौतीबारे सचेतना अभिबृद्धिका संयुक्त प्रयासको शुरुवात गरिने छ । थप शैक्षिक तथा तालिम कार्यक्रमका साथै शिक्षक र विद्यार्थीलक्षित साइबर र सूचनासम्बन्धी शैक्षिक सामाग्री निर्माण र सचेतनाका अभियान जारी राखिनेछन् ।

साइबर र सूचना सुरक्षाका विषयमा आम नागरिक, व्यवसायी र सार्वजनिक निकायलाई सचेत बनाउने

एउटा सूचना पोर्टल निर्माण गरिनेछ जहाँ सहज पहूँचमा भएका सूचना र सल्लाह हनेछन् । साथै, नागरिक, उद्यमी र अन्य निकायहरूका लागि सूचना सुरक्षा र तथ्यांक संरक्षणका साथै मौजुदा कानूनसँग कसरी मेल खाने सूचनाहरु बनाउने भन्ने बारेमा विशिष्ट उपायहरू उपलब्ध हुनेछन् । पोर्टलका सामाग्री गतिशील र आधुनिक ज्ञानले निरन्तर अद्यावधिक हुनेछन् ।" (पेज ३२)

उचित, समानुपातिक र प्रभावकारी तथ्यांक संरक्षण कानून निर्माण, र दोश्रो, डिजिटल साक्षरता र आवश्यकअनुसार बालबालिका र बृद्धबृद्धालगायत जोखिममा रहेका समूहलाई विशेष ध्यान दिई आम नागरिकको सुरक्षा ।

(४) साइबर दुर्घटना प्रतिकार्य

मापदण्ड ४.क. साइबर दुर्घटना प्रतिकार्यका लागि चालिने कदमले वैधताको सिद्धान्तप्रति सुस्पष्ट प्रतिवद्धता जनाउनुपर्छ ।

मापदण्ड ४.ख.साइबर दुर्घटना प्रतिकार्यका लागि चालिने कदमले समानुपातिकताको सिद्धान्तप्रति सुस्पष्ट प्रतिवद्धता जनाउनुपर्छ ।

साइबर दुर्घटना भएपछि राज्यले गर्ने गरेको प्रतिकार्यले मानवअधिकारमा ठूलो असर पार्न सक्छ । जस्तो कि इन्टरनेटको नेटवर्क बन्द भयो वा प्रतिबन्ध गरियो भनें त्यहाँका व्यक्तिको सूचनाको स्वतन्त्रताको अधिकारका मूल तत्व मानिने सञ्चार, सूचना प्रवाह र खोज गर्ने क्षमतामा कटौति हुन्छन् ।

राज्यले साइबर दुर्घटनामा विस्तृतरुपमा चाल्ने कदमका बारेमा नीतिमा विरलै उल्लेख गरिन्छ । यद्यपि रासासुरले साइबर दुर्घटनामा चालिने कदम अन्तर्राष्ट्रिय मानवअधिकारको सिद्धान्त विशेष

कोसोभो: कोसोभोको रासासुर (२०१५) को निर्देशक सिद्धान्तमा लेखिएको छ -

"संवैधानिकता र वैधताको सिद्धान्त- साइबर सुरक्षा सबल बनाउन लिइने कदम कोसोभो रिपब्लिकको संविधान, मौजुदा कानून र अन्तर्राष्ट्रिय सन्धिका प्रावधानहरूमा आधारित हुनुपर्छ ।" (पेज १३)

माल्टा: माल्टाको रासासुर (२०१६) को निर्देशक सिद्धान्तले उल्लेख गरेको छ -

"साइबर सुरक्षाप्रतिको दृष्टिकोणले युरोपेली युनियन र राष्ट्रिय विधानले उल्लेख गरेका मौलिक अधिकार र स्वतन्त्रताको सम्मान र प्रवर्द्धन गर्नेछ । सम्पूर्ण कार्यले जवाफदेहीता र समाधानको सुनिश्चितताका लागि उचित संरक्षणसहितको आवश्यकताको सिद्धान्त, समानुपातिकताको सिद्धान्त र वैधताको सिद्धान्तसँग मेल खाने छन् ।"(पेज १२)

पारागुए: पारागुएको रासासुर (२०१७) को सिद्धान्तले उल्लेख गरको छ -

"समानुपातिकता: अवलम्बन गरिने कार्यहरू राज्यका उच्चतम् प्राथमिकतामा रहेका मौलिक अधिकार विशेषगरी घनिष्ठताको गोपनीयताको अधिकार, अभिव्यक्ति स्वतन्त्रता र संगठनको स्वतन्त्रताको सम्मान गर्न पर्याप्त, आवश्यक र समानुपातिक हुनुपर्छ ।" (पेज २२)

गरी वैधताको सिद्धान्त (जस्तै, ती उपायहरू राष्ट्रिय कानूनले अधिकार दिएको क्षेत्रमा मात्रै) र समानुपातिकताको सिद्धान्त (जस्तै, मानवअधिकारमा नकारात्मक असर पार्ने उपायहरू जो वैधानिक उद्देश्यको अनुपातमा हुनेछन् जुन ती उपायहरूको पुस्ट्याइमा प्रयोग हुनेछन् ।) सँग मेल खानुपर्ने मान्यता राख्छन् ।

(५) साइबर अपराध

मापदण्ड ५.क. यदि रणनीतिले साइबर अपराधको परिभाषा गरेको छ भनें, त्यो परिभाषा मानवअधिकार र अन्तर्राष्ट्रिय असल अभ्याससँग तादात्म्य हुनुपर्दछ ।

मापदण्ड ५.ख. रणनीतिले बुढापेष्ट महासन्धी (Budhapest Convention)**सँग मेल खाने गरी सरकारलाई उचित, समानुपातिक र प्रभावकारी साइबर अपराधसम्बन्धी कानून निर्माणका लागि प्रतिवद्ध बनाउनु पर्दछ ।**

रासासुरमा उल्लेख गरिने 'साइबर अपराध'को परिभाषा महत्वपूर्ण पक्ष हो । यसले मानवअधिकार र अन्तर्राष्ट्रिय असल अभ्याससँग मेल खानु पर्छ । साइबर अपराधको सम्बोधन गर्न विशेष गरी कानूनमार्फत् चालिने कदमले अर्थ राख्दछ । अपराधसम्बन्धी विधानले साइबर अपराध सामना गर्न उचित, समानुपातिक र प्रभावकारी सहयोग पुऱ्याउनुका साथै मानिसलाई साइबर चुनौतीबाट रक्षा गर्दै मानवअधिकारको संरक्षण गर्दछ । यद्यपि, साइबर अपराधसम्बन्धी विधानले मानवअधिकारलाई नकारात्मक असर पनि पार्न सक्छ । निश्चित कार्य वा व्यवहारको अपराधीकरण

यूके: बेलायतको रासासुर (२०१६) ले दुई किसिमका साइबर अपराधको उल्लेख गरेको छ -

"साइबर निर्भर अपराध (Cyber dependant crime) - यी अपराधहरू सूचना तथा सञ्चार प्रविधिका उपकरणको प्रयोगमार्फत् मात्रै हुन्छन्, जहाँ उपकरण अपराधको माध्यम र लक्ष्य दुवै हुन्छन् (जस्तै आर्थिक लाभका लागि मालवयरको निर्माण गर्नु र फैलाउनु, तथ्यांक चोर्न, गडबड गर्न र तथ्यांक वा नेटवर्क वा कुनै गतिविधि नष्ट गर्नु)

र साइबरप्रबर्द्धित अपराध (Cyber enabled crime)- यी परम्परागत अपराध हुन् जुन कम्प्युटर, कम्प्युटर नेटवर्क वा सूचना तथा सञ्चार प्रविधिका कुनै स्वरुप (जस्तो साइबरको सहयोगले हुने ठगी र तथ्यांकको चोरी) को प्रयोगबाट बृद्धि हुन्छन्, फैलिन्छन् ।" (पेज १७)

बङ्गलादेश: साइबर अपराधसम्बन्धी बङ्गलादेशी रासासुर (२०१४)मा लेखिएको छ:

"राष्ट्रिय साइबर अपराध कानून साइबर अपराधसम्बन्धी बुढापेष्ट कन्भेन्सन (२००१) का प्रावधानअनुरुप तर्जुमाका लागि सिफारिस गरिएको छ ।" (पेज ५)

आयरल्यान्ड: आइरिस रासासुर (२०१५)को साइबरअपराधसम्बन्धी दफामा यस्तो उल्लेख छ:

"न्याय तथा समानता मन्त्रीले केही समयमै साइबर अपराधसम्बन्धी बुढापेष्ट महासन्धी र सूचना प्रणालीमाथि हुने हमलाको विरुद्धमा इयूको निर्देशिकाका प्रावधानअनुरुप विधेयक प्रस्तुत गर्नुहुने छ ।" (पेज १४)

आफैंमा मानवअधिकारमाथि प्रतिबन्ध हो । वैकल्पिकरुपमा, असमानुपातिक सजायसहितको निश्चित अपराध वा फौजदारी अपराधको अति बृहद् परिभाषाले मानवअधिकारमा प्रतिबन्ध लगाउन सक्छ । राष्ट्रिय साइबर सुरक्षा रणनीतिमा भन्दा पनि छुट्टै विशेष कानूनमा अपराधबारे उल्लेख हुनसक्ने हुँदा रासासुर आफैंले चाहिं बुढापेष्ट महासन्धीलगायतका अन्तर्राष्ट्रिय असल अभ्याससँग मेल खानेगरी उचित, समानुपातिक, र प्रभावकारी अपराध संहितामार्फत् साइबर अपराधको सामना गर्नुपर्छ ।

(६) अन्तर्राष्ट्रिय सहयोग

मापदण्ड ६.क.: स्वतन्त्र, खुला र सुरक्षित इन्टरनेटको प्रबर्द्धन राज्यको परराष्ट्र नीतिको एक भाग हुनुपर्ने कुरामा स्पष्ट प्रतिवद्धता हुनुपर्दछ ।

मापदण्ड ६.ख.: इन्टरनेट गभर्नेन्समा बहूसरोकारवाला दृष्टिकोण राज्यको परराष्ट्र नीतिको एक भाग हुनुपर्ने कुरामा स्पष्ट प्रतिवद्धता हुनुपर्दछ ।

मापदण्ड ६.ग.: साइबरस्पेसमा राज्यको व्यवहार अन्तर्राष्ट्रिय कानूनले निर्दिष्ट गरेबमोजिम हुन्छन् भन्ने सिद्धान्तप्रति स्पष्ट प्रतिवद्धता हुनुपर्छ ।

मापदण्ड ६.घ. यस्ता अन्तर्राष्ट्रिय र क्षेत्रीय मञ्च र नीति निर्माणका ठाउँ पहिचान गर्नुपर्दछ जहाँ साइबर सुरक्षासम्बन्धी सहयोग मिल्छ र परराष्ट्र नीतिलाई अघि बढाउन सकिन्छ ।

राष्ट्रिय साइबर सुरक्षा रणनीतिले मुख्यगरी राष्ट्रियस्तरमा लिइने कदममा जोड दिन्छ । तर, साइबरस्पेसको विश्वव्यापी प्रकृतिले धेरै चुनौतीहरू/असुरक्षाहरू विश्वव्यापी प्रकृतिका हुने अर्थ राख्छ जसले धेरै र प्रायः सबै राज्यलाई नै असर गर्छ । रणनीतिको ढाँचा निर्माण गर्दा होस् वा सहकार्य गर्दा होस्, प्रतिकार्य सामान्यतया विश्वव्यापी वा क्षेत्रीय सन्दर्भमा निर्माण गरिन्छ । अतः रणनीतिहरुले यस्ता माध्यमको उल्लेख गर्छन् जसले सरकार साइबर सुरक्षाका विषयमा अन्य राज्यहरूसँग काम गर्न चाहन्छ भन्ने स्पष्ट गर्दछ ।

विश्वव्यापी तहमा होस् वा क्षेत्रीय, राज्यहरूवीच राखिने सामूहिक दृष्टिकोणले राष्ट्रिय तहमा लिइने प्रयासहरुले पनि मानवअधिकारमा असर पार्न सक्छन् । यो कुराले विशेषगरी राज्यहरूले सामूहिक रुपमा संयुक्त ढाँचा निर्माण गर्दा ती अन्तर्राष्ट्रिय कानूनको रुपमा जस्तै सन्धी, गैह्रबाध्यकारी दस्तावेज वा अनौपचारिक प्रयासहरू हुन्छन् कि हुदैनन् भन्नेमा महत्व राख्छ । यस्तो ढाँचाले अन्तर्राष्ट्रिय मापदण्डको निर्धारण गर्न सक्छन् वा राज्यहरूलाई राष्ट्रिय स्तरमा कुनै कार्य गर्न प्रतिवद्ध गराउँछन् ।उदाहरणको लागि, साइबर सुरक्षा र तथ्यांक संरक्षणसम्बन्धी अफ्रिकन युनियन महासन्धीले आम सिद्धान्तमा धेरै छुट दिएको छ- "सार्वजनिक चासो" को आधारमा भन्दै प्रयोगकर्ताको सहमतिबिना व्यक्तिगत तथ्यांक सङ्कलन वा प्रयोग गर्नु हुदैन । यस्तो धेरै छुट तथ्यांकको गोपनीयताको अधिकारसँग मेल खाँदैन । वुढापेष्ट कन्भेन्सनको अनुमोदन आवश्यक छ जसले राज्यलाई राष्ट्रिय तहमा यसका प्रावधानहरू कार्यान्वयनका लागि बाध्यकारी बनाउँछ ।

त्यसकारण, जसरी राष्ट्रिय तहमा नीति निर्माण गर्दा र कुनै कदम लिंदा रासासुरले मानवअधिकारको सम्मान, संरक्षण र प्रवर्द्धन गर्नुपर्दछ, त्यसैगरी विश्वव्यापी र क्षेत्रीय संरचनाबारे पनि सुस्पष्ट प्रतिबिम्वित गर्नुपर्छ । यी कुरा यसरी गर्नुपर्दछः

- स्वतन्त्र, खुला र सुरक्षित इन्टरनेटको प्रवर्द्धन राज्यको परराष्ट्र नीतिको एक भागको रुपमा समावेश गर्ने स्पष्ट प्रतिवद्धता,

- इन्टरनेट गभर्नेन्समा बहूसरोकारवाला दृष्टिकोण पररा्ष्ट्र नीतिको एक भागको रुपमा समावेश गर्ने स्पष्ट प्रतिवद्धता,
- साइबरस्पेसमा हुने राज्यको व्यवहार अन्तर्राष्ट्रिय कानूनले निर्दिष्ट गरेवमोजिम पररा्ष्ट्र नीतिको एक भागका रुपमा समावेश गर्ने स्पष्ट प्रतिवद्धता,
- सान्दर्भिक अन्तर्राष्ट्रिय र क्षेत्रीय मञ्च तथा नीति निर्माण गर्ने ठाउँको पहिचान गर्ने जहाँ साइबर सुरक्षामा सहयोग हुन्छ र पररा्ष्ट्र नीतिको प्रवर्द्धन गरिन्छ ।

अस्ट्रेलिया: अस्ट्रेलियाली रासासुर (२०१६) ले विश्वव्यापी उत्तरदायित्व र प्रभावसम्बन्धी दफामा यस्तो लेखेको छ:

"अस्ट्रेलियाले वाक् स्वतन्त्रता, गोपनीयताको हक र कानूनको शासनका मूल्यको आधारमा सदैव खुला, स्वतन्त्र र सुरक्षित इन्टरनेटको वकालत गरेको छ । इन्टरनेटको सेन्सरसिपको विरोध गर्दै अस्ट्रेलियाले इन्टरनेटले सबैलाई प्रदान गर्ने अवसरको प्रवर्द्धन जारी राख्नेछ ।"

अस्ट्रेलियाली रासासुर (२०१६) ले देशको अन्तर्राष्ट्रिय साइबर संलग्नतालाई निर्देशन गर्ने दुइवटा मुख्य सिद्धान्त यसरी लेख्छ:

"हाल जसरी सरकार जत्तिकै समान साझेदारको रुपमा नीजि क्षेत्र र समुदायलाई सहभागी गराएर इन्टरनेटको व्यवस्थापन (गभर्न) गरिएको छ, त्यो नै अत्यन्त प्रभावकारी मोडेल हो । इन्टरनेटको बहुसरोकारवाला व्यवस्थापन/नियमन (governance)ले मौलिक मानवअधिकार जस्तै अभिव्यक्ति तथा गोपनीयताको हक बीच सन्तुलन कायम गर्दै आर्थिक लाभ र सामाजिक अवसर प्रदान गर्दछ ।"

साइबरस्पेसमा राज्यको व्यवहार अन्तर्राष्ट्रिय कानूनले निर्धारण गर्छ । जुन कुरा द्वन्द्वको खतरा कम गर्ने राज्यको मान्यता एवं व्यवहारिक विश्वास निर्माण गर्ने उपायले सुदृढ गरिन्छ ।" (पेज ४१)

स्विडेन: स्वेडिस रासासुर (२०१७) को उद्देश्यमा लेखिएको छ:

"साइवर सुरक्षामा अन्तर्राष्ट्रिय सहयोग, स्वतन्त्रता र मानवअधिकारको सम्मान गर्ने उद्देश्य सहितको विश्वव्यापी, पहूँचयोग्य, खुला र सबल इन्टरनेटको एक अंशको रुपमा सुदृढ गरिने छ । (पेज २४)

स्वेडिस रणनीति अगाडि लेख्छ:

स्वतन्त्रता र मानवअधिकारको सम्मान गर्ने विश्वव्यापी, पहूँचयोग्य, खुला र सबल इन्टरनेट नै सरकारको इन्टरनेटको विकासको लक्ष्य हुन्छ। (...)

खुला, स्वतन्त्र र सुरक्षित इन्टरनेटमा पहूँचले मानवअधिकार, प्रजातन्त्र, कानूनको शासन र विकासको विश्वव्यापी बृद्धिका लागि महत्वपूर्ण संयन्त्र निर्माण गर्छ। मानिसहरूलाई सञ्चार, अन्तरक्रिया गर्न, आफ्ना विचार व्यक्त गर्न र आफ्ना इच्छालाई अन्तर्राष्ट्रियकरण गर्न नयाँ मार्ग त्यो हदसम्म प्रशस्त गर्छ, जुन यस अघि सम्भव थिएन। सूचना र ज्ञानमा बढ्ने पहुँचले लैङ्गिक समानताको अभिवृद्धि गर्छ। डिजिटल रुपान्तरण र सूचना प्रविधिको विकास सामाजिक तथा आर्थिक विकासको बढ्दो औजार हो- कम्तिमा गरिब मानिस, महिला र उनीहरूको अवसरको स्वतन्त्रता सिर्जनाका लागि मात्र होइन कि शिक्षा, अर्थ, कृषि, स्वास्थ्य र वातावरणका विकाससम्बन्धी समस्या नयाँ किसिमले समाधान गर्नका लागि पनि।(पेज २४ र २६)

स्वेडिस रासासुर थप्छ:

"साइबरस्पेसमा अन्तर्राष्ट्रिय कानून लागू हुने कुरा राष्ट्र संघमा सैद्धान्तिरुपमा सहमति छ, तर नियमको एकरुपमै व्याख्या सुनिश्चित गर्ने कुरामा भनें धेरै कठिनाइ र चुनौतीहरू छन्। यस पृष्ठभूमिमा, राज्यको उत्तरदायी व्यवहारका लागि साइबरस्पेसमा अन्तर्राष्ट्रिय कानूनको व्याख्या र प्रयोग, तथा स्वेच्छिक अन्तर्राष्ट्रिय मापदण्ड र विश्वास निर्माणको संभावनका बारेमा अन्तर्राष्ट्रियस्तरमा बहस भइरहेका छन्। उत्तरदायित्व प्रमाणित गर्न, तोक्न र माग गर्नका लागि अन्तर्राष्ट्रिय नियमन, मापदण्ड र सम्झौताको प्रयोग गर्ने सम्भावनाको सन्दर्भमा पनि बहस छ। सरकारले यी छलफल र प्रक्रियामा स्विडेनले दिने सक्रिय प्रयासको महत्वमा जोड दिन्छ। यी प्रयासको उद्देश्य द्वन्द्व रोक्नु र राज्यको उत्तरदायी व्यवहारका लागि मापदण्डमा अन्तर्राष्ट्रिय सहमतिका लागि सहयोग गर्नु हो। (पेज २५)

संयुक्त राज्य अमेरिका: अमेरिकाको रासासुर (२०१८)मा लेखिएको छ:

"अमेरिकाले अन्तर्राष्ट्रिय कानून र उत्तरदायी राज्यका व्यवहारसम्बन्धी स्वैच्छिक गैह्रबन्धनकारी मूल्यको पालन गर्दै साइबरस्पेसमा राज्यको उत्तरदायी व्यवहारको ढाँचाको प्रवर्द्धन गर्ने छ। जुन कुरा शान्तिको समयमा र दुर्भावनापूर्ण साइबर गतिविधिबाट

सिर्जित खतरालाई कम गर्न व्यवहारिक विश्वास आर्जनका लागि लागू हुन्छन् । यी सिद्धान्तहरूले यस ढाँचासँग बेमेल राख्ने अनुत्तरदायी राज्यका कार्यहरुको प्रतिवाद गर्न सहयोगी प्रतिकार्यको आधार पनि तयार गर्दछ ।" (पेज २०)

अमेरिकाको रासासुरको उद्देश्यमध्येको एकमा लेखिएको छ -

"खुला, अन्तरसञ्चालित (interoperable), विश्वसनीय र सुरक्षित इन्टरनेटको प्रवर्द्धन गर्ने

विश्वव्यापी इन्टरनेटले औद्योगिक क्रान्तिपछि केही ठूला प्रगति ल्याएको छ, जसले वाणिज्य, स्वास्थ्य, सञ्चारक्षेत्र र अन्य राष्ट्रिय पूर्वाधारले फड्को मारेको छ । अर्कोतिर, शताब्दीयौ देखिका मानवअधिकार र मौलिक स्वतन्त्रताका संघर्षहरू अहिले अनलाईनमा हुन्छन् । अभिव्यक्ति स्वतन्त्रता, शान्तिपूर्ण सभा र संगठन साथै गोपनीयताको अधिकार असुरक्षित भएका छन् । अभूतपूर्व विकासका बावजुद इन्टरनेटको आर्थिक र सामाजिक क्षमता अनलाइन सेन्सरसिप र दमनले कमजोर भइरहेको छ । अमेरिका खुला, अन्तरसञ्चालित (interoperable), विश्वसनीय र सुरक्षित इन्टरनेट प्रवर्द्धन गर्ने आफ्नो सिद्धान्तमा दृढ छ । हामी खुला इन्टरनेटप्रति हाम्रो दृष्टिकोण अन्तर्राष्ट्रिय मापदण्ड हुने कुरा सुनिश्चित गर्न काम गर्छौं ।र, हामी इन्टरनेटलाई राजनीतिक खतराका रुपमा लिई स्वतन्त्र र खुला इन्टरनेटलाई सर्वसत्तावादी वेब बनाई सुरक्षा वा आतंकवादको भेषमा आफ्नो नियन्त्रणमा राख्ने अधिनायकवादी राज्यहरूलाई रोक्छौं । (...)

खुलापन र स्वतन्त्रता कमजोर पार्ने, नवप्रवर्तनमा बाधा पुऱ्याउने, र इन्टरनेटको कार्यक्षमतालाई जोखिममा राख्ने राज्य केन्द्रित ढाँचा निर्माणको विरुद्ध अमेरिका इन्टरनेट गभर्नेन्समा बहुसरोकारवाला मोडेलको सुनिश्चित गर्ने विश्वव्यापी प्रयासमा सक्रियरुपमा सहभागी भइरहनेछ । इन्टरनेटको बहूसरोकारवाला मोडेल भन्नाले पारदर्शी, वटमअप, सहमतिमा आधारित प्रक्रिया हुन् जसले सरकार, नीजि क्षेत्र, नागरिक समाज, शैक्षिक जगत् र प्राविधिक समुदायलाई समान हिसाबले भाग लिन सबल बनाउँछ । अमेरिकी सरकारले बहूपक्षीय र अन्तर्राष्ट्रिय मञ्चमा इन्टरनेटको खुला र अन्तरसञ्चालित (interoperable) विशेषताको पक्ष लिन्छ । यो पक्षमहत्वपूर्ण संगठनहरू जस्तै आइक्यान (Internet Corporation for Assigned Names and Numbers), इन्टरनेट गभर्नेन्स फोरम, यूएन् र अन्तर्राष्ट्रिय दूरसञ्चार युनियनमा गहन सक्रिय संलग्नताका लागि हुन्छ ।" (पेज २४, २५)

फ्रिडम फोरम अनुसन्धान एवं वकालतकर्ता प्राज्ञिक समुदायको साझा पहल हो। लोकतन्त्र, मानवअधिकार, प्रेस स्वतन्त्रता र राष्ट्रको समविकासमा समर्पित रहने उद्देश्यले २०६२ सालमा यसको स्थापना भएको हो । मानव स्वतन्त्रताको उच्चतम मूल्यप्रति प्रतिवद्ध पत्रकार, कानुन व्यवसायी, मानव अधिकारकर्मी, प्राध्यापक-शिक्षक, समाजशास्त्री तथा विकास कार्यकर्ताहरुको साझा मञ्चका रूपमा यो फोरम स्थापना गरिएको हो । प्रेस तथा अभिव्यक्ति स्वतन्त्रता, सूचनाको हक, वजेट पारदर्शिता, निर्वाचन तथा लोकतान्त्रिक शासन प्रणाली, सार्वजनिक वित्त व्यावस्थापन र सामाजिक जवाफदेहिता प्रवर्द्धनका गतिविधिमार्फत आम जनतालाई लोकतन्त्रको प्रतिफल प्राप्त गर्ने अवस्थामा पुऱ्याउन यो संस्था प्रयासरत छ । समुन्नत लोकतान्त्रिक समाज यसको लक्ष्य हो । मुलुकका विभिन्न क्षेत्रमा छरिएर रहेका स्वतन्त्रताका पुजारीहरु यसका सदस्य वन्न सक्छन् । नागरिक समाज, आमसञ्चार, पेसागत क्षेत्र र तल्लो तहका सामुदायिक संगठनसँग सहकार्य गरेर अगाडि वढ्ने हाम्रो नीति रहेको छ । सम्पुर्ण स्वतन्त्रता मानव सभ्यताको अनन्त चाहना हो । स्वतन्त्रताभन्दा मूल्यवान अरू केही छैन भन्ने फ्रिडम फोरम ठान्छ ।

फ्रिडम फोरम

थापाथली, काठमाडौं, नेपाल

पोष्ट बक्स: २४२९२

फोन: ४१०२०३०/४१०२०२२

इमेल: info@freedomforum.org.np

www.freedomforum.org.np