२८ जेठ २०७८

माननीय मन्त्रिज्यू,
सूचना तथा संचार प्रविधि
सिंहदरवार, काठमाडौं ।

विषय: राय, सुझाव तथा पृष्ठपोषण उपलब्ध गराएको बारे

सूचना प्रविधिको विकासले मानव सभ्यताको प्रत्येक क्षेत्रमा प्रभाव पारेको छ । यसको प्रयोग नेपालमा पनि दिनानुदिन बढ्दै गएको छ । नेपाल दुरसंचार प्राधिकरणको फागुन २०७७ को रिपोर्ट अनुशार भ्वाइस फोनको प्रयोग एक सय तेत्तिस प्रतिशत छ भने ब्रोडब्याण्ड सेवा सताशी प्रतिशत छ । नेपाल राष्ट्र बैंकको गत महिना (वैशाख, २०७८) को तथ्यांक अनुशार इन्टरनेट बैंकिंङ सेवा एघार लाख भन्दा बढी, मोबाइल बैंकिंग सुबिधा एक करोड पैंतीस लाख भन्दा बढी र बैंकिंग कार्ड सेवा लिने एघार लाख भन्दा बढी व्यक्तिहरुले प्रयोग गरिरहेका छन् । नेपालमा करिब चालिस लाख व्यक्तिहरु डिजिटल वालेट प्रयोग गर्छन । विश्व ब्यांकको २०१७ को तथ्यांक अनुशार नेपालमा ६६ अरब रुपियाँको सूचना तथा संचार साधन सामग्री आयात भएको देखिन्छ जुन समग्र आयातको पाँच दशमलव दुई प्रतिशत हो । धेरै जसो सरकारी, गैर सरकारी संघ संस्था व्यापारिक प्रतिष्ठाणहरुले इन्टरनेटमा उपस्थिति जनाइसकेका छन भने आफ्नो सेवाहरु प्रदान गर्न डिजिटल प्रविधिको प्रयोग गर्दै छन । हालै मात्र नेपाल सरकारको पच्चिस भन्दा बढी संस्थाहरुको सूचनाहरु नेपाल सरकारको एकिकृत डाटा सेन्टरको डाटा भण्डारमा आबद्ध भएका छन् । यस तथ्यांकलाइ आधार मान्ने हो भने पनि नेपालमा उच्च स्मार्ट फोनको प्रयोग तथा प्रविधिमा बढ्दो पहुचँ र प्रविधि अनुकुलताको आंकलन गर्न सकिन्छ । यस्तै गरि सूचना प्रविधिको प्रगतिशील विकासको साथसाथै साइबर अपराधका विभिन्न समस्याहरु देखिदै आएको छ । सूचना प्रणालीमा अनधिकृत पहुँचको समस्या, गोपनीयता र अन्य धेरै मुद्दाहरु दिन प्रतिदिन बृद्धि हुँदैछन् र त्यसको लागि नितिगत तथा प्राविधिक रुपमा तयार हुन पर्ने अवस्था आएको छ ।

कुनै पनि कानुन तर्जुमा गर्दा सरोकारवालाहरुसँगको छलफल महत्वपूर्ण हुन्छ । यसै सन्दर्भमा तहाँ संचार र सूचना प्रविधि मन्त्रालयले मिति २०७८।०२।२८ गते भित्र सरोकारवालाहरुलाई राय, सुझाव तथा पृष्ठपोषणकोलागि मिति २०७८।०२।१४ गते एक सूचना सहित मस्यौदा सार्वजनीक गरेको थियो । यस मान्यतालाई आत्मसात गर्दै इन्टरनेट गभर्नेन्स इन्स्टीच्यूट, डिजिटल राइट्स नेपाल र फोरम फर डिजिटल इक्वालीटीको आयोजना तथा सेन्टर फर साईबर सेक्युरिटि रिसर्च एण्ड इनोभेसन, इन्फर्मेशन सेक्युरिटी रेस्पोन्स टिम नेपाल (एनपीसर्ट), डिजिटल मिडिया फाउण्डेशन, डेल्टा ल फर्म, नेपाल इन्टर्नेट फाउन्डेसन र मिडिया एक्शन नेपालको सहआयोजनामा मिति २०७८ जेठ २३ गते जुममा आधारित सरोकारवालाहरु समक्ष छलफल संचालन गरेका थियौं ।

अधिवक्ता बाबुराम अर्याल, अधिवक्ता सन्तोष सिग्देल र अधिवक्ता टंकराज अर्यालको प्रारम्भिक विश्लेषण तथा मिति २०७८ जेठ २३ गतेको सरोकारवाला छलफलमा प्राप्त सुझाव समेतलाई समेटेर यो टिप्पणी सहितको सुझाव तयार गरी पेश गरिएको छ। यस टिप्पणीले सूचना प्रविधिको नयाँ युग सापेक्ष राष्ट्रिय साईबर सुरक्षा नीति बन्न सघाउ पुर्याउने विश्वास लिइएको छ । यस समिक्षा तथा सरोकारवाला छलफलमा उपस्थित सबैलाई धन्यवाद दिन चाहन्छौं ।

मन्त्रालयले आवश्यक ठानेमा हामी सरोकारवालाहरु थप छलफलको लागि उपलब्ध हुने नै छौं ।

धन्यवाद ।

भवदीय,

अधिवक्ता सन्तोष सिग्देल
अध्यक्ष
डिजिटल राइट्स नेपाल

सुरज अधिकारी
महासचिव
फोरम फर डिजिटल इक्वालिटी

अधिवक्ता बाबुराम अर्याल
संस्थापक/निर्देशक
इन्टरनेट गभर्नेन्स इन्स्टीच्यूट

प्रा.डा. सुवर्ण शाक्य
अध्यक्ष
सेन्टर फर साइबर सेक्युरिटी रिसर्च एण्ड इनोभेसन

चिरन्जिवी अधिकारी
अध्यक्ष
इन्फर्मेशन सेक्युरिटी रेस्पोन्स टिम (एनपीसर्ट)

डा. बलराम प्रसाद राउत
अध्यक्ष
डेल्टा ल फर्म

प्रवेश सुवेदी
अध्यक्ष
डिजिटल मिडिया फाउन्डेशन

विक्रम श्रेष्ठ
अध्यक्ष
नेपाल इन्टरनेट फाउन्डेशन

लक्ष्मणदत्त पन्त
अध्यक्ष
मिडिया एक्सन नेपाल

# राष्ट्रिय साईबर सुरक्षा नीति २०७८ को समिक्षा

## कार्यकारी साराँश

साईबर सुरक्षा सम्बन्धी राष्ट्रिय नीति यथासम्भव चाडो तर्जुमा गरी कार्यान्वयन गर्न आवश्यक रहेको हालको सन्दर्भमा प्रस्तावित मस्यौदा एक महत्वपूर्ण पहल हो । अहिले सम्म नेपालमा नितिगत तथा कानुनी रुपमा साइबर सुरक्षाको क्षेत्राधिकार विद्युतिय कारोवार ऐन, २०६३ को अधीनमा रहेको छ । तर परिष्कृत साइबर आक्रमण र साइबर अपराधका नविनतम तथा विकसित साइवर अपराध एवंम आक्रमणका मुद्दाहरूलाई यस ऐनले राम्रोसँग सम्बोधन गर्न सक्ने अवस्था छैन । नीतिगत रुपमा नेपालमा हाल सूचना प्रविधि नीति २०७२ मा सामान्य प्रसंग निस्केपनि साइबर सुरक्षा सम्बन्धी नीतिमा खास प्रगति हुन सकेको थिएन । वि. सं. २०७३ मा एक साईबर सुरक्षा नीति तर्जुमा भएको भएपनि त्यसले औपचारिक रुप लिन पाएको थिएन । गत वर्ष नेपाल दूरसंचार प्राधिकरणले साईबर सुरक्षा विनियामवली, २०७७ कार्यन्वयनमा ल्याएता पनि त्यसको प्रभावकारिता उ मातहतका सेवा प्रदायकमा मात्रै सिमित थियो । यस परिवेशमा राष्ट्रिय स्तरमा नेपाल सरकारले प्रस्ताव गरेको राष्ट्रिय साइबर सुरक्षा नीति, २०७८ को मस्यौदा स्वागतयोग्य छ ।

नेपाल सरकारले राष्ट्रिय साइबर सुरक्षा नीतिको मस्यौदा पेश गर्दै, यस नीतिमा संवेदनशील डाटा, व्यक्तिगतरुपमा पहिचान योग्य जानकारी, संरक्षित स्वास्थ्य जानकारी, अन्य व्यक्तिगत जानकारी, बौद्धिक सम्पत्ति, डाटा, सरकार तथा उद्योग सूचना प्रणालीको सुरक्षाको प्रावधान समावेश छ। यस नीतिले आगामी ३ वर्षमा संस्थागत र संगठनात्मक आवश्यकताहरू स्थापना गर्ने र त्यसको आधारमा आगामी ५ वर्षमा  भरपर्दो र सुरक्षित साइबरस्पेस निर्माण गर्न मार्ग प्रशस्त गरेको छ ।

पहल आफैंमा सकारात्मक रहँदा रहँदै पनि यस नीतिमा कतिपय विषयवस्तु छुटेका छन् त कतिपय विषयवस्तु सुधार गर्नुपर्ने अवस्था छ । खास गरी, यस नीतिले मानवाधिकारको पक्षलाई आफ्नो सबल पक्ष मानेको छैन । संवेदनशील पूर्वाधार र डिजिटल सम्पत्तिको सुरक्षा र अनलाईन सामग्रीलाई एकै डालोमा राखेर नियमनमुखी नीतिलाई प्रस्ताव गरिएको छ । साइबर सुरक्षा नीति सूचना प्रणालीलाई सुरक्षित बनाउने मात्र नभएर नागरिकको विचार र अभिव्यक्तिको स्वतन्त्रता,भेला हुने स्वतन्त्रता, सञ्चारको हक, गोपनीयताको हक र सूचनाको हक लगाएतका संविधानले रक्षा गरेको मौलिक हक लागु र रक्षा गर्ने हेतुले जारी भएको कुरा प्रष्ट रुपमा उल्लेख गरिनु पर्छ ।

साइवर सुरक्षा इन्टरनेट गर्वनेन्स इकोसिस्टमकै एक पाटो हो र यससम्बन्धी नीति तथा कानून निर्माणमा पनि सबै सरोकारवालाहरुको उत्तिकै भुमिका हुन्छ । तर यस नीतिले सरकारी र केहि हदसम्म नीजि क्षेत्र बाहेक अन्य सरोकारवालाहरुलाई समेट्न सकेको छैन । यस नीतिले नागरिक समाज तथा नागरिक समाज सँस्थाहरुको कतै पनि उल्लेख गरेको छैन । यो समस्या एक प्रणालीगत समस्याको रुपमा रहेको देखिन्छ ।  साइवर जोखिमलाई न्यूनीकरण गर्न जनचेतना वृद्धि देखि सूरक्षीत इन्टरनेट अभियान सम्ममा नागरिक समाजको निकै ठुलो भूमीका हुन्छ तर त्यसलाई नजरअन्दाज गरिएको छ । त्यसैगरी विश्वविद्यालय, प्राविधिक समुह जस्ता सरोकारवालाहरुलाई पनि अर्थपूर्ण हिसाबले समेटिएको छैन ।

सार्वजनिक क्षेत्रको सुचना प्रणालिमा सबैभन्दा बडी आक्रमणका घटनाहरु हुने गर्दछ । सार्वजनिक क्षेत्रको धेरै जसो सुचना प्रणालिमा सहि किसिमको सुरक्षण संयन्त्र  नभएको अवस्थामा बडि एक्सपोजर हुने र बढी जोखिमहरु उठाउनु पर्ने हुँदा सार्वजनिक क्षेत्रका डाटा, सम्पत्तिहरु एक्सपोज हुन बाट कसरि जोगाउने र त्यसलाई कसरी हेर्ने भन्ने कुरा यो नीतिमा कम बोलीएको छ। त्यसैगरी, यस नीतिमा नीजि क्षेत्रको संलग्नता धेरै कम देखिएको छ। यस नितिको मस्यैदा तजुर्मा गर्दा नागरिक समाज निजि क्षेत्र तथा अन्य सरकोकारवाला हरुको सहभागिता तथा संलगनता खासै गरिएको देखिदैन । यस प्रकारका सम्वेदनशिल नीति तजुर्मा गर्दा विभिन्न सरोकारवालाहरुको सहभागीता गराउन अत्यन्त जरुरी छ र बिभिन्न सरोकारवालाहरुको प्रतिनिधित्व साथै प्रविधि र विज्ञहरुको राय समावेश गर्नुपर्ने हुन्छ। यसरी बनेको नीतिले भोलिको आउने

दिनमा ऐन बन्न लाइ रचनात्मकरुपले मदत् गर्दछ। यदि विज्ञ र सरोकारवालाहरु सहभागिता भएन भने कानुन को प्रभावकारीता घटेर जान्छ।

यस नितिमा साइबर सुरक्षा जस्तो संवेदनशील विषयमा सरकारले ल्याएको निजी एकदम सकारात्मक छ तर साइबर सुरक्षा जस्तो विषयमा ३ वर्षको लक्ष्य लगाउने समय भनेको धेरै समय हो त्यसैगरी संगठानत्मक पूर्वाधार बनाउने कुराहरु ५ वर्ष लगाउने भन्ने किसिमको प्रस्तुत गरिएको छ त्यस समयलाई छोट्याउनु पर्ने देखिन्छ। साइवर विषय एकदमै संवेदनशील विषय भईसकेको र सधैँ नयाँ नयाँ चुनौति आई राखेको कारण लामो समय राख्नु उचित देखिदैँन।चाँढो भन्दा चाँढो यसमा काम गर्नु पर्ने अवस्था छ किनभने यही विद्यमान कोभिड १९ बाट धेरै अनलाईन सर्भिस र कामहरु भईसकेका छन् र जुन किसिमको पब्लिकले अनलाइन सर्बिस प्रयोग गरी रहेको सन्दर्भमा बढी साइबर आक्रमण र साइबर घटना हुने कारणले गर्दा तोकिएको समयलाई घटाउनु पर्छ।

प्रस्तावित मस्यौदामा संचार मन्त्रालयलाई जिम्मेवार (फोकल) मन्त्रालयको रुपमा लिइएको छ । तथापी, साईबर सुरक्षा बहुआयामिक बिषय हो । यो नीति तर्जुमा गर्दा राष्ट्रिय सुरक्षा नीति, स्वास्थ्य नीति, परराष्ट्र नीति, शिक्षा नीति लगायतका नीतिहरु समन्वय गर्नु आवश्यक हुन्छ । यस मस्यौदामा त्यसको अभाव छ । त्यसै गरी, व्यवसायिक संगठनले मात्र यसको कार्यान्वयन संभव छ । भएका पूर्वाधार तथा संगठनलाई कानुनी रुपमा नै बलियो बनाई प्रभावकारी रुपमा नेतृत्व तय गर्नु आवश्यक हुन्छ । साइबर सुरक्षा सबै क्षेत्रको आवस्यकता रहेको हुनाले एक केन्द्रिय साइबर सुरक्षा प्राधिकरणको स्थापना आवस्यक देखिन्छ । समन्वयात्मक सहकार्य र प्रतिकार्यका लागि  प्राधिकरणमा बिभिन्न निकायहरु, बिज्ञहरु, महत्वपूर्ण सूचना तथा संचार प्रबिधि पूर्वाधार तथा सेवा प्रदायकहरुको साझा संयन्त्र बनाउने । उक्त प्राधिकरणले एक साइबर मोनिटरिङ्ग केन्द्रको परिचालन गरि साइबर जोखिमको अनुगमन गर्ने व्यवस्था गर्नु पर्दछ । राष्ट्रिय साइबर प्रतिकार्य टोलि गठन गर्ने र चौबिसै घण्टा आपतकालीन सूचना केन्द्र संचालन गर्ने व्यवस्था मिलाउनु आवश्क हुन्छ ।

साइबर आक्रमणका घटनाहरु भएमा तुरुन्तै एकद्वार प्रणाली अन्तर्गत सम्बन्धित निकायमा जानकारी दिने कानुनी व्यवस्था गर्ने र साइबर घटना सम्बन्धि सूचना आदान प्रदान गर्ने प्रणाली निर्माण गर्नु आवश्यक छ । साथै प्राधिकरणले अन्तरराष्ट्रिय समन्वयका तथा सहकार्यकालागि प्रमुख भूमिका निर्वाह गर्ने र नेपाली सेनालाई साइबर डिफेन्स कमाण्ड सेन्टर स्थापना गर्न सहयोग गर्ने र नेपाली सेनाको साइबर सुरक्षा शाखालाई निर्देशनालय स्तरमा अभिवृद्धि गर्ने व्यवस्था गर्नु उपयुक्त हुन्छ । साइबर स्पेसले असिमेट्रिक द्वन्दलाई बढावा दिने हुनाले अन्वेषण तथा अनुशन्धानका लागि नेपाली सेनामा डिजिटल रक्षा विधिबिज्ञान प्रयोगशाला स्थापना गर्नु पर्ने देखिन्छ ।

यस नीतिले सार्वजनिक क्लाउड र सूचना सुरक्षाको प्रावधानलाई क्लाउड परिसरमा समाहित गर्न बेवास्ता गरेको छ। खासगरी, कस्तो सूचना आन्तरिक पूर्वाधार र कस्तो सूचना वाह्य पूर्वाधारमा राख्न सकिने हो ? पब्लिक क्लाउडको सुरक्षा नीति कस्तो हुने हो यसमा थप प्रष्ट हुनु जरुरी छ ।

यस नितिमा सिमान्तिकृत समुदायको सुरक्षाको बारेमा थप प्रष्ट पार्नु जरुरी छ । खास गरी महिला, बालबालिका तथा लैंगिक अल्पसंख्यकको सुरक्षामा जोड दिनु जरुरी छ र यो नीति सबैको सुरक्षाका निमित्त हो भन्ने कुरा जानकारी दिलाउन जरुरि देखिन्छ। व्यक्तिको निर्धक्क (confidence) साथै साइबर विश्वमा “म” कत्तिको सुरक्षित हुन सक्छु भन्ने संयन्त्रको कुरा पुष्टि हुन आवश्यक छ।

……

# समिक्षा खण्ड

## उद्देश्य

सञ्चार तथा सूचना प्रविधि मन्त्रालयले सार्वजनिक गरेको 'राष्ट्रिय साइबर सुरक्षा नीति, २०७८' को मस्यौदामाथि बहु सरोकारवालासगँको सरोकार संलग्न गरी समय सापेक्ष तथा प्रगतिशिल नीति निर्माणमा योगदान गर्नु यस प्रतिवेदनको मुल उद्देश्य हो । यस समिक्षाको देहाय बमोजिमका थप उद्देश्य रहेका छन् ।

- नागरिक तथा सरोकारवालको निती प्रतिको धारणा र सरोकार उठान गर्नु ।
- नीतिगत सुधारको लागि आवश्यक सुझाव दिनु ।
- सरोकारवालालाइ साइबर नीति त्यसले पार्ने प्रभावको बारेमा आवश्यक जानकारी दिने ।
- पछि बन्ने कानुनको बारेमा समयमा नै आवश्यक छलफल सूनिश्चित गर्ने ।

## समिक्षा तथा सुझाव

### सुरक्षा नितीमा समेटिनु पर्ने पक्ष

- "साइबर स्पेश" भनेर नीतिमा धेरै ठाउँहरुमा उल्लेख भएपनि साइबर स्पेश के हो, यसको सीमा (SCOPE) कतिसम्म हो, यसले के के लाई समेट्छ भनेर कतै पनि इंकित गरिएको छैन । त्यसो गरिनु उपयुक्त हुन्छ ।

- यस नीतिले संविधानले सुनिश्चित गरेका नागरिक तथा व्यक्तिका मौलिक अधिकारहरुको दृष्टिकोणलाई वा अधिकारमा आधारित दृष्टिकोण (Right based approach) समेट्न सकेको छैन । उदाहरणका लागि, नीतिमा सूचना प्रविधि प्रणालीहरुमाथिको अनाधिकृत पहुँच हुनबाट प्रणालीलाई सुरक्षित बनाउने र सो को जोखिम न्यूनीकरणका लागि संस्थागत र संरचनागत व्यवस्था गर्ने जस्ता कुरा राखिएको छ तर त्यो प्रणालीलाई सुरक्षित बनाउनुको उद्देश्य नै नागरिक तथा व्यक्तिको विभिन्न मौलिक तथा कानूनी अधिकारको रक्षाका लागि हो भन्ने प्रस्टउन सकेको छैन । त्यसैगरी प्रणालीलाई सुरक्षित बनाउने नाममा नागरिकको मानव अधिकार उल्लंघन गरिनेछैन, गर्न दिइने छैन भन्ने प्रत्याभुती पनी छैन । तसर्थ, नागरिकको मौलिक अधिकारको संरक्षणको विषय दीर्घकालीन सोच, परिदृष्य तथा उद्देश्यको खण्डमा समावेश गर्नुपर्दछ ।

- साइबर सुरक्षा नीति सूचना प्रणालीलाई सुरक्षित बनाउने मात्र नभएर नागरिकको विचार र अभिव्यक्तिको स्वतन्त्रता,भेला हुने स्वतन्त्रता, सञ्चारको हक, गोपनीयताको हक र सूचनाको हक लगाएतका संविधानले रक्षा गरेको मौलिक हक लागु र रक्षा गर्ने हेतुले जारी भएको पनि कतै प्रष्ट रुपमा उल्लेख गरिनु पर्छ ।

- साइवर सुरक्षा इन्टरनेट गर्वनेन्स इकोसिस्टमकै एक पाटो हो र यससम्बन्धी नीति तथा कानून निर्माणमा पनि सबै सरोकारवालाहरुको उत्तिकै भुमिका हुन्छ । तर यस नीतिले सरकारी र केहि हदसम्म नीजि क्षेत्र बाहेक अन्य सरोकारवालाहरुलाई समेट्न सकेको छैन । यस नीतिले नागरिक समाज तथा नागरिक समाज सँस्थाहरुको कतै पनि उल्लेख गरेको छैन । यो समस्या एक प्रणालीगत समस्याको रुपमा रहेको देखिन्छ । साइवर जोखिमलाई न्यूनीकरण गर्न जनचेतना वृद्धि देखि सूरक्षीत इन्टरनेट अभियान सम्ममा नागरिक समाजको निकै ठुलो भूमीका

हुन्छ तर त्यसलाई नजरअन्दाज गरिएको छ । त्यसैगरी विश्वविद्यालय, प्राविधिक समुह जस्ता सरोकारवालाहरुलाई पनि समेटिएको छैन ।

- साइवर इकोसिस्टमको एक महत्वपूर्ण पक्ष विश्वास वा विश्वास निर्माण (Trust or trust-building)। नीतिको उद्देश्यमा सर्वसाधारणमा आईटी प्रणालीहरू र साइबरस्पेस भित्रको लेनदेन तथा कारोवार (Transaction) मा पर्याप्त विश्वास उत्पन्न गर्ने र अर्थव्यवस्थाको सबै क्षेत्रमा आईटीको प्रयोग बढाउने कुरा पनि समावेश गरिनु उपयुक्त हुन्छ ।
- नितीले उपचारको, अधिकार कार्यान्वयनको पाटोलाई समेट्न सकेको छैन ।
- आधारभुत समिक्षाका क्रममा यो नीति भारतीय साइवरसुरक्षा नीतिबाट एकदमै प्रभावीत देखिन्छ । मस्यौदा तयारीका क्रममा सरोकारवालाहरुसँग छलफल नभएकाले पनि यसले नेपाली समस्या, चुनौती तथा उपायहरुलाई समेट्न नसेकेको देखिन्छ ।

## मस्यौदामा सुधार गरिनु पर्ने पक्ष

- सरकारी वा निजी क्षेत्रको साइबर सुरक्षा कमजोरी वा हेलचेक्रयाईको कारणले पीडित हुन पुगेका नागरिकहरुलाई उपचार क्षतिपूर्ति दिने कुनै व्यवस्था गरिने छ भनेर राख्न आवश्यक छ । (रणनीति १०.१, १०.२, १०.३)
- नीतीले आवश्यक कानून निर्माण तथा संस्थागत र संगठनात्मक पूर्वाधार स्थापनाका लागि तोकेको समय एकदमै ढिलो छ । कानूनी व्यवस्थाका लागि ३ वर्ष र संस्थागत र संगठनात्मक पूर्वाधार स्थापनाका लागि ५ वर्ष तोकिएको छ, सरोकारवालाहरुसँगको परामर्शमा यसलाई पूनरावलोकन गरिनु उपयुक्त हुन्छ । (८.१) (८.२)
- साइवर जोखिमलाई न्यूनीकरण गर्न जनचेतना वृद्धि एवम् दक्ष जनशक्ति उत्पादन गर्ने भन्ने लक्ष्य राखिएको छ (८.३.) तर कुनै मात्रात्मक लक्ष तथा समयसिमा तोकेको छैन ।
- सबै संघसंस्था संगठनहरूमा साइबर सुरक्षा पहलहरू कार्यान्वयन गर्न र साइबर घटनाहरूबाट उत्पन्न हुने आपतकालीन अवस्थालाई सामना गर्न विशेष बजेट राख्नुपर्ने व्यवस्ता समावेश गर्नुपर्ने । (कार्यनीति रणनीति नं. १०.१ सँग सम्बन्धित)
- आईसीटी उत्पादनहरु र सेवाहरूको सुरक्षाको परीक्षण र गुणस्तर मापनको लागि पूर्वाधार स्थापना गर्ने कुरा समावेश गर्नुपर्ने ।(कार्यनीति रणनीति नं. १०.३ सँग सम्बन्धित)
- आईटी प्रणाली र नेटवर्कमा लागू गरिएका प्राविधिक र अपरेशनल सुरक्षा नियन्त्रण उपायहरूको पर्याप्तता र प्रभावकारताको परीक्षण गर्न र नियमितरुपमा सबै संस्थाहरूलाई प्रोत्साहित गर्ने कुरा समावेश गर्नुपर्ने । (कार्यनीति रणनीति नं. १०.३ सँग सम्बन्धित)

- साइबर सुरक्षा घटनाहरुको प्रतिरोध र सामना गर्ने सन्दर्भमा आपतकालीन तयारीको स्तरको आकलन गर्न राष्ट्रिय, क्षेत्रिय र स्थानिय स्तरमा नियमित साइबर सुरक्षा ड्रिल र अभ्यासहरु सञ्चालन गर्ने कुरा समावेश गर्नुपर्ने ।(कार्यनीति रणनीति नं. १०.३ सँग सम्बन्धित)
- साइबर सुरक्षा नीतिमा सम्वाद, समिक्षा र सुझावका लागि थिंक ट्याकं समूह बनाउन आवश्यक देखिन्छ । यसमा नागरिक समाज लगायत सबै सरोकारवालाहरुलाई समेटिनुपर्छ । (रणनीति नं. १०.६ सँग सम्बन्धित )
- साइबर सुरक्षाको क्षेत्र र विशेष गरी साइबर खतरा –जोखिम, सम्भावित सुरक्षात्मक उपायहरु, र उत्तम अभ्यासहरु अपनाउने सम्बन्धी कार्यहरुको लागि सूचना पूर्वाधारको संरक्षणको विषयमा निजी क्षेत्रलगायत सरोकारवाला निकायहरु बीच सहयोग र सहकार्य गर्नुको साथै सहजीकारण भूमिका सरकारले लिने कुरा समावेश गर्नुपर्ने । (रणनीति नं. १०.६ सँग सम्बन्धित )
- ह्याक, ह्याक्टिविस्ट, पहिचान चोरी, साइबर ब्ल्याकमेल जस्ता समस्या रणनीति नं. १०.८ सँग सम्बन्धित कार्यनितिमा समावेश गर्नुपर्ने ।
- नीतिमा साइबर सुरक्षाको लागि अन्तर्राष्ट्रिय समुदायसँग सहकार्य गर्ने भनिएको छ र यस्को जिम्मा राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह (NITERT) लाई दिएको छ तर अन्तर्राष्ट्रिय समुदायसँग सहकार्यको लागि १२.३ अनुसारको समन्वय समितिमा जिम्मेवारीको बुदा थपि परराष्ट्र मन्त्रालयको पदादिकारी पनि राख्न उपयुक्त हुन्छ ।
- १२.६ महिला तथा बालबालिका अनलाइन सुरक्षा कार्यसमूहले LGBTQA र अल्पसंख्यकलाई पनि अनलाइन सुरक्षाका सम्बन्धमा समावेश गर्नुपर्ने देखिन्छ । (सामाजिक संजालमा सो समुदाय माथीको द्वेषपूर्ण अभिव्यक्ति बढ्दै गैरहेको छ । )
- साइवर सुरक्षाको सुनिश्चितताको लागि दक्ष जनशक्ति विकास गर्ने भनेर लेखिएको छ । तर, यस सम्बन्धमा अनुसंधान संस्थाहरुसँगको साझेदारी कसरी गर्ने भन्ने प्रष्ट हुनु जरुरी छ । तर, यसमा दक्ष जनशक्ति विकास गर्न क्षमता निर्माणको साथसाथै साइबर जागरुकताको कुरा पनि समावेश गर्नुपर्दछ । Cyber Capacity building is about more than just securing and utilising cyberspace successful implementation can help to provide broader stability and socio–economic growth -Muller, 2015. (समस्या र चुनौती खण्ड ४.३)
- ११.६मा बौद्धिक सम्पत्ती तथा प्रतिलिपि अधिकार संरक्षणको व्यवस्था मिलाइने भनिएको छ यो रक्षा नीति सँग नभएर वाणिज्य नीतिको एक हिस्सा जस्तो देखिन्छ । यसलाई साइबर सुरक्षासँग जोडेर उल्लेख गरिनुपर्छ ।
- ११.५ मा नेपाली नागरिकहरुको अनलाईन पहिचानको सुरक्षा तथा डाटा सुरक्षा सम्बन्धी उपायहरु अवलम्बन गरिने भनिएको छ तर डाटा सुरक्षा नेपाली नागरिक मात्रलाई नभएर सबैसँग सम्बन्धित छ साथै डाटा सुरक्षा सम्बन्धी उपायहरु के हुने छन् त्यो प्रस्त पार्नुपर्ने देखिन्छ ।

- नीतीमा प्रयोग भएका भाषा र कतीपय प्रावधान अस्पष्ट तथा दुविधापूर्ण देखिन्छन । स्पष्टताका लागि त्यसमा सुधार जरुरी छ । उदाहरणका लागि :
    - ४.१ आम जनताको सूचना एवं तथ्याङ्कमा सहज पहुँच सँगै सार्वजनिक, व्यवसायिक र व्यक्तिका तथ्याङ्क एवम् सूचनाहरुमा अनाधिकृत पहुँच नियन्त्रण गर्ने।
    - ११.३ अपराधिकरण, अनुसन्धान, विद्युत्तीय प्रमाण तथा अन्तर्राष्ट्रिय सहयोगका साथै मौलिक अधिकारहरूको संरक्षणका सन्दर्भमा क्षेत्रीय एवं अन्तर्राष्ट्रिय मापदण्ड अनुरुप कानूनी तथा नीतिगत व्यवस्था गरिने।
- ११.९मा गुणस्तरीय सफ्टवयर निर्माणका लागि आवश्यक पर्ने मापदण्ड तयार गरी लागु गरिने लेखिएको छ तर सबै सफ्टवेयर देश भित्र विकसित हुदैनन् त्यसैले सफ्टवेयर आयातमा पनि आवश्यक पर्ने मापदण्ड तयार गरिने भन्नु आवश्यक छ .
- ११.१०मा नेपाली नागरिकका गोपनीयताको हक, सूचनाको हक एवं स्वतन्त्रताको संरक्षण गर्न व्यक्तिगत एवं सामूहिक साइबर सुरक्षाका उपायहरु निर्धारण गरिने भनिएको छ तर सो उपायहरु के हुने कस्तो हुने लिखिएको छैन।
- ११.११ व्यक्तिगत वा संस्थागत तथ्यांकहरु संकलन, प्रशोधन, प्रयोग एवं भण्डारण गर्ने निकायहरूमा भएका साइबर आक्रमण तथा प्रयोगकर्ताका डाटा हानी, नोक्सानी, तथा चोरी सम्बन्धी सूचना सार्वजनिक गर्नुपर्ने व्यवस्था गरिने भनिएको छ यसलाई थप स्पष्ट पार्नु पर्छ तर त्यस्ता एजेन्सीहरूको लापरवाहीका लागि तिनीहरुलाई जिम्मेवार बनाउने कुरा राख्न आवश्यक छ ।
- ११.१५ साइवर सुरक्षाको विषयमा अनुसन्धान तथा विकास, साइबर सुरक्षा प्रवर्धन, जनचेतना अभिवृद्धि, साइबर सुरक्षा सम्बन्धी तयारी, रोकथाम, पहिचान, प्रतिक्रिया तथा पुनर्लाभ गर्न, २४/७ सम्पर्क निकायको रुपमा कार्य गर्न तथा डिजिटल फोरेन्सिक अनुसन्धान गर्न राष्ट्रिय साईबर सुरक्षा केन्द्र स्थापना गरिने भनिएको छ । यसमा जनचेतना अभिवृद्धि, साइबर सुरक्षा सम्बन्धी तयारी, रोकथाम, पहिचान, प्रतिक्रिया तथा पुनर्लाभ गर्न नागरिक र नागरिक समाजको भूमिका धेरै महत्वपुर्ण हुन सक्छ त्यसैले नागरिक समाजको भूमिका पनि यहाँ राख्न जरुरी छ ।
- रणनीति नं. १०.५ सँग सम्बन्धित (साइवर सुरक्षाको विषयमा जनचेतना अभिवृद्धि गरिने।)मा नागरिक समाजको भूमिका धेरै महत्वपुर्ण हुन सक्छ तर नागरिक समाजको भूमिका यहाँ राखिएको छैन ।

सुझावका अन्य विषय

- नीतिको ११.५६ र ११.५७मा भएको कन्टेन्ट मनिटरिङ्ग तथा फिल्टरिङ्गको विषय हटाउँदा उपयुक्त हुन्छ ।
- नीतिको ११.३मा सुरक्षा विशेषताहरु जस्तै confidentiality, integrity, availability and authenticity हरुको कुरा गरेको छ। त्यहाँ non-repudiation को पनि व्यवस्था राख्न आवश्यक छ ।

- प्रविधिलाई सुरक्षित गर्न इथिकल ह्याकिङ ( Ethical hacking) लाई कानूनी मान्यता दिन आवश्यक छ ।
- पछिल्लो समयमा जुन किसिमका data leakage का घटनाहरु बढी देखिको छ त्यसको लागि डाटा रिसोर्स बिमा (Insurance) के कसरी गर्नु पर्छ भन्ने कुराहरु नीतिमा राख्न आवश्यक छ ।
- साइबर सुरक्षा नियमावली २०७७ र रेडियो सुरक्षा ऐन २०१४ लाई राष्ट्रिय साइबर सुरक्षा निति २०७८ ले आकर्षित गर्ने प्रावधान राख्नु पर्छ।
- कुनै पनि संस्थामा साइवर आक्रमण भयो भने र सो संस्थामा कुनै पनि सुरक्षा कमजोरी देखियो भने त्यस्तो संस्थालाई कारबाही गर्ने नीतिमा उल्लेखित हुनुपर्छ।
- आपत्कालीन हवाई सेवा, ट्राफिक व्यवस्थापन, सिसि टिभी, दूरसंचार,डिजीटल नेटवर्कहरु सुरक्षित राख्ने कानूनी प्रावधानहरु बनाइने छ भनेर नीतिमा उल्लख गर्न जरुरी छ ।
- यस नीतिले global cyber security index मा नेपालको स्थानलाई कसरी उक्साउने भन्ने किसिमले अगाडि बढ्नु पर्ने देखिन्छ र यसका लागि एउटा राष्ट्रिय साइबर सुरक्षाको आयोजना ल्याउनु पर्ने देखिन्छ।
- नीतिमा उल्लेख भए अनुसार साइबर सुरक्षा केन्द्र भएर मात्र हुदैंन । यसमा सेक्युरिटी अपरेस्नल(security operational) केन्द्र जसले threat intelligence monitoring हरु गर्न सक्ने अथवा कसैले threat पत्ता लगाएकोमा त्यसतो threat कहाँ गएर रिपोर्टींङ गर्ने त्यसतो कुराहरु पनि उल्लेखित गर्न जरुरी छ।
- साइबर अपराधबाट पिडितहरुलाई परामर्श (counseling) गर्नुपर्ने हुन्छ र त्यसका लागि परामर्श ईकाइ को व्यवस्था हुनेछ भनेर यस नितिमा उल्लेख गर्न पर्ने आवश्यक छ।
- प्रस्तावित साईबर सुरक्षा नीतिमा क्लाउड सेवाको सुरक्षाको कुराहरु छुटेकोछ । राष्ट्रिय तथा अन्तर्राष्ट्रिय सेवा प्रदायकले उपलब्ध गराउने क्लाउड सेवाको सुरक्षाको सवालमा नीतिगत व्यवस्था गर्नु जरुरी छ ।

# अनुसूचि १

बहुसरोकारवाला छलफलको विस्तृत विवरण

## उद्देश्य

सञ्चार तथा सूचना प्रविधि मन्त्रालयले सार्वजनिक गरेको 'राष्ट्रिय साइबर सुरक्षा नीति, २०७८' को मस्यौदामाथि बहु सरोकारवालासगँको आवश्यक छलफललाइ सहजिकरण गरि उक्त मस्यौदामा केन्द्रित सुझावहरु सहितको प्रतिवेदन तयार पार्नु यस कार्यक्रमको मुल उद्देश्य हो ।

## कार्यक्रमको संक्षिप्त विवरण

कार्यक्रममा इन्टरनेट गभर्नेन्स इन्स्टीच्युटका संस्थापक तथा प्रमुख कार्यकारी निर्देशक अधिवक्ता बाबुराम अर्यालले आयोजकहरुको तर्फबाट प्रस्तावित राष्ट्रिय साइबर सुरक्षा नीति, २०७८ को मस्यौदा माथीको संक्षिप्त टिप्पणी छलफलको लागि राख्नु भएको थियो । प्रस्तावित राष्ट्रिय साइबर सुरक्षा नीति, २०७८ को मस्यौदा माथिको संक्षिप्त प्रस्तुति पछि सरोकारवालासँग छलफल संचालन भएको थियो । कार्यक्रमको अध्यक्षता इन्टरनेट गभर्नेन्स इन्स्टीच्यूटका अध्यक्ष मनोहरकुमार भट्टराईले गर्नु भएको थियो भने डिजिटल राईट्स नेपालको अध्यक्ष सन्तोषबाबु सिग्देलले सहभागीहरुलाई स्वागत गर्दै कार्यक्रमको उद्देश्यमाथि प्रकाश पार्नु भएको थियो । सरोकारवालासँगको छलफलमा डिजिटल राईट्स नेपालका महासचिव टंकराज अर्यालले सहजीकरण गर्नुभएको उक्त कार्यक्रममा इन्फर्मेशन सेक्युरिटी रेस्पोन्स टिम नेपाल (एनपीसर्ट)का अध्यक्ष चिरंजीवी अधिकारीले धन्यवाद ज्ञापन गर्नु भएको थियो । कार्यक्रमको प्रतिवेदन डेल्टा ल फर्मकी लिगल एसोसिएट अधिवक्ता एलिसा भण्डारी र डिजिटल राइट्स नेपालका कार्यक्रम संयोजक सौरभ भट्टराईले तयार गर्नु भएको थियो भने प्रविधिको संयोजन इन्टरनेट गभर्नेन्स इन्स्टीच्यूटका कार्यक्रम अधिकृत आनन्द गौतमको रहेको थियो ।

कार्यक्रम विवरण यस प्रकार थियो ।

- कार्यक्रम मिति: २०७८।०२।२३
- समय: ४ बजे देखि ६ बजे सम्म
- आयोजक:
    - इन्टरनेट गभर्नेन्स इन्स्टीच्यूट,
    - फोरम फर डिजिटल इक्वालीटी र
    - डिजिटल राइट्स नेपालको आयोजना
- सह-आयोजक:
    - सेन्टर फर साईबर सेक्युरिटि रिसर्च एण्ड इनोभेसन,
    - इन्फर्मेशन सेक्युरिटी रेस्पोन्स टिम नेपाल (एनपीसर्ट),
    - डिजिटल मिडिया फाउण्डेशन,
    - डेल्टा ल फर्म,
    - नेपाल इन्टर्नेट फाउन्डेसन र
    - मिडिया एक्शन नेपाल

## छलफलको विस्तृत विवरण तथा सुझाव

### केपी ढुँगाना, संस्थापक अध्यक्ष, अनलाईन पत्रकार संघ

नेपालमा साइबर अपराध बढ्दै गहिरहेको अवस्थामा साइबर सुरक्षाका लागि जारि गरेको राष्ट्रिय साइबर सुरक्षा नीति, २०७८ मा धेरै सकरात्मक कुरा हरुलाई सामावेश गरिएको भएता पनि कुनै कुराहरु प्रष्ट रुपमा देखापरेका छैनन्। जस्तै दफा ११.५६ र दफा ११.५४ मा इन्टरनेट तथा सामाजिक सञ्जालको प्रयोग गरी मिथ्या खबर (fake news) सम्प्रषेण गर्ने कार्यलाई नियमन गरिने र राष्ट्रिय सुरक्षामा आँच पुर्याउने, घृणा वा द्वेष फैलाउने, अनलाइन उत्पिडन (online harassment) र साइबर बुलिङ्ग गर्ने, विभिन्न जनजाति र सिमुदायबिचको सुमधुर सम्बन्धमा खलल पुर्याउने किसिमको डिजिटल सामाग्रिको सम्प्रषेणलाई नियमन गरिने भन्ने उल्खेख भएतापनि मिडिया क्षेत्रको सामग्रीलाई यस साइबर सुरक्षा नीतिले कसरी हेर्छ भन्ने कुरामा स्पष्ट छैन।यसको रुपमा काम गर्न नेपाल प्रेस काउन्सिल सगँ सम्नीय गरेर उसको नेतृत्वमा समुदाय गठन गर्नुपर्छ। त्यस्तो समुदायजहाँ नेपाल प्रेस काउन्सिल, नेपाल पत्रकार महासघँको प्रतिनिधि, अनलाइन पत्रकार सघं लगायतका पेशागत सगंठन, व्यवसाय सगंठन, साइबर सुरक्षा र सुरक्षा र संचार सगँ सम्बन्धि विग्यहरु भएर आर्को एउटा छुट्टै समुदाय गराउनु पर्छ र यस नीतिको कार्यान्वियनको सन्दर्भमा र संयन्त्रमा (mechanism) उचेत ध्यान दिनुपर्छ।

### नितु पंडित, अध्यक्ष संचारिका समूह

साइबर सुरक्षाको कुरा गर्दा यहाँ महिला र पुरुष सवैको पहुचँको कुरा हो जस्तो लाग्छ। अहिलेको समयमा डिजिटल्लि हेर्दा महिला र पुरुषको खाडल असाध्यै ठुलो छ र लैङ्गिक दृष्टिकोणबाट हेर्दा सामाजिक सन्जालमा जो जिति महिलाहरु आउनुहुन्छ कोहि न कोहि उत्पीडनको (harassment) सिकारमा पर्नुहुन्छ। यस कारणले यहाँ ढुक्क र सुरक्षित हुने खालको वातावरण देखिदैन। सुरक्षाको लागि आएको हुदाँ हुदैँ पनि हामीलाइ प्रविधिले विश्वास दिन सकेको छैन। यो भनेको नितिमा कामीकमजोरि रहेको बुझिन्छ।दिर्घकालिन सोचको कुरा गर्दा भरपर्दो, सुरक्षित एवं लचिलो साइबर स्पेश निर्माण भन्दा खेरी सुरक्षा कहाँ सम्म होत भन्ने कुरा पनि पुष्टि हुन जरुरी छ। यस नितिमा कतैपनि Marginalized Community को कुरा गरिएको छैन। यस नीतिमा Marginalized community का बारेमा बोल्नु जरुरि छ र सबैको सुरक्षाका निमित्त हो भन्ने कुरा जानकारी दिलाउन जरुरि देखिन्छ। व्यक्तिको निर्धक्क (confidence) साथै साइबर विश्वमा “म” कत्तिको सुरक्षित हुन सक्छु भन्ने संयन्त्रको कुरा पुष्टि हुन आवश्यक छ।

### विवेक राणा, प्रमुख सल्लाहकार, इन्फो एस्योर एलएलपी

राष्ट्रिय साइबर सुरक्षा नीति, २०७८ सरकारले अध्ययन गरेरै ल्याएको होला तर यसले आगामी दिनमा बन्नु पर्ने कानूनलाई जति स्पष्ट दिशा दिनुपर्ने हो त्यति दिशा दिन सकेको देखिंदैन । इन्टरनेट स्वतन्त्रता र डिजिटल अधिकारमा मानव अधिकार तथा अभिव्यक्ति स्वतन्त्रतालाई प्रत्याभूत गर्ने गरी साइबर सुरक्षा नीति तथा कानून बन्नुपर्ने हुन्छ। नियमन, दिशानिर्देश, प्राविधिक सहयोग, सूचना र प्रशिक्षण साइबर जगतमा सार्वजनिक सेवा र नागरिकहरूको सुरक्षाको हिसाबले अतिनै महत्वपूर्ण स्तम्भहरू हुन्। यदि सूचना प्रविधिको प्रणालि अथवा संरचना गलत भयो भने त्यो प्रभावकारी हुन सक्दैन र यिनि कुरा हरुको कमी कमजोरि यस नीतिमा देखिन्छ।

सार्वजनिक क्षेत्रको सुचना प्रणालिमा सबैभन्दा बडी आक्रमण का साथसाथै घटनाहरु हुने गर्दछ । सार्वजनिक क्षेत्रको धेरै जसो सुचना प्रणालिमा सहि किसिमको सुरक्षण संयन्त्र नभएको अवस्थामा बडि एक्सपोजर हुने र बढी जोखिमहरु उठाउनु पर्ने हुँदा सार्वजनिक क्षेत्रका डाटा, सम्पत्तिहरु एक्सपोज हुन बाट कसरि जोगाउने र त्यसलाई कसरी हेर्ने भन्ने कुरा यो नीतिमा कम बोलीएको छ। त्यसैगरी, यस नीतिमा नीजि क्षेत्रको संलग्नता धेरै कम देखिएको छ। यस नितिको मस्यैदा तजुर्मा गर्दा नागरिक समाज निजि क्षेत्र तथा अन्य सरकोकारवाला हरुको सहभागिता तथा संलगनता खासै गरिएको देखिदैन । यस प्रकारका सम्वेदनशिल नीति तजुर्मा गर्दा विभिन्न सरोकारवालाहरुको सहभागीता गराउन अत्यन्त जरुरी छ र बिभिन्न

सरोकारवालाहरुको प्रतिनिधित्व साथै प्रविधि र विज्ञहरुको राय समावेश गर्नुपर्ने हुन्छ। यसरी बनेको नीतिले भोलिको आउने दिनमा ऐन बन्न लाइ रचनात्मकरुपले मदत् गर्दछ। यदि विज्ञ र सरोकारवालाहरु सहभागिता भएन भने कानुन को प्रभावकारीता घटेर जान्छ।

यस नीतिले हेर्नु पर्ने मुख्य मुद्दाहरु सामाजिक मुद्दा र आर्थिक मुद्दा हो राष्ट्रियलेनै जुन डिजिटल अर्थव्यवस्था आउने भन्ने कुराहरु गर्छ त्यो डिजिटल अर्थव्यवस्थामा नेपालको अर्थव्यवस्था सुरक्षा कसरी छ? भन्ने कुरा बढी उल्लेखित गर्नु पर्ने देखिन्छ ।यसका साथै यस नीतिमा सुचना सुरक्षाका (Information Security) आधारभुत मान्यताहरू गोपनियता (confidentiality), अखण्डता integrity र गोपनियता availability हरुको कुरा गरेको छ ।त्यहाँ non-repudiation को मर्म र शब्द दुबै जरुरी देखिन्छ किनभने आफूले पठाइसकेको कुनै पनि डाटा तथा सूचना पठाएको होइन भनि भन्न नपाओस्।

यस नितीलाई अन्तराष्ट्रिय विश्वव्यापि अभ्यासको रुपमा हेर्दा राष्ट्रिय स्तरमै साइबर सुरक्षालाई नियमन गर्ने त्यसतो निकाय एउटा मन्त्रालयको महाशाखामा मात्र भएर हुदैँन।सरकारले साइबर सुरक्षा समबन्धि मुद्दा नियमन गर्ने एकल संगठन हुनु पर्ने भनेको छ तर धेरै ठाउँमा हेर्दा साइबर सुरक्षा लाई नियन्त्रण गर्ने संगठन असफल रहेका छन् र त्यसको कारण भनेको तिनीहरू वैधानिक निकायद्वारा स्थापित नभएर प्रत्यायोजित(delegated)कानूनबाट स्थापित हुन्छन्। यदि वैधानिक निकायद्वारा स्थापित भयो भने त्यो अधिक प्रभावकारी हुनेछ।

### डा. राजिव सुब्बा, पूर्व उपमहानीरिक्षक, नेपाल प्रहरी

विगतका केहि घटनाहरुबाट अब भौतिक सीमामा हुने द्वन्दको अवस्थामा साइबर जगतमा पनि द्वन्द हुन्छ भन्ने प्रमाणित हुन्छ । साधारण साइबर आक्रमण भन्दा जिरो-डे हमला हुने जसको बारेमा ज्ञान नहुने र निदान पनि थाहा नहुने र आक्रमण साधारण कम्प्युटर प्रणालीमा भन्दा महत्वपुर्ण सूचना प्रणालीमा हमला हुने देखिन्छ । अन्तरराष्ट्रिय प्रहरी संगठन (इन्टरपोल)को २०२० को रिपोर्ट अनुशार व्यक्ति र साना व्यापारिक संस्था भन्दा ठुला ठुला प्रतिस्ठान, निगम, सरकारी संस्थाहरु र महत्व पूर्ण पूर्वाधार संरचनाहरु ह्याकरहरुको निशानामा पर्न थालेका छन । साइबर हमलामा राष्ट्रहरु प्रत्यक्ष संलग्न नरहने तर उनीहरुको सहयोगमा ननइस्टेट ह्याकरहरुले साइबर हमला गर्ने रणनीति देखिन्छ । डिजिटल प्रविधिका कारण द्वन्दरत पक्षहरुले परम्परागत भन्दा असिमेट्रिक द्वन्द रणनीति अख्तियार गरेको देखिन्छ । अबको लडाईं भनेको बन्दुक र गोलिको मात्र नभई डिजिटल बिट्सको पनि हुने देखिन्छ । अन्तरराष्ट्रिय साइबर आक्रमणहरु साधारण तया प्रमाणको अभावमा ननएट्रीब्युटेवल कार्य हुन सक्ने हुनाले आक्रमणकरीहरुलाई सजिलै अन्तरराष्ट्रिय कानुनी दायरामा ल्याउन सकिदैन ।

साइबर सुरक्षा भनेको कम्प्युटर सुरक्षा मात्र नभई एक बृस्तीत राष्ट्रिय सुरक्षाको बिषय हो । किन भने सूचना तथा संचार प्रविधि प्रयोग नहुने कुनै पनि क्षेत्र छैन । तसर्थ नेपालका विभिन्न राष्ट्रिय नीतिहरु, ऐनहरु, नियमावलीहरू, निर्देशिकाहरुलाई बदलिँदो साइबर परिस्तिथि अनुसार परिमार्जन गरि राष्ट्रिय साइबर सुरक्षा नीति संग आबद्ध गर्नु पर्दछ । केहि दफावार सुझाव यस प्रकारका छन्:

- राष्ट्रिय सुरक्षा नीति २०७३ लाई परिमार्जन गरि बुंदा एक दशमलव नौ र दुई दशमलव आठमा उल्लेखित साइबर अपराध र बिध्युतिय बित्तिय संरचना सुरक्षा सहित साइबर डिफेन्स तथा महत्वपूर्ण सूचना प्रणाली (क्रिटिकल पूर्वाधार) जस्तै सूचना तथा संचार, स्वस्थ, शिक्षा आदि लाई समेत सुरक्षा प्रदान गर्ने व्यवस्था थप गर्ने ।
- दुरसंचार तथा इन्टरनेट सेवा प्रदायतहरुको महत्वपूर्ण सूचना प्रणाली (क्रिटिकल पूर्वाधार) सुरक्षाकालागी दुरसंचार ऐन २०५३ ले व्यवस्था गरे अनुरुप नेपाल दुरसंचार प्राधिकरणले तयार गरेको साइबर सुरक्षा बिनियमावली २०७७ लाई राष्ट्रिय साइबर सुरक्षा नीतिले आकर्षित गर्न सक्ने व्यवस्था गर्ने ।
- यस बिनियमावलीले नसमेट्ने क्षेत्रको हकमा साइबर सुरक्षा नीतिमा उल्लेख गर्ने । तथ्याङ्क सम्बन्धी गोपनीयता तथा सङ्कलित सूचनाको संरक्षणको व्यवस्था गरिएको वैयक्तिक गोपनीयता सम्बन्धी ऐन २०७५ को परिच्छेद छ र परिच्छेददस र बुंदा पच्चीसलाई साइबर सुरक्षा नीतिले आकर्षित गर्न सक्ने व्यवस्था गर्ने ।
- पररास्ट्र नीति २०७६ मा उल्लेखित साइबर अपराध मात्र रहेको हुनाले साइबर जोखिम तथा साइबर डिफेन्स समेत थप गर्ने । साथै सिमानाको परिभाषा परिमार्जन हुँदै गएको अवास्थामा पररास्ट्र नीतिमा नेपालको भुमि

अरु रास्ट्रको बिरुद्धमा मात्र होइन साइबर पूर्वाधारहरु समेत् प्रयोग गर्न दिइने छैन भन्ने प्रतिबद्धता थप गर्नु पर्ने । राष्ट्रिय स्वास्थ नीति २०७६ को बुंदा छदशमलवएकपाँचलाई परिमार्जन गरि साइबर सुरक्षा कार्यनीति निश्चित गर्ने प्रावधान थप गर्ने ।

- यसका साथै नेपालका बैंकहरुका लागि राष्ट्र बैंकले जारी गरेको सूचना प्रविधि निर्देशिका २०१२ (२०६९) लाई परिमार्जन गरि कुनै पनि बित्तिय कारोबार गर्ने संस्थाहरुले अनिवार्य सूचना प्रणाली अडीट गर्नु पर्ने प्रावधान थप गर्ने ।
- रेडियो सिग्नल सूचना सुरक्षार्थ रेडियो ऐन १९५७ लाई साइबर सुरक्षा नीतिले आकर्षण गर्न सक्ने प्रावधान राख्ने ।
- भरपर्दो र रिजिलीएन्ट साइबर सुरक्षाका लागि नेपालले तत्कालै केहि महत्व पूर्ण कदमहरु लिनु पर्दछ । सर्वप्रथम राष्ट्रिय साइबर सुरक्षा नीति निर्माण गरि लागु गर्ने ।
- राष्ट्रिय साइबर सुरक्षा नीतिमा तिन मुख्य कार्यक्षेत्रहरु पर्दछन । ति हुन, महत्वपूर्ण सूचना तथा संचार प्रबिधि पूर्वाधार तथा सेवाहरु, साइबर डिफेन्स, र साइबर अपराध । साइबर सुरक्षा सबै क्षेत्रको आवस्यकता रहेको हुनाले एक केन्द्रिय साइबर सुरक्षा प्राधिकरणको स्थापना आवस्यक देखिन्छ ।
- डिजिटल नेपाल फ्रेमवर्क २०१९ ले साइबर सुरक्षा केन्द्रको परिकल्पना गरेको देखिन्छ तर बिषयको गाम्भीर्यतालाई मध्य नजर गरेर बिशिस्ट अधिकार सहितको प्राधिकरण उपयुक्त हुन्छ । समन्वयात्मक सहकार्य र प्रतिकार्यका लागि  प्राधिकरणमा बिभिन्न निकायहरु, बिज्ञहरु, महत्वपूर्ण सूचना तथा संचार प्रबिधि पूर्वाधार तथा सेवा प्रदायकहरुको साझा संयन्त्र बनाउने ।
- उक्त प्राधिकरणले एक साइबर मोनिटरिङ्ग केन्द्रको परिचालन गरि साइबर जोखिमको अनुगमन गर्ने व्यवस्था गर्नु पर्दछ । राष्ट्रिय साइबर प्रतिकार्य टोलि गठन गर्ने र चौबिसै घण्टा आपतकालीन सूचना केन्द्र संचालन गर्ने ।
- साइबर आक्रमणका घटनाहरु भएमा तुरुन्तै एकद्वार प्रणाली अन्तर्गत सम्बन्धित निकायमा जानकारी दिने कानुनी व्यवस्था गर्ने र साइबर घटना सम्बन्धि सूचना आदान प्रदान गर्ने प्रणाली निर्माण गर्ने । साथै प्राधिकरणले अन्तरराष्ट्रिय समन्वयका तथा सहकार्यकालागि प्रमुख भूमिका निर्वाह गर्ने ।नेपाली सेनालाई साइबर डिफेन्स कमाण्ड सेन्टर स्थापना गर्न सहयोग गर्ने र नेपाली सेनाको साइबर सुरक्षा शाखालाई निर्देशनालय स्तरमा अभिवृद्धि गर्ने । साइबर स्पेसले असिमेट्रिक द्वन्दलाई बढावा दिने हुनाले अन्वेषण तथा अनुशन्धानका लागि नेपाली सेनामा डिजिटल रक्षा विधिबिज्ञान प्रयोगशाला स्थापना गर्नु पर्ने देखिन्छ ।
- बढ्दै गएको साइबर अपराधको सन्दर्भमा नेपाल प्रहरीको साइबर अपराध अनुसन्धान प्रणाली तथा डिजिटल फोरेन्सिक ल्याबलाई थप मजबुत बनाउने र विस्तार गर्ने, साथै नेपाल प्रहरीको साइबर ब्युरो प्राविधिक व्यक्तिले नेतृत्व प्रदान गर्ने व्यवस्था मिलाउनु पर्दछ ।
- आपतकालीन सेवा, हवाई सेवा तथा ट्राफिक व्यवस्थापनमा प्रयोग हुने दुरसंचार  सेवा, सिसिटिभी लगायत डिजिटल प्रविधि तथा नेटवर्कहरु सुरक्षित राख्ने व्यवस्था गर्ने ।
- विश्वविध्यालयहरु, अन्तरराष्ट्रिय संस्थाहरु, र बिदेशमा रहेका बिज्ञ नेपालीहरु संगको सहकार्यमा अनुशन्धान गर्ने, ज्ञान स्थानान्तरणको प्रयास गर्ने र आवस्यक जनशक्ति उत्पादन गर्ने।
- सवारी चालक अनुमति पत्र, राष्ट्रिय परिचय पत्र आदि जस्ता प्रणालीहरुमा रहेका डाटा सुरक्षित राख्ने, सरकारी र गैर सरकारी संस्थाहरुको सूचना प्रबिधि तथा सुरक्षा प्रणाली अडिट बेलाबेलामा अडिट गर्नु पर्ने व्यवस्था निश्चित गर्ने र येथिकल ह्याकिंगलाई कानुनी मान्यता प्रदान गर्ने। लाइसेन्स वा अनुमति प्राप्तगरी डिजिटल रडियो संचार (वाकीटाकी), दुरसंचार, इन्टरनेट, आइपी बेस्ड सिसिटिभी प्रणालीहरुको अनुगमन गर्ने व्यवस्था निश्चित गर्ने ।
- साइबर अपराध बिरुद्ध बालबालिका तथा बृद्धबृद्धा लगायत सबै नागरिकहरुलाई साइबर स्वास्थ्य सचेतना कार्यक्रमहरु गर्ने।

### रोजा किरण बासुकला, उपाध्यक्ष, सेन्टर फर साइबर सेक्युरिटी रिसर्च एण्ड इनोभेसन

अहिलेको समयमा घर-घर र हात-हात मा इन्टरनेट सेवा पुगिरहेको सन्दर्भमा, विषेश गरी अनलाईन तथा मोबाईल कारोबार जस्ता संमवेदनशील कारोबारहरु समेत भइरहेको र साइबर सुरक्षाका घटनाहरु दिनहु दिन बढिरहेकोमा अहिले साइबर सुरक्षा हरेकको जिम्मेवारि भइसकेको छ। अनुसन्धान अनुसार नेपाल "cyber threat" मा टप टार्गेट देशमा परेको सन्दर्भमा यो अहिले एकदम सन्दर्भिक विषय बनेको छ।

यस नितिमा साइबर सुरक्षा जस्तो संवेदनशील विषयमा सरकारले ल्याएको निजी एकदम सकारात्मक छ तर साइबर सुरक्षा जस्तो विषयमा ३ वर्षको लक्ष्य लगाउने समय भनेको धेरै समय हो त्यसैगरी संगठानत्मक पूर्वाधार बनाउने कुराहरु ५ वर्ष लगाउने भन्ने किसिमको प्रस्तुत गरिएको छ त्यस समयलाई छोट्याउनु पर्ने देखिन्छ।साइवर विषय एकदमै संवेदनशील विषय भईसकेको र सधैँ नयाँ नयाँ चुनौति आई राखेको कारण लामो समय राख्नु उचित देखिदैँन।चाँढो भन्दा चाँढो यसमा काम गर्नु पर्ने अवस्था छ किनभने यही विद्यमान कोभिड १९ बाट धेरै अनलाईन सर्भिस र कामहरु भईसकेका छन् र जुन किसिमको पब्लिकले अनलाइन सर्बिस प्रयोग गरी रहेको सन्दर्भमा बढी साइबर आक्रमण र साइबर घटना हुने कारणले गर्दा तोकिएको समयलाई घटाउनु पर्छ।

समग्रमा यस नितिले ग्लोबल साइबरसुरक्षा सूचकांक (index) मा चाँहि नेपालको स्थानलाई कसरी उक्साउने भन्ने किसिमले अगाडि बढ्नु पर्ने देखिन्छ र यसका लागि एउटा राष्ट्रिय साइबर सुरक्षाको आयोजना ल्याउनु पर्ने व्यवस्था देखिन्छ।विशेष गरी यो प्रविधीको क्षेत्रमा छिटो परिवर्तन हुने प्रविधि भएका र जुन अहिले 5g, मेसिन टु मेसिन टेक्नोलोजीका कुराहरुलाई समेट्न सक्ने गरी रिर्सच र इनोभेसनका कुराहरु यस नितिमा समावेश गर्नु पर्नेछ।साइबर थ्रेटमा टप टार्गेट देशमा परिरहेको सम्बन्धमा साइबर सुरक्षा केन्द्र भएर मात्र हुदैँन कि यसमा सेक्युरिटी अपरेस्नल केन्द्र जसले "threat intelligence monitoring" हरु गर्न सकुन् अथवा कसैले threat पत्ता लगाएकोमा  त्यसतो threat कहाँ गएर रिपोर्टीङ गर्ने त्यसतो कुराहरु पनि उल्लेखित गर्न जरुरी छ। यसका निम्ति ethical hacker लाई नै प्रोत्साहन गर्नु पर्ने देखिन्छ।जसरी बोर्डर नाकाहरुमा चेक जाँच गर्ने देखि अन्तर्राष्ट्रिय गेटवे हरु छन् जुन इन्टरनेट मार्फतबाट आउँछन् त्यहाँ पनि साइबर सुरक्षाको जाँच गर्नु पर्ने कुरा यस नितीमा समावेश गर्नु पर्ने देखिन्छ।

त्यसैगरि डिजीटल सिग्नेचरको व्यवस्था भई सक्दा पनि धेरैले यसलाई अपनाउन नसकेको अवस्था रहेको र यसको महँगीका कारणले गर्दा पनि यसलाई कसरी सस्तो बनाउने अथवा शुल्का घटाउने वा नि:शुल्क गर्न सकिन्छ त्यता तिर योजना बनाउनु पर्ने देखिन्छ।धेरै भन्दा धेरै प्रयोगकर्ताहरु इन्टरनेट/उपकरणमा जोडिसकेको अवस्थामा यस नितिले सार्वजनिक कुञ्जी पूर्वाधार (public key infrastructure) लाई  केन्द्रीकृत गर्नु पर्छ।अहिले सम्म प्रयोगकर्ता प्रमाणीकरण (user authentication) लाई मात्र अभ्यासमा ल्याइरहेको अवस्थामा अब उपकरण प्रमाणीकरण (device authentication) लाई पनि बढावा दिनु पर्ने देखिन्छ।पछिल्लो समयमा जुन किसिमका डाटा लिकेज का घटनाहरु बढी देखिए र पब्लिकको व्यक्तिगत सम्पत्ति, सूचना जुन किसिमको घाटा भई रहेको छ त्यसको लागि डाटा बिमा (Insurance) के कसरी गर्नु पर्छ भन्ने कुराहरु नितिमा अप्नाउनु पर्ने देखिन्छ।

त्यसैगरी अहिलेको अवस्थामा डिजिटल ब्लकचेन (digital blockchain) का कुराहरुलाई समेट्न पर्ने पनि देखिन्छ।साइबर पिडितहरुलाई परामर्श (counseling) गर्नु पर्ने जरुरी हुन्छ र त्यसका लागि परामर्श एकाइ के कसरी आउनु पर्ने हो त्यो कुरा पनि यस नितिमा उल्लेख गर्न पर्ने आवश्यक छ। त्यसैगरी साइबर सुरक्षा desk, फिन-टेक सुरक्षा को बारेमा व्यवस्था गर्नु पर्ने आवश्यकता देखिएको छ।साथै अनलाइन सर्भिस सेवा दिनादुन बढी रहेको क्रममा अनलाईन साइबर सुरक्षा सम्बन्धि नियमन गर्नु पर्छ। यस नितिले निजी क्षेत्रलाई कम फोकस गरेको देखिएको छ त्यसैले यसको लागि public-private partnership के कसरी गरेर यसलाई अगाडी बढाउने भन्ने व्यवस्था यस नितिमा उल्लेखित गर्नु पर्ने देखिन्छ।

### **अन्जली फुयाँल, ग्लोबल चीफ टेक्नोलोजी अफिसर, जेनेस सोलुसन**

यस नितिमा पब्लिक क्लाउडको कुराहरु छुटेको देखिन्छ। अमेजन, अलिबाबा, गुगल, माईक्रोसफ्ट  Amazon, Alibaba, Google, Microsoft जस्ता कम्पनीहरुले प्रदान गर्ने public cloud का कुराहरु यस नितिले समेटेको छैन।नेपालमा डाटा

सेन्टर कम्पनीहरु चलिरहेका छन् र डाटा आउटसोर्स गर्दा त्यो डाटा सेन्टर कम्पनीको जिम्मेवारी कति हुन्छ भन्ने कुरा मध्यनजर गरिएको छैन। ३,५ वर्षको लक्ष्य लिएको समयमा साइबर सुरक्षाका लागि एक महिना समय पनि धेरै हुन जान्छ र त्यो समयमा अहिलेको नितिनै पुरानो(outdated) हुन जान्छ । त्यसकारण समय मूल्याङ्कन गर्न जरुरी छ। अहिलेको समयमा नयाँ प्रविधिहरु आई रहेको बेला जस्तै: क्लाउड कम्प्युटिङ, आर्टिफिसियल, इन्टेलिजेन्स, मशिन लर्निङ, बिग डाटा, इन्टरनेट अफ थिंग्स, भर्चुअल रियालीटी सँगसँगै अरु नयाँ प्रविधी आएकाले यिनि सबै सुरक्षाका कुराहरु साइबर नितिले समेट्नु पर्ने देखिन्छ। यस नितिमा उल्लंघन (breach) र जरिवाना(fine) का कुराहरु पनि समेट्नु पर्ने देखिन्छ।त्यसैगरि नेपालमा सर्भर डाउन हुने समस्यालाई कसरी न्यूनीकरण गर्ने भन्ने कुरालाई पनि जोड दिनु पर्ने देखिन्छ। साथै साइबर सुरक्षा विषय अनिवार्य रुपमा विद्यार्थीहरुको लागि mainstream स्तरमा राख्नु पर्छ।विश्वव्यापी सामाग्रीको वितरणमा अनधिकृत बिक्री (unauthorized sell) र त्यसको प्रभाव पर्यो भने के गर्ने त भन्ने कुराहरु पनि यस नितिमा आएका छैनन्।

**प्रा.डा. सुवर्ण शाक्य, सेन्टर फर साइबर सेक्युरिटी रिसर्च एण्ड इनोभेसन**

नेपालमा सूचना प्रविधिको विकाश सँगै साईबर सुरक्षाको प्रत्याभूत हुनु आवश्यक छ । यस सन्दर्भमा ल्याइएको यस साईबर सुरक्षा नीति २०७८ को मस्यौदा एक सकारात्मक पहल हो । यस नीतिको प्रभावकारी कार्यान्वयको लागि वृहद् साईबर सेक्युरीटी फ्रेमवर्क तर्जुमा गरी प्रभावकारी संरचना निर्माण गर्नु आवश्यक देखिन्छ । बहुसरोकारवाला सहभागितामा आधारित रहि नीजि तथा सार्वजनिक सहकार्यमा आधारित मोडल यसको लागि प्रभावकारी मोडल हुन सक्छ । खासगरी, डिजिटल नेपाल फ्रेमवर्क आईसकेको परिदृश्यमा नेपाल सुहाउँदो अनुसन्धानमा आधारित मानव संशाधन विकास गरी सुरक्षित साईबर स्पेश प्रत्याभूत गर्नु आवश्यक छ । अहिले विकाशको लागि क्लाउड सेवा एउटा महत्वपूर्ण पूर्वाधार हो । यस परिप्रेक्षमा क्लाउड सुरक्षालाई अझ बलियो बनाउनेगरी उच्च प्राथमिकता दिनु आवश्यक हुन्छ । प्रस्तावित मस्यौदा यस पाटोमा चुकेको हुँदा यस सम्बन्धमा थप सुधार गरी यस नीतिलाई अन्तिम रुप दिनु जरुरी छ ।

**अनिल कुमार दत्ता, सहसचिव, सञ्चार तथा सूचना प्रविधि मन्त्रालय**

सूचना तथा संचार प्रविधि मन्त्रालयको सहसचिवको नेतृत्वमा गठित एक समितिले यस नीतिको मस्यौदा तर्जुमा गरेको हो । उक्त समिति मन्त्रालय अन्तरगत विभिन्न निकायहरु तथा अन्य सम्बन्धित मन्त्रालय समेतको विज्ञहरुको पनि यसमा योगदान रहेको छ। हामीले यस नीतिको मस्यौदा गर्दा अन्तर्राष्ट्रिय दूरसंचार युनियनको गाइडलाइनलाई आत्मसात गरेका छौं । साथै अरु देशले के-कस्ता साइबर सुरक्षा नीति बनाएका छन् त्यो हामीले रिफ्रेन्स लिएका छौँ। यस नीतिमा धेरै राम्रा कुराहरु आएको छ। यो नीति छलफल गर्ने आधार बनेको छ। यहाँ दिर्घकालीन सोच, मिशन, उदेश्य, लक्ष्य चुनौति देखि बालबालिका , महिलाहरुका बारेमा सबै कुराहरु राखेका छौँ। यो नीति धेरै चोटि अध्ययन गरी एक-एक शब्द हेरि लिएर आएको नीति हो। अब हामीले बनाउँदा बनाउँदै पनि केहि कुरा छुटेको हुन सक्छ। कुनै पनि डकुमेन्ट पूर्ण हुँदैन। त्यहाँ केही न केही कमि कमजोरी हुन्छ त्यसकारणनै विभिन्ब मन्त्रालय, विभागहरु र सम्बन्धित निकायहरुलाई चिठी पत्र पठाएका छौँ र यस नीतिमा छलफल गर्न र राय सुझाब लिनका निम्ति समय दिएका छौँ। यस कार्यक्रमबाट आएको सुझावहरु यथासंभव समेट्न हामी प्रतिवद्ध छौं ।

**चिरन्जिवी अधिकारी, अध्यक्ष, इन्फर्मेसन सेक्युरीटी रेस्पोन्स टीम नेपाल (एनपीसर्ट)**

हामीले सधैं विदेशबाट आएको प्रतिक्रियालाई उच्च प्राथमिकता दिदैं आएका छौं र नेपालीहरुको प्रतिक्रियालाई कत्तीपनि प्राथमिकता नदिने जुन हामीले देखिराछौं, जुन सत्य पनि हो। यसले नेपालमा भएका जति पनि साइबर सुरक्षा सम्बन्धि काम गर्ने समुदायहरु छन् उनीहरुलाई दुखिद तुल्याउन्छ। त्यस कारण सरोकारवालाहरुबाट आएको प्रतिक्रियालाई राम्रोसगँ अमल गरियोस् । मन्त्रालयले देशको साइबर सुरक्षालाई अज मजबुत बनाउन पहल गर्ने छ भन्ने आशा छ।

**मनोहरकुमार भट्टराई, अध्यक्ष, इन्टरनेट गभर्नेन्स इन्स्टीच्यूट**

हामी दिनहुँ दिन नेटवर्क र डिजिटल पूर्वाधारमा निर्भर हुदैँ गइराखेका छौँ। साइबर सुरक्षाको थ्रेट मूलत: संवेदनशिल पूर्वाधारमा हुन्छ। त्यस कारण संवेदनशिल पूर्वाधार र अन्य डिजिटल सम्पत्तिहरूको सुरक्षामा नीति बढी केन्द्रित हुनुपर्छ। हाम्रो पूर्वाधार लचिलो ( resilient) कसरी हुनसक्छ र थ्रेट ( threat), आक्रमणबाट दिगो कसरी रहन सक्छ भन्ने सबै पाटोलाई समेटेर यस नीतिले हेर्नुपर्छ। महत्वपूर्ण जानकारी पूर्वाधार, डाटा गोपनीयता कसरी सुरक्षित हुन्छ र त्यसबाट हुने अपराध कसरी mitigate गर्न सकिन्छ भन्ने कुराहरु यस नीतिमा आउन जरुरी छ र संविधानले दिएको गोपनीयताको अधिकार सुरक्षित गर्नपर्छ। साईबर सुरक्षा र कन्टेन्ट नियमन फरक फरक हुन् । प्रविधिको प्रगतिको खुसीसगैँ अर्को तिर यहि प्रगतिले पुराउने threat पनि बढि रहेको हुनाले नयाँ प्रविधि र बढ्दो चुनौतीहरूलाई सम्बोधन गर्न नीतिलाई समयमै अद्यावधिक गर्नुपर्छ र यो नीति कसरी कार्यान्वयनको बारेमा कुरा गर्छ भन्ने कुरा पनी स्पष्ट हुन जरुरी छ। नीति बनाउँदा बिभिन्न सरोकारवालाहरुको प्रतिनिधित्व साथै प्रविधि र विज्ञ (frontline)हरुको राय समावेश गर्नुपर्ने हुन्छ।

## सुझाव प्रस्तुतकर्ता संस्थाहरु

### इन्टरनेट गभर्नन्स इंस्टिट्यूट

इन्टरनेट गभर्नन्यान्स इंस्टिट्यूट (आईजीआई) एशिया प्रशान्त क्षेत्रमा इन्टरनेट गभर्नन्यान्स सँग सम्बन्धि अनुसन्धान, क्षमता बिकास, बहस तथा नीति निति निर्माणमा योगदान गर्ने हेतुले ग्रास रूट स्तरमा इन्टरनेट गभर्नन्सको सुदृढीकरणको लागि स्थापित एक मुनाफा रहित संस्था हो । इन्टरनेट गभर्नन्यान्स इंस्टिट्यूटले विभिन्न सुचना प्रविधि सम्बन्धि निति निर्माणमा नागरिक समाजको भुमिकामा रहि सुझाभ हरु प्रदान गर्दै आएको छ । इन्टरनेट गभर्नन्यान्स इंस्टिट्यूट एशिया प्रशान्त क्षेत्रिय इन्टरनेट गभर्नन्यान्स फोरम २०२१ को मुख्य आयोजक पनि रहेको छ ।

### डिजिटल राइट्स नेपाल

डिजिटल राइट्स नेपाल एक गैर-नाफामुखी पहल हो जुन नेपालमा डिजिटल अधिकारको संरक्षण र प्रवर्धन गर्नमा समर्पित छ। यो अनलाइन अभिव्यक्ति र संघको स्वतन्त्रता, अनलाइन गोपनीयता, सुचनाको पहुँच, इन्टरनेट गभर्नन्यान्स, साइबर कानून / नीति र साइबर सुरक्षा जस्ता डिजिटल अधिकार मुद्दाहरूमा केन्द्रित छ। डिजिटल अधिकार नेपाल, प्रासंगिक सरोकारवालाहरूको सहकार्यमा नीति अनुसन्धान र वकालत, सार्वजनिक जागरूकता अभियान, क्षमता निर्माण पहल, र प्राविधिक सहयोग प्रदान गर्न प्लेटफार्महरू सिर्जना गर्नमा संलग्न छ।

### फोरम फर डिजिटल इक्वालिटी

फोरम फर डिजिटल इक्वालिटी एक गैर-नाफामुखी संस्था हो जुन जागरूकता, क्षमता निर्माण, नीति हस्तक्षेप र सामुदायिक संलग्नता मार्फत नेपालमा डिजिटल ग्याप भर्ने अन्तर समर्पित छ। एफडीई मुख्यतया इन्टरनेट गभर्नन्स, टेलिकम नीति, सामुदायिक नेटवर्क, साइबर नीति पहल, र दिगो विकासको लागि सामाजिक उद्यमशीलताको क्षेत्रमा संलग्न छ। एफडीई सबैको समान अवसरको लागि वकालत गर्दछ र उचित, खुला, पारदर्शी, समावेशी र उत्तरदायी साइबरस्पेसका लागि अग्रसर छ।

**इन्फर्मेसन सेक्युरीटी रेस्पोन्स टीम नेपाल (एनपीसर्ट)**

सूचना सुरक्षा प्रतिक्रिया टोली नेपाल, जसलाई एनपीकार्टका नामले चिनिन्छ, सूचना सुरक्षा विशेषज्ञहरूको एक टोली हो जो एकजुट भएर राष्ट्रिय सूचनाको संरक्षण र नेपालमा बढ्दो साइबर सुरक्षा खतराको तत्काल आवश्यकतालाई सम्बोधन गर्छन्।

**सेन्टर फर साइबर सेक्युरिटी रिसर्च एण्ड इनोभेसन**

सीएसआरआईले उद्योग चालित साइबरसुरक्षा विश्लेषण परिणामहरू पुर्‍याउने कुरामा केन्द्रित छ जुन एक प्रभावकारी र वास्तविक समाधानको साथ विश्व साइबरसुरक्षा मुद्दाहरूको समाधान गर्दछ। यसको अभियानले कडा साइबरसुरक्षा अभ्यासहरू समर्थन गर्ने व्यवसाय विश्लेषण द्वारा समस्याहरूको जागरूकता बढाउन मद्दत गर्दछ।

**डेल्टा ल फर्म**

डेल्टा ल फर्म एक काठमाडौंमा आधारित ल फर्म हो जसले विश्वव्यापी पहुँच र मापदण्डहरूको साथ विस्तृत विशेषज्ञता र अनुभव राख्दछ। "ग्राहकहरुको चासो पहिले सेवा गर्ने" भन्ने आदर्शको साथ, डेल्टा ल फर्म नेपालको एक सबैभन्दा विश्वसनीय कानून फर्म हो जसले नवीनता, उत्कृष्टता, व्यावहारिक र सटीक कानूनी समाधानहरूको माध्यमबाट ग्राहकको आवश्यकतालाई गुणस्तरीय सेवा प्रदान गर्दछ। यसको अभियान भनेको उत्तम कानूनी समाधानको साथ ग्राहकहरूको कानुनी आवश्यकताहरूलाई मद्दत गर्नु हो।

**मिडिया एक्शन नेपाल**

मिडिया एक्शन नेपाल अभिव्यक्ति स्वतन्त्रता र मिडिया विकासको प्रबर्द्धन गर्न कार्यरत छ। यसको मुख्य कार्यक्षेत्रमा मिडिया र पत्रकारिता, मानव अधिकार, मिडिया अनुसन्धान, सूचनाको अधिकार, सञ्चार र नीति वकालत समावेश छ।

**डिजिटल मिडिया फाउण्डेशन**

डिजिटल मिडिया फाउण्डेशन  नेपाल अभिव्यक्ति स्वतन्त्रता र मिडिया विकासको प्रबर्द्धन गर्न कार्यरत छ। यसको मुख्य कार्यक्षेत्रमा मिडिया र पत्रकारिता, मानव अधिकार, मिडिया अनुसन्धान, सूचनाको अधिकार, सञ्चार र नीति वकालत समावेश छ।

**नेपाल इन्टर्नेट फाउन्डेसन**

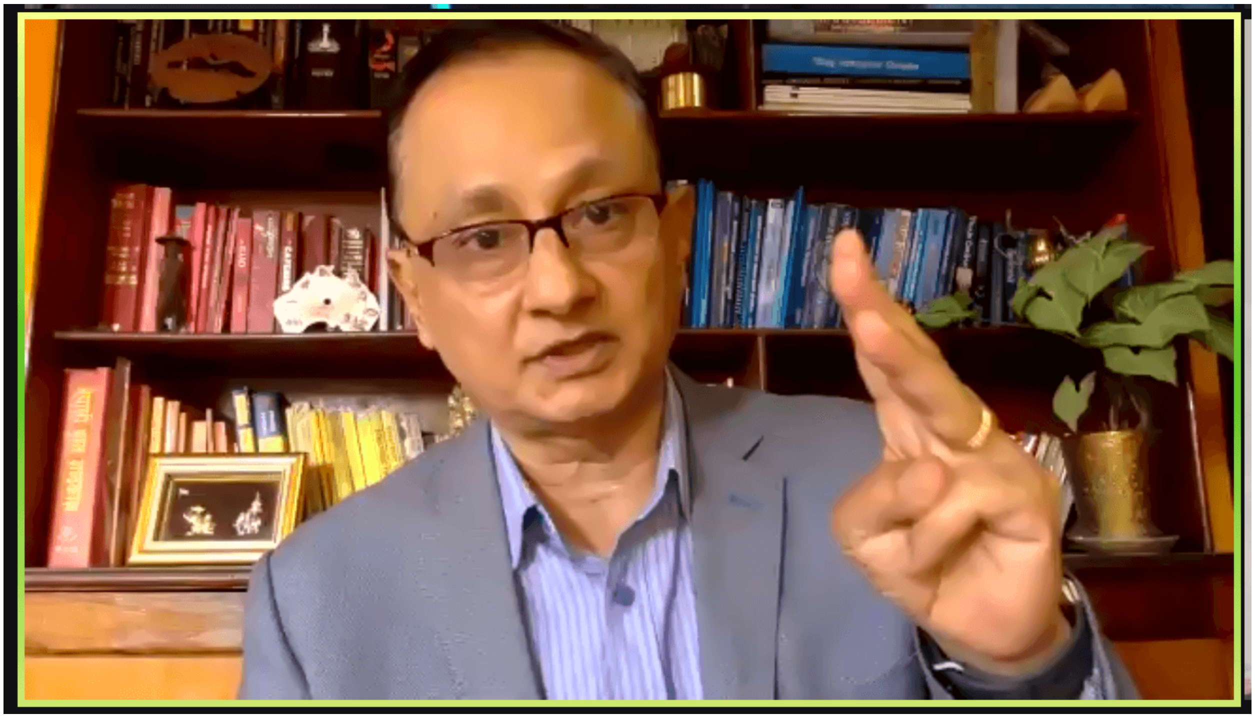
नेपाल इन्टर्नेट फाउन्डेसन (एनआईएफ) एक अनुशन्धान र विकास मञ्च हो जसले नेपालको सन्दर्भमा प्राविधिक र भौगोलिक अनुसन्धानलाई देश भित्र इन्टरनेटको पहुँच अभिवृद्धि गर्न समर्थन र प्रदर्शन गर्दछ। फाउंडेशनको मूल मान्यताहरू प्राथमिकता र राम्रो नीतिहरूको कार्यान्वियन, साइबर कानूनहरु र समाज र यसको सुधारको लागि इन्टरनेटको महत्त्वमा सेट गर्दछ।

जेठ २३, २०७८ मा आयोजित सरोकारवाला छलफलका केही तश्विरहरु

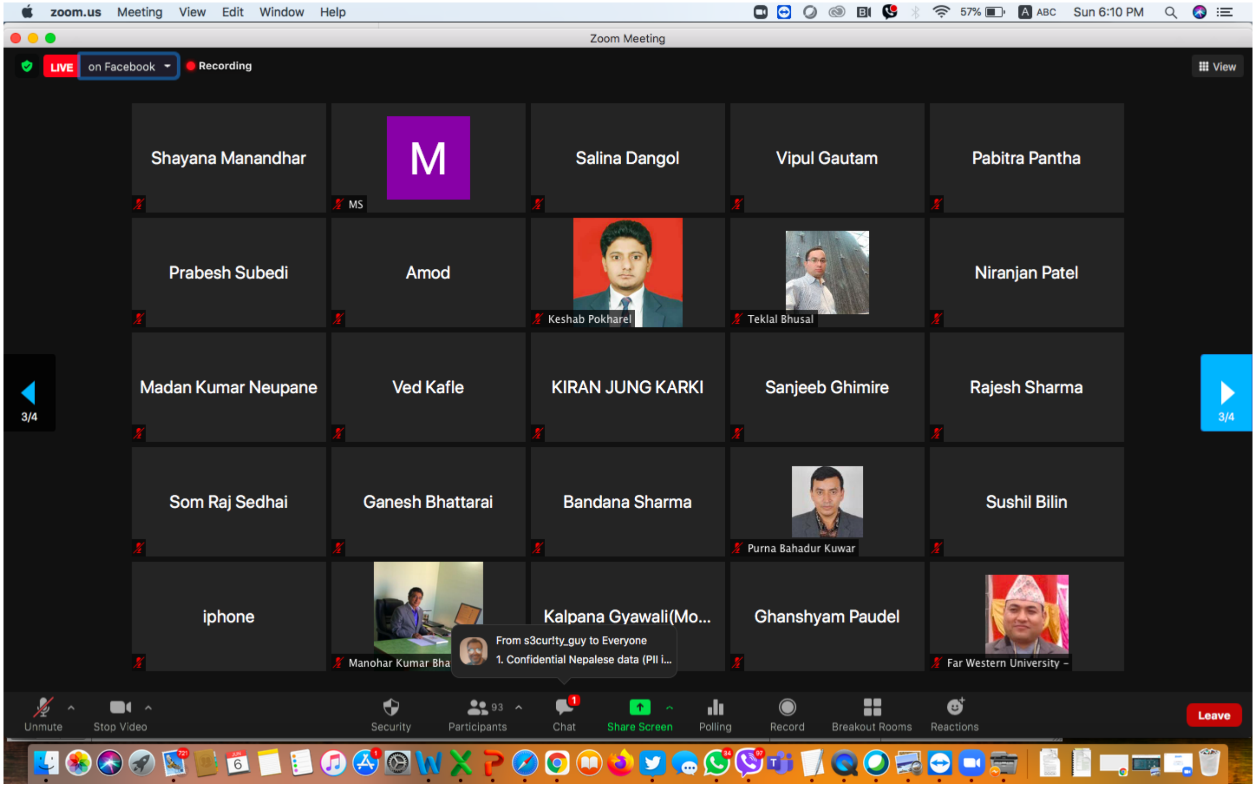
Buddha Air

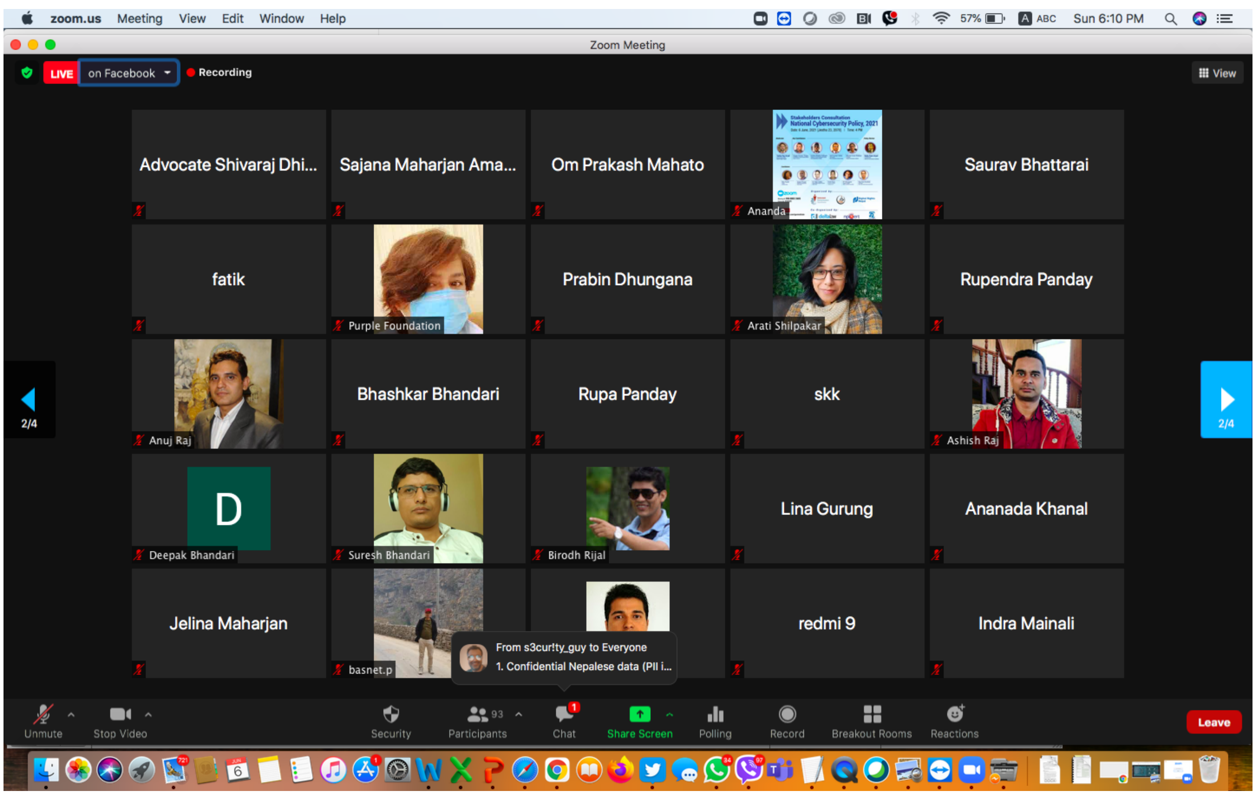
Babu Ram Aryal

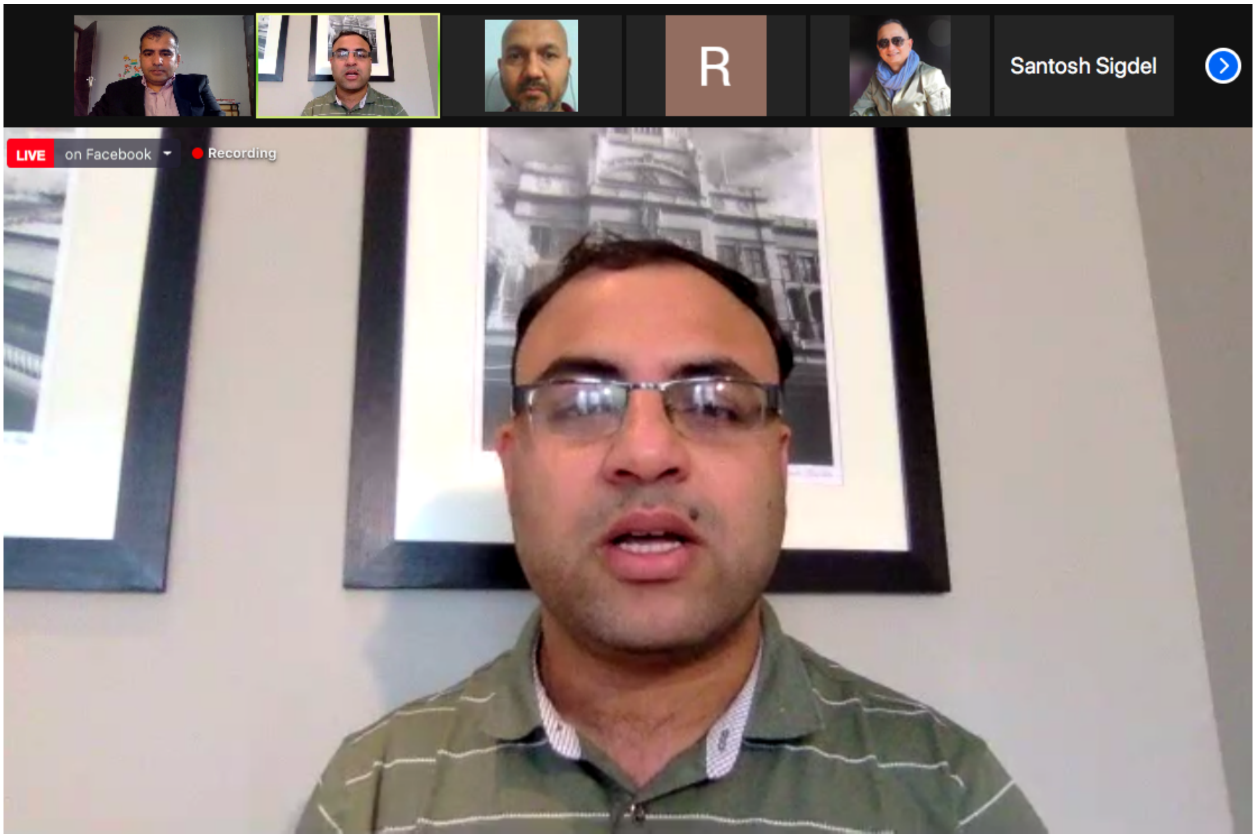
Shrestha
Babu Ram Aryal
Aryal
Taranath Dahal



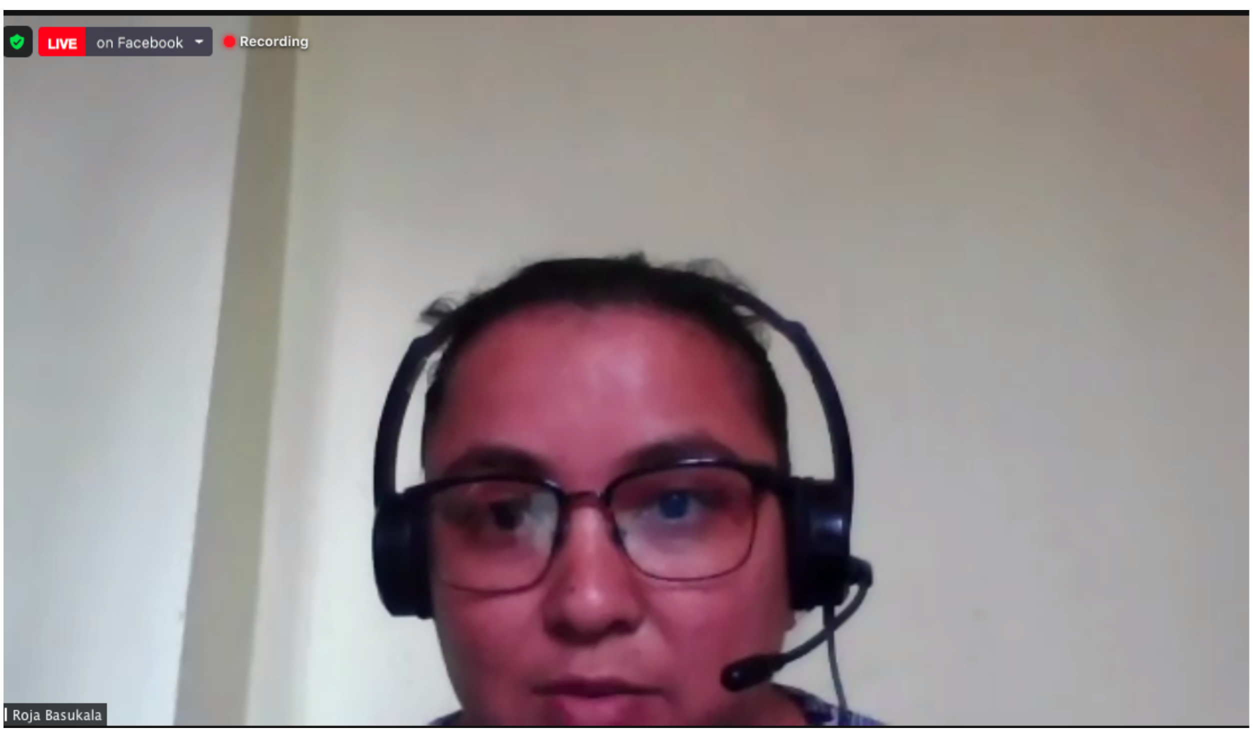
Nitu Pandit


zoom.us Meeting View Edit Window Help
57% ABC Sun 6:10 PM
Zoom Meeting
LIVE on Facebook
Recording
View
Shayana Manandhar
M
MS
Salina Dangol
Vipul Gautam
Pabitra Pantha
Prabesh Subedi
Amod
Keshab Pokharel
Teklal Bhusal
Niranjan Patel
3/4
Madan Kumar Neupane
Ved Kafle
KIRAN JUNG KARKI
Sanjeeb Ghimire
Rajesh Sharma
3/4
Som Raj Sedhai
Ganesh Bhattarai
Bandana Sharma
Purna Bahadur Kuwar
Sushil Bilin
iphone
Manohar Kumar Bha
Kalpana Gyawali(Mo...
From s3curity_guy to Everyone
1. Confidential Nepalese data (PII i...
Ghanshyam Paudel
Far Western University -
Unmute
Stop Video
Security
93
Participants
Chat
Share Screen
Polling
Record
Breakout Rooms
Reactions
Leave


zoom.us Meeting View Edit Window Help
57% ABC Sun 6:10 PM
Zoom Meeting
LIVE on Facebook
Recording
View
Advocate Shivaraj Dhi...
Sajana Maharjan Ama...
Om Prakash Mahato
Ananda
Saurav Bhattarai
fatik
Purple Foundation
Prabin Dhungana
Arati Shilpakar
Rupendra Panday
2/4
Anuj Raj
Bhashkar Bhandari
Rupa Panday
skk
Ashish Raj
2/4
D
Deepak Bhandari
Suresh Bhandari
Birodh Rijal
Lina Gurung
Ananada Khanal
Jelina Maharjan
basnet.p
From s3curity_guy to Everyone
1. Confidential Nepalese data (PII i...
redmi 9
Indra Mainali
Unmute
Stop Video
Security
93
Participants
Chat
Share Screen
Polling
Record
Breakout Rooms
Reactions
Leave

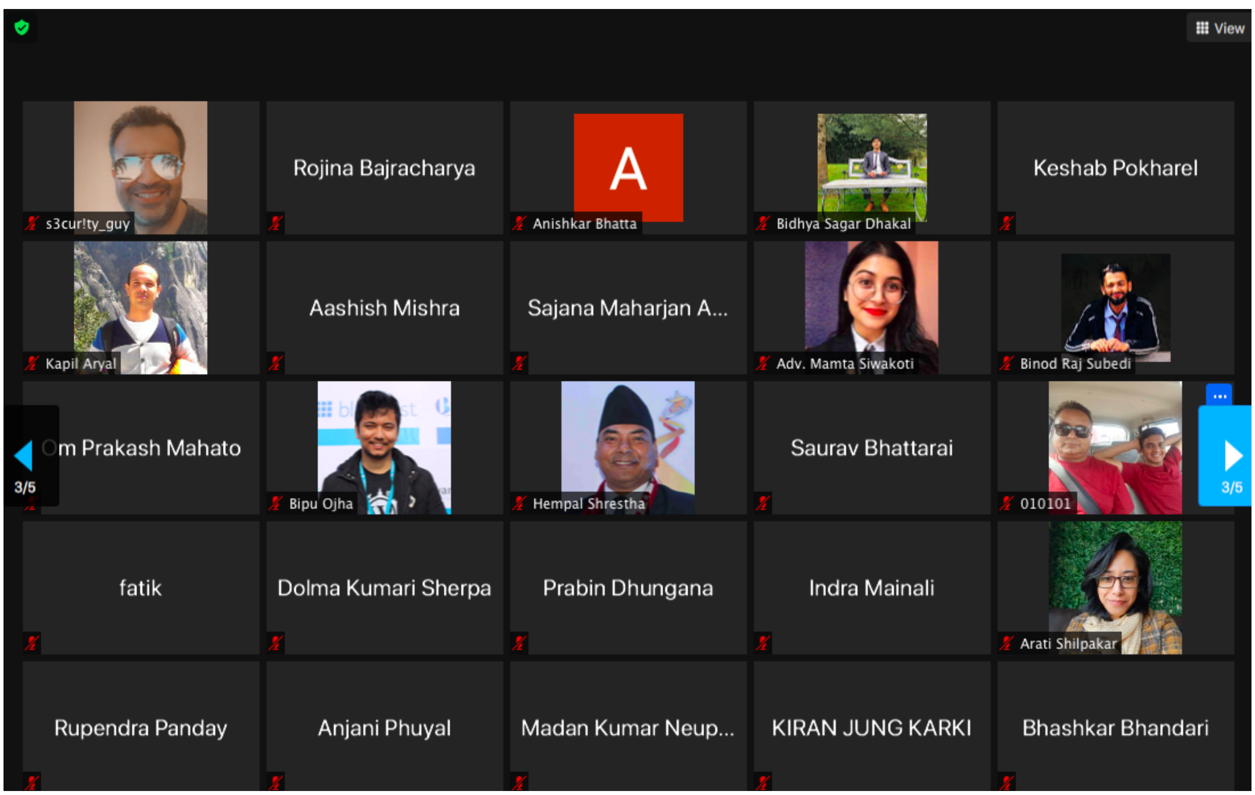


Santosh Sigdel
LIVE
on Facebook
Recording

LIVE
on Facebook
Recording
Roja Basukala

Rupa Panday
skk
Far Western University –
Chandra mohan Ac...
GAJENDRA Sharma
Saroj Bista (YoungInno...
Ashish Raj
Kishor Panth
D
Deepak Bhandari
Karna Nepali
Kundan Raj Sharma
Pralhad Dani Chhetri
Prabin Subedi
surya
Suresh Thapa
4/5
Tek Nath Acharya
Lina Gurung
Namrata Rimal
Bharat Khanal
Rajesh Gurung
S.S
Sadikshya
TUkanath Paudel
Jelina Maharjan
subash


View
s3cur!ty_guy
Rojina Bajracharya
A
Anishkar Bhatta
Bidhya Sagar Dhakal
Keshab Pokharel
Kapil Aryal
Aashish Mishra
Sajana Maharjan A...
Adv. Mamta Siwakoti
Binod Raj Subedi
3/5
Om Prakash Mahato
Bipu Ojha
Hempal Shrestha
Saurav Bhattarai
010101
3/5
fatik
Dolma Kumari Sherpa
Prabin Dhungana
Indra Mainali
Arati Shilpakar
Rupendra Panday
Anjani Phuyal
Madan Kumar Neup...
KIRAN JUNG KARKI
Bhashkar Bhandari