VISION IAS

www.visionias.in

P172

सुरक्षा

सामान्य अध्ययन

VISIONIAS
www.visionias.in

Classroom Study Material

सुरक्षा

संचार नेटवर्क के माध्यम से आंतरिक सुरक्षा को चुनौती

विषय सूची

1. परिचय (Introduction)

संचार नेटवर्क **महत्वपूर्ण सूचना अवसंरचना (Critical Information Infrastructure:CII)** का हिस्सा हैं और यह **अन्य महत्वपूर्ण अवसरंचनाओं** जैसे ऊर्जा; परिवहन; बैंकिंग एवं वित्त; दूरसंचार; रक्षा; अंतरिक्ष; कानून प्रवर्तन, सुरक्षा और आसूचना; संवेदनशील सरकारी संगठन; सार्वजनिक स्वास्थ्य; जलापूर्ति; महत्वपूर्ण विनिर्माण; ई-शासन आदि के कनेक्टिविटी के लिए अत्यंत महत्वपूर्ण हैं। संचार नेटवर्क के प्रति जोखिम, नेटवर्क के माध्यम से होने के साथ-साथ नेटवर्क के लिए भी हो सकते हैं।

दूरस्थ स्थानों से संचालित या समन्वित साइबर-हमलों में इन महत्वपूर्ण संचार नेटवर्कों को जोखिम में डालने का और इन पर निर्भर महत्वपूर्ण अवसंरचनाओं को बाधित करने का सामर्थ्य होता है। भारत में, जहाँ आतंकवाद, उग्रवाद, नक्सलवाद, शत्रु राष्ट्र द्वारा किये गए कथित साइबर हमलें आदि के रूप में विभिन्न जोखिम पहले से विद्यमान हैं, वहां संचार नेटवर्क की सुरक्षा आंतरिक सुरक्षा के लिए महत्वपूर्ण चुनौतियां प्रस्तुत करता है।

2. संचार नेटवर्क क्या है

(What is Communication Network)

संचार नेटवर्क इलेक्ट्रॉनिक यंत्रों और उपकरणों का अंतःसंयोजन है जो उन्हें डाटा, वाइस और वीडियो के रूप में सूचना को संचारित करने में सक्षम बनाता है। नेटवर्क अवसंरचना में हार्डवेयर और सॉफ्टवेयर संसाधन जैसे मोबाइल, लैपटॉप, संवेदक सेंसर, सर्वर, वेब एप्लीकेशन, उपग्रह, SCADA, LAN, WAN और ऑप्टिक फाइबर नेटवर्क इत्यादि सम्मिलित हैं। यह उपयोगकर्ताओं, प्रक्रियाओं, अनुप्रयोगों, सेवाओं और बाहरी नेटवर्कों/इंटरनेट के बीच संचार मार्ग और सेवाएं प्रदान करता है।

महत्वपूर्ण अवसंरचना या क्रिटिकल इंफ्रास्ट्रक्चर (CI) - IT अधिनियम 2000 की धारा 70 के तहत, महत्वपूर्ण सूचना अवसंरचना (CII) को इस प्रकार परिभाषित किया गया है: "ऐसा कंप्यूटर संसाधन, जिसकी अक्षमता या विनाश, राष्ट्रीय सुरक्षा, अर्थव्यवस्था, सार्वजनिक स्वास्थ्य या सुरक्षा पर दुष्प्रभाव डालेगी।"

भारत में संचार प्रौद्योगिकियों और सूचना प्रणालियों के बढ़ते अभिसरण के साथ, महत्वपूर्ण क्षेत्रक अपने CII पर तेजी से निर्भर हो रहे हैं। ये CII विभिन्न भौगोलिक स्थानों पर परस्पर संबद्ध, परस्पर निर्भर, जटिल और वितरित होते हैं। आतंकवादी हमलों से लेकर संगठित अपराध, जासूसी, दुर्भावनापूर्ण साइबर गतिविधियों आदि से CII को होने वाले जोखिम निरंतर बढ़ रहे हैं। इन CII की क्रियाशीलता में होने वाले किसी भी प्रकार के विलंब, विरूपण या व्यवधान में अन्य CII को भी सोपानी रूप से प्रभावित कर राजनीतिक, आर्थिक, सामाजिक या राष्ट्रीय अस्थिरता पैदा करने की क्षमता है। इस प्रकार CII और राष्ट्र की महत्वपूर्ण अवसंरचनाओं की सुरक्षा सरकार की सर्वोच्च चिंताओं में से एक है।

3. आधुनिक जगत में संचार नेटवर्क की भूमिका

(Role of Communication Network in Today's World)

- **महत्वपूर्ण अवसंरचना क्षेत्रकों द्वारा**, संचार नेटवर्क का उपयोग केवल सहायक कार्यों के लिए ही नहीं अपितु प्रत्येक महत्वपूर्ण कार्य के लिए किया जाता है, चाहे वह कार्य मानव संसाधन प्रबंधन, उत्पादन, परियोजना प्रबंधन या व्यावसायिक विश्लेषण से संबन्धित हो।
- यह **वाइस और डाटा संचार** को सक्षम बनाता है।

- वित्तीय क्षेत्र तेजी से डिजिटल प्रौद्योगिकियों जैसे नेट बैंकिंग, एटीएम नेटवर्क इत्यादि का उपयोग कर रहा है और ये संचार नेटवर्क पर निर्भर हैं। बैंकिंग क्षेत्रक की संचार अवसंरचना पर कोई भी अतिक्रमण **भारत की वित्तीय स्थिरता** के लिए खतरा पैदा कर सकता है।
- यह **अवसंरचना प्रणालियों, उपप्रणाली और घटकों** को इस प्रकार संयोजित करता है कि वे बाद में अत्यधिक परस्पर संबद्ध और परस्पर निर्भर हो जाते हैं। उदाहरण के लिए, संचार नेटवर्किंग प्रौद्योगिकियों का उपयोग करके विद्युत क्षेत्र, स्मार्ट ग्रिड में बदल रहा है।
- इसी प्रकार, स्मार्ट सिटी, स्मार्ट कृषि आदि परस्पर संबद्ध प्रणालियों पर बहुत अधिक निर्भर हैं।
- बड़ी-बड़ी औद्योगिक और विनिर्माण सुविधाएं भी स्वचालन (ऑटोमेशन) का उपयोग करती हैं और इस प्रकार सूचना अवसंरचना पर निर्भर करती हैं|
- इसके अतिरिक्त, सरकार, राष्ट्रीय ई-गवर्नमेंट प्लान, डिजिटल इंडिया, ई-क्रांति आदि जैसे विभिन्न कार्यक्रमों के माध्यम से ई-गवर्नमेंट के निर्माण में अत्यधिक संसाधनों का निवेश कर रही है।
- इस प्रकार, नेटवर्क अवसंरचना **संपूर्ण महत्वपूर्ण अवसंरचना का आधार** बन गई है और यह हमारे जीवन में **सर्वत्र व्याप्त** है।

3.1. विशेष विषय - स्मार्ट शहर में संचार नेटवर्क

(Special Case-Communication Network in the Smart city)

संचार, स्मार्ट शहरों में अति महत्वपूर्ण भूमिका निभाते हैं। यातायात की स्थिति को प्रसारित करने से लेकर, वायु की गुणवत्ता के आंकड़ों को प्रदर्शित करने, और नागरिकों को ऐप्स या कंप्यूटरों के माध्यम से सुदूर सेवाएँ प्रदान कराने तक संचार, एक स्मार्ट शहर के प्रत्येक पहलू को संचालित करता है। संचार संबंधी अवसंरचनात्मक नेटवर्क किसी शहर को भविष्य का शहर बनाते हैं।

भारतीय स्मार्ट शहरों के लिए संचार नेटवर्क में सम्मिलित हैं-

- तारयुक्त नेटवर्क - ऑप्टिकल फाइबर नेटवर्क
- तार-रहित नेटवर्क - 4G, 5G, वाई-फाई
- सैटेलाइट नेटवर्क
- मशीनों में पारस्परिक कनेक्टिविटी
- MAN, WAN, PAN, HAN सहित विभिन्न नेटवर्क
- समर्पित संसाधन जिन्हें महत्वपूर्ण संचार या आपात स्थितियों व आपदाओं के दौरान संचार के लिए आबंटित किया जा सकता है।

4. संचार नेटवर्क के लिए खतरे

(Threats to Communication Networks)

चूंकि संचार नेटवर्क की विफलता के कारण होने वाली क्षति बहुत अधिक होती है, इसलिए व्यवधान (भंग) उत्पन्न करने के लिए ये क्षमतावान सॉफ्ट टारगेट होते हैं। नेटवर्क अवसंरचना के प्रति खतरे को व्यापक रूप से दो श्रेणियों में वर्गीकृत किया जा सकता है: प्राकृतिक खतरे और मानव प्रेरित खतरे।

4.1. प्राकृतिक खतरे (Natural Threats)

प्राकृतिक खतरों में बाढ़, भूकंप, सुनामी, ज्वालामुखीय गतिविधियां सम्मिलित हैं। ये प्राकृतिक आपदाएं भौतिक रूप से संचार नेटवर्क को क्षति पहुंचा सकती हैं। उदाहरण के लिए, एक ICT द्वारा संचालित स्मार्ट सिटी में, यदि एक मामूली भूकंप स्थानीय दूरसंचार टावरों को तोड़ देता है, तो यह ICT पर निर्भर सभी उपयोगी सेवाओं को बाधित कर देगा। जैसे, बिजली और जल आपूर्ति आदि। स्थानीय ATM और बैंकिंग सेवाएं काम करना बंद कर सकती हैं। इसी प्रकार, सौर तूफान, पृथ्वी की परिक्रमा कर रहे संचार उपग्रहों को क्षति पहुंचा सकते हैं और यह उपग्रह संचार पर निर्भर सभी क्षेत्रों को प्रभावित करेगा जैसे मौसम पूर्वानुमान, मोबाइल सेवाएं, DTH, टेली-मेडिसिन आदि।

4.2. मानव-प्रेरित खतरे (Human induced threats)

- विभिन्न कर्ता संचार नेटवर्क के लिए खतरे का काम कर सकते हैं, जैसे -
  - असंतुष्ट कर्मचारियों/सोशल इंजीनियरिंग द्वारा मनोवैज्ञानिक रूप से भड़काकर फंसाए गए कर्मचारियों के रूप में संगठन के कार्मिक
  - आर्थिक, सैन्य या विरोधी राष्ट्र
  - आतंकवादी संगठनों से सम्बद्ध आपराधिक समूह
- **खतरों के प्रकार-** इसमें दुर्भावनापूर्ण कर्ताओं द्वारा हानि या क्षति के इरादे से सिस्टम तक पहुंच प्राप्त करने के सभी प्रयास सम्मिलित हैं। खतरा पैदा करने वाले कर्ता नेटवर्क में वांछित स्थान तक पहुंच प्राप्त करने के लिए एप्लिकेशन सॉफ्टवेयर, नियंत्रण प्रणाली सॉफ्टवेयर, हार्डवेयर या यहां तक कि संगठनों के व्यक्तियों के भीतर अंतर्निहित विरोधों का लाभ उठाते हैं।
- एक बार नेटवर्क को भंग करने या नियंत्रित करने के बाद वे कमांड दे सकते हैं, डिजाइन या विन्यास (configuration) जैसी संवेदनशील जानकारी चुरा सकते हैं या इंटरफेस में उपलब्ध जानकारी को उपयोगहीन (करप्ट) बना सकते हैं।
- सभी कर्ताओं की अलग-अलग क्षमताएं तथा योग्यताएं होती हैं। एक राष्ट्र के पास दीर्घकालिक परिचालनों को संचालित करने तथा उसे संधारणीय बनाए रखने के आवश्यक तकनीकी साधन एवं उपाय होते हैं, जिनमें जासूसी, डेटा या प्रत्यायक (क्रेडेंशल्स) की चोरी तथा हमलों का निष्पादन एवं निगरानी सम्मिलित हैं।
- आतंकवादी संगठनों पर बाजार में उपलब्ध पेशेवर कौशल तक सरल पहुंच के कारण CII पर हमला करने के अपराध में सक्षम होने का भी आरोप है।

नेटवर्क ऑपरेशन इंफ्रास्ट्रक्चर में **संभावित लक्ष्य** निम्नलिखित होते हैं-

- राउटर, स्विच, फ़ायरवॉल, मोबाइल फोन, डेटाबेस, डोमेन नेम सिस्टम (DNS) सर्वर के रूप में डिवाइस या उपकरण;
- वेब पोर्टल, प्रोटोकॉल, पोर्ट तथा संचार चैनल;
- सैटेलाइट नेटवर्क संचार प्रणाली;
- क्लाउड-आधारित सेवाओं जैसे नेटवर्क अनुप्रयोग;
- SCADA

आंतकी हमलों के उदाहरण और उनके प्रभाव

- वर्ल्ड ट्रेड सेंटर पर 9/11 के आक्रमण ने बैंकिंग, वित्त, दूरसंचार, आपातकालीन सेवाओं, हवाई और रेल यातायात के साथसाथ ऊर्जा एवं जलापूर्ति को सीधे-सीधे प्रभावित किया।
- मुंबई और लंदन के शहरी यातायात व्यवस्था पर आक्रमण ने आम जनजीवन को प्रभावित किया।

मानव जनित खतरों के कर्ताओं का वर्गीकरण

यद्यपि, मानव जनित खतरे के कर्ताओं के बीच कोई स्पष्ट भेद नहीं है, परंतु इन्हें व्यापक रूप से निम्नलिखित के रूप में वर्गीकृत किया जा सकता है -

- **आतंकवादी संगठन एवं गैर-राज्य कर्ता**

आमतौर पर एक आतंकवादी संगठन का प्राथमिक उद्देश्य पीड़ितों के साथ-साथ सामान्य जनों को भी करना होता है। संचार नेटवर्क पर हमला (भौतिक या साइबर) पीड़ितों व जन सामान्य के मनोविज्ञान पर प्रभावी तथा दूरगामी प्रभाव डालता है। इस प्रकार, आतंकवादियों का उद्देश्य पूरा होता है।

शिक्षित युवाओं के बीच बढ़ते कट्टरपंथीकरण या उग्रवाद के साथ ही, इन आतंकवादी संगठनों के पास कंप्यूटर, नेटवर्क व प्रोग्रामिंग के अच्छे कामकाजी ज्ञान रखने वाले मानव संसाधनों तक सरल पहुंच हो गई है। वास्तव में, इस्लामिक स्टेट ऑफ इराक एंड सीरिया (ISIS) एवं लश्कर-ए-तैयबा जैसे कुछ समूह स्मार्टफोन के लिए अपने स्वयं के सुरक्षित संचार अनुप्रयोग विकसित करने के लिए जाने जाते हैं।

साइबर क्षमताओं को प्राप्त करने वाले राज्य

कई देशों ने आक्रामक साइबर क्षमताओं को विकसित करने के लिए संस्थानों की स्थापना की है। संयुक्त राज्य अमेरिका ने आक्रामक क्षमताओं के लिए यूएस साइबर कमांड (USCYBERCOMM) का गठन किया है। परिणामस्वरूप, दक्षिण कोरिया ने 2009 में साइबर वारफेयर कमांड बनाया, यह उत्तर कोरिया की साइबर युद्ध इकाइयों के निर्माण का भी प्रत्युत्तर था। ब्रिटिश सरकार संचार मुख्यालय (GCHQ) तथा फ्रांस ने भी साइबर बल की तैयारी आरंभ कर दिया है। रूस सक्रिय रूप से साइबर युद्ध की तैयारी कर रहा है। 2010 में चीन ने USCYBERCOMM के निर्माण के प्रत्युत्तर में रक्षात्मक साइबर युद्ध व सूचना सुरक्षा को समर्पित अपना पहला विभाग आरंभ किया। इस प्रकार, यह होड़ पूरे विश्व में है।

विरोधी राज्यों के समर्थन के साथ ही, आतंकवादी समूह अधिक प्रामाणिक खतरे बन गए हैं क्योंकि पर्याप्त वित्तीय संसाधनों तथा प्रौद्योगिकी व कौशल तक उनकी सरल पहुंच है।

आतंकवादी संगठनों के अतिरिक्त, साइबर अपराधी भी महत्वपूर्ण समझे जाने वाली सूचना अवसंरचनाओं के लिए सीधा खतरा हैं। उनका मुख्य उद्देश्य मौद्रिक लाभ है, जिसका किसी भी विरोधी (आतंकवादी समूह या राष्ट्र) द्वारा सरलता से लाभ उठाया जा सकता है।

- **राज्य प्रायोजित कर्ता**

संसाधनों पर उनके नियंत्रण के कारण राष्ट्र सूचना अवसंरचना के लिए सबसे शक्तिशाली खतरा हैं। किसी भी परिस्थिति में एक-दूसरे के CII को लक्षित करने से राष्ट्रों को रोकने के लिए विश्व स्तर पर सर्वसम्मत मानदंडों या कानूनी उपायों की अनुपस्थिति में CII एक आकर्षक लक्ष्य बना हुआ है। इन परिस्थितियों में, साइबर-आधारित हमलों में युद्ध जैसा प्रभाव उत्पन्न करने की क्षमता है, क्योंकि उनका उपयोग राष्ट्रों को अस्थिर करने के लिए किया जा सकता है।

हाल ही में, **एडवांस्ड परसिस्टेंट थ्रेट्स (APT)** ने खतरे के परिदृश्य को पूर्णरूपेण बदल दिया है। ये राज्य प्रायोजित अभियान हैं और महत्वपूर्ण सूचना अवसंरचना, विशेष रूप से संचार नेटवर्क पर लक्षित हैं। APT, SQL इंजेक्शन, मैलवेयर, स्पाइवेयर, फिशिंग तथा स्पैम सहित विभिन्न प्रकार की तकनीकों का उपयोग करके घुसपैठ तथा सूचना चोरी के परिष्कृत, लक्षित तथा लंबे समय के प्रयास हैं। APT के हमले संवेदनशील सर्वरों में घुसपैठ करते हैं, जैसे ईमेल सर्वर। वे इस प्रकार से डिजाइन किए गए होते हैं कि प्रशासकों से कभी-कभी वर्षों तक छिपे रहते हैं। चूंकि APT बेहद उन्नत व नियोजित रूप से तथा सतर्कतापूर्वक निष्पादित होते हैं, वे शायद ही कभी कोई संकेत छोड़ते हैं। इसलिए सुरक्षा एवं फोरेंसिक के पारंपरिक साधनों को वे अक्षम कर देते हैं। APT का उपयोग औद्योगिक संचालन में व्यवधान या यहां तक कि औद्योगिक उपकरणों के विनाश के लिए भी किया जा सकता है।

5. संचार नेटवर्क सुरक्षा का महत्व

(Importance of Securing Communication Networks)

- संचार नेटवर्क, **डिजिटल परिवेश का आधार** निर्मित करते हैं। **समग्र साइबर सुरक्षा सुनिश्चित करने के लिए**, सभी प्रकार के संभावित खतरों (मानव व प्राकृतिक) से संचार नेटवर्क को सुरक्षित करना आवश्यक है।

एस्टोनिया का मामला

संचार नेटवर्क की विफलता के प्रभाव की प्रबलता को 2007 के एस्टोनियन मामले से समझा जा सकता है। यह संचार नेटवर्क से सबसे सघनतापूर्वक जुड़े देशों में से एक है तथा ई-सरकार, इंटरनेट वोटिंग तथा ऑनलाइन बैंकिंग लेनदेन (98 प्रतिशत) जैसी सुविधाओं में अग्रणी है। भारत भी उसी मार्ग का पालन करने का इच्छुक है।

2007 में, एस्टोनिया ने इंटरनेट ट्रैफिक में बड़े पैमाने पर वृद्धि देखी गयी, जिससे उसके बैंकों, प्रसारणकर्ताओं, पुलिस, संसद और मंत्रालयों के नेटवर्क धराशायी हो गए। इस हमले के लक्ष्य पर इसका बुनियादी सूचना ढांचा था। इस हमले ने एस्टोनिया को व्यावहारिक रूप से ठहराव की स्थिति में पहुंचा दिया था।

- **राष्ट्रीय सुरक्षा:** संचार नेटवर्क में व्यवधान देश की स्थिरता को प्रभावित कर सकता है, विशेष रूप से यदि महत्वपूर्ण क्षेत्रकों वाले संचार नेटवर्क लक्षित हों। संचार नेटवर्क की विफलता सुरक्षा एजेंसियों को अप्रभावी करने की क्षमता रखती है। इसे निम्नलिखित द्वारा समझा जा सकता है -
  - सुरक्षा एजेंसियां पदानुक्रम का पालन करती हैं तथा कमांड की कुछ श्रृंखलाएं होती हैं। जानकारी (क्षैतिज तथा लंबवत) के आदान-प्रदान के लिए सुरक्षा बल व एजेंसियां वायरलेस हैंडसेट जैसी संचार तकनीकों का उपयोग करती हैं। इन उपकरणों के लिए सुदृढ़ संचार नेटवर्क अवसंरचना की आवश्यकता होती है। इस प्रकार के संचार नेटवर्क अवसंरचना पर हमले का सुरक्षा एजेंसियों की कार्य क्षमताओं पर दूरगामी प्रभाव हो सकता है।
  - ऐसी विफलताओं के कारण स्थानीय खुफिया अधिकारी द्वारा एकत्र खुफिया सूचनाएं निर्णय लेने वाले सक्षम अधिकारियों तक नहीं पहुंचाई जा सकती हैं। परिणामस्वरूप निर्णय लेने में देरी से सेनाओं तथा अधिकारियों को समय पर सुधारात्मक कार्रवाई में बाधाओं का सामना करना पड़ सकता है।
- **बढ़ती परस्पर निर्भरता:** परिवहन, संचार तथा सरकारी सेवाओं जैसे सभी महत्वपूर्ण क्षेत्रक विद्युत आपूर्ति की अपनी मूल आवश्यकता के लिए विद्युत/ऊर्जा क्षेत्रक पर निर्भर करते हैं। रेलवे, हवाई अड्डे तथा संचार प्रणालियों जैसे स्विचिंग सेंटर या टेलीफोन एक्सचेंज को ऊर्जा इन्हीं से प्राप्त होता है। एक परस्पर निर्भर कार्य प्रणाली में विद्युत क्षेत्र स्वयं ईंधन की आपूर्ति के लिए परिवहन पर निर्भर रहता है तथा अपने डेटा के प्रसारण के लिए या संचरण/ वितरण नेटवर्क को बनाए रखने के लिए संचार पर निर्भर रहता है। इसी प्रकार, सरकार सभी मौद्रिक आवश्यकताओं के लिए बैंकिंग व वित्तीय सेवाओं पर निर्भर रहती है। बैंकिंग क्षेत्र प्रौद्योगिकी द्वारा संचालित है तथा संचार क्षेत्रक बैंकिंग के निर्बाध परिचालनों में महत्वपूर्ण भूमिका निभाता है।
- **डिजिटल संप्रभुता की रक्षा:** व्यक्तिगत परिप्रेक्ष्य में डिजिटल संप्रभुता, कौन-सा डेटा एकत्र, वितरित, उपयोग या सहेजा जा सकता है, इसके विषय में इंटरनेट उपयोगकर्ताओं द्वारा स्वतंत्र रूप से निर्णय लेने के नियंत्रण एवं अधिकार से संबंधित है। चूंकि ये सभी डेटा संचार नेटवर्क पर उपलब्ध हैं, इसलिए संचार नेटवर्क के असुरक्षित होने पर लोगों की डिजिटल संप्रभुता प्रभावित होगी।
- **डिजिटल प्रौद्योगिकी को विश्वासनीय बनाना:** इंटरनेट हमारे जीवन के सभी पहलुओं में प्रवेश कर रहा है तथा सरकार भी अपने लोगों को डिजिटल सेवाओं, जैसे महत्वपूर्ण दस्तावेजों को संग्रहित करने के लिए डिजी-लॉकर, का उपयोग करने के लिए प्रोत्साहित कर रही है। लोगों द्वारा इन सेवाओं का उपयोग करने तथा ऐसी पहल में भाग लेने के लिए डिजिटल संचार पर लोगों के विश्वास को बनाए रखने के लिए इन संचार नेटवर्क को सुरक्षित करना आवश्यक है।

6. संचार नेटवर्क की सुरक्षा सुनिश्चित करने में चुनौतियाँ

(Challenges in Securing Communication Network)

संचार नेटवर्क सुनिश्चित करने की प्रक्रिया में कई चुनौतियाँ है; उनमे से कुछ पर नीचे चर्चा की गई है:

- **उपकरणों और प्रौद्योगिकी का विदेशी स्रोतों पर निर्भर रहन:** संचार प्रणाली के अधिकांश सॉफ्टवेयर और हार्डवेयर अन्य देशों से आयात किये जाते हैं (कुल दूरसंचार उपकरणों के आयात में चीनी उपकरणों का 60% भाग है)। हाल ही में, भारतीय विद्युत् और इलेक्ट्रॉनिक निर्माता एसोसिएशन (IEEMA) ने विद्युत् ग्रिड के संचालन और प्रबन्धन में विदेशी स्वचालन और संचार व्यवस्था के बढ़ते उपयोग से महत्त्वपूर्ण विद्युत् सरंचना में "सुरक्षा संबंधी खतरे" पर प्रकाश डाला था। इन संचार उपकरणों में विद्यमान किसी मैलवेयर और स्पाईवेयर को किसी भी समय रिमोट द्वारा सक्रिय किया जा सकता है।
- **परिवर्तित होती तकनीकी:** प्रौद्योगिकी विकास की गति का अर्थ है सुरक्षा प्रणालियों के लिए निरंतर खतरों का विकसित होना। इसके कारण निरंतर ऐसी सुरक्षा प्रणालियों को विकसित किया जाता है जो इन हमलों को निष्फल कर सकें। लेकिन यह एक कठिन कार्य बन जाता है क्योंकि हमलावर के पास अनाम बने रहने की सुविधा है और प्रणाली को लक्षित करने के लिए व्यापक विकल्प उपलब्ध हो सकते हैं।
- **राज्य और गैर-राज्य कर्ताओं की संलिप्तता:** आजकल के खतरे और उनकी पहचान और लक्ष्यों के सन्दर्भ अस्पष्ट, अनिश्चित और अव्यक्त हैं। जहाँ राष्ट्रों के पास व्यापक राजनीतिक और सुरक्षा संबंधी प्रेरण हो सकते है, लेकिन गैर-राज्य कर्ताओं के पीछे निहित प्रेरणों को समझना कठिन है और यह मौद्रिक लाभ से प्रेरित आतंकवाद या संकीर्ण राजनीतिक एजेंडा भी हो सकता है।
- **परस्पर निर्भरताओं की अपर्याप्त समझ:** महत्त्वपूर्ण अवसंरचना के जटिल होने के कारणों में से यह एक है। अंतरक्षेत्रक और अंतराक्षेत्रक निर्भरताओं को समझने के लिए वैज्ञानिक विश्लेषण और उपकरणों की कमी प्राथमिक कारण है, इसीलिए हमारी सुरक्षा एजेंसियां परस्पर निर्भरताओं को समझ नहीं पायी हैं।
- **सरंचनात्मक चुनौतियाँ:** भारत को सरंचनात्मक चुनौतियों का भी सामना करना पड़ता है। यहां संघ और राज्यों के बीच शक्तियों का सीमांकन है और सुरक्षा एजेंसियों की बहुतायत है।
    - **संघवाद** – साइबरस्पेस भौगोलिक सीमाओं से परे होता है। साइबर सुरक्षा 7वीं अनुसूची की तीनों सूचियों में कहीं भी विशिष्ट रूप से किसी एक में भी सूचीबद्ध नहीं है। इस कारण से, कई बार केंद्र सरकार को अपनी विभिन्न पहलों के विरोध में राज्य सरकारों से चुनौती का सामना करना पड़ता है। राज्य सरकारों की प्रमुख चिंता भारत की संघीय राजनीति को सरंक्षित रखने की होती है। उदाहरण के लिए जब सुरक्षा एजेंसियों के बीच आसूचना समन्वय के लिए NATGRID की स्थापना की गयी थी तो राज्य सरकारों ने इसका विरोध किया था।
    - **सुरक्षा एजेंसियों के बीच समन्वय:** सरकारी क्षेत्रक के साथ-साथ निजी विभिन्न संगठनों ने साइबर सुरक्षा एजेंसियों की स्थापना की है, जो स्वयं अपने अधिदेश और हितों की सेवा के लिए अधिक संरेखित हैं। इस प्रकार का खंडित दृष्टिकोण बहुत बड़ी चुनौती बनता है, क्योंकि ये सब एजेंसियां अपनी-अपनी सीमा में कार्य करती हैं और अपने हितधारकों के छोटे समूहों के अनुरूप ही नीतियाँ तैयार करती हैं।
    - साइबर खतरों का आकलन कर सकने और उसके प्रति प्रभावी अनुक्रिया दे सकने वाले **राष्ट्रीय सुरक्षा आर्किटेक्चर का भी अभाव** है।

- **सूचना अवसरंचना का एक महत्त्वपूर्ण भाग का स्वामित्व और संचालन निजी क्षेत्रक के पास है,** जैसे दूरसंचार क्षेत्रक (अधिकाँश निजी क्षेत्रक का है), बैंकिंग क्षेत्रक (बड़ी संख्या में निजी बैंक हैं), स्टाक एक्सचेंज, ऊर्जा उपयोगिताएं आदि। उन्हें सुरक्षा ऑडिट, अन्य विनियमन और अन्य फ्रेमवर्क उनकी अपनी लागत में वृद्धि के रूप में दिखाई देती है।
    - सरकार अपने CII को सुरक्षित करने का कार्य अकेले निजी क्षेत्रों के हाथों में नहीं छोड़ सकती। उदाहरण के लिए यदि किसी निजी स्वामित्व के CII पर साइबर हमला होता है तो उसके दुष्प्रभाव पूरे देश पर होगा, उसका प्रभाव निजी स्वामित्व की CII तक ही सीमित नहीं रहेगा। उदाहरण के लिए यदि किसी राष्ट्रीय स्टाक एक्सचेंज पर साइबर हमला होता है तो उससे सम्भवतः सभी व्यवसायिक संचालन ठप्प हो सकते हैं। यह अर्थव्यवस्था को प्रभावित करेगा और निवेशकों के बीच आतंक व्याप्त हो जाएगा।
    - **साइबर सुरक्षा बेहतर बनाने हेतु प्रोत्साहनों का अभाव:** प्रतिस्पर्धी बाजारों की तुलना में असंगत बाजारों में निजी फर्मों द्वारा साइबर सुरक्षा में पर्याप्त निवेश की अत्यंत कम सम्भावना होती है। उदाहरण के लिए बिजली कम्पनियों और अन्य प्रदाताओं के समक्ष बहुत कम प्रतिस्पर्धा होती है; किसी भी ग्राहक को आमतौर पर एक ही बिजली कम्पनी द्वारा सेवा दी जाएगी। लाभप्रद बाजार शक्तियों की यह अनुपस्थिति इस बात की व्याख्या करती है कि सार्वजनिक उपयोगिताएं प्रायः बिना लागत के सुरक्षा उपायों को कार्यान्वित करने में क्यों विफल रहती हैं।
    - **विनियमों का खराब प्रवर्तन** –निजी क्षेत्रक सरकारी विनियामकों को अपने संगठनात्मक उद्देश्यों के मार्ग में बाधा के रूप में देखते हैं क्योंकि उनका संगठनात्मक उद्देश्य मुख्यतः अपने हितधारकों को लाभ प्रदान करने का ही होता है। इसलिए, महत्त्वपूर्ण अवसरंचनाओं को परिचालित करने वाली कई फर्मों की साइबर सुरक्षा में बहुत कम निवेश करने की भावना रहती है। वे जान बूझकर नियमों के कमियों को ढूंढते हैं और परिचालन की लागत में कमी करने के लिए उनसे बच कर निकलते हैं। इसके अतिरिक्त सरकारी एजेंसियों के पास परीक्षण क्षमता की कमी नेटवर्क संचालकों को सस्ता, परन्तु सुभेद्य संचार उपकरण खरीदने में सहायता करती है।

7. हाल की घटनाएँ (Recent Developments)

भारत ने हाल के वर्षों में अपनी संचार अवसरंचना की सुरक्षा हेतु अपनी अनुक्रिया में वृद्धि की है:

- साइबरस्पेस से, विशेषकर साइबर आतंकवाद से उत्पन्न होने वाले खतरों को सम्बोधित करने के लिए IT अधिनियम 2000 में 2008 में किये गये संशोधन से एक विधिक ढांचा विकसित किया गया था।
- सरकार ने 2012 में राष्ट्रीय दूरसंचार नीति प्रारम्भ की थी, जिसमें उसने 2020 तक 60 से 80 प्रतिशत की सीमा तक भारतीय दूरसंचार क्षेत्रक की मांग पूरी करने के लिए दूरसंचार उपकरणों का घरेलू उत्पादन करने का लक्ष्य निर्धारित किया है।
- आयातित संचार उपकरण सुभेद्यताओं से मुक्त हैं, यह सुनिश्चित करने के लिए स्थानीय प्रमाणीकरण जैसे कई उपायों की घोषणा की गयी है। इनमें उपकरण परीक्षण प्रयोगशाला की स्थापना करना भी सम्मलित है।
- सरकार ने राष्ट्रीय तकनीकी अनुसन्धान संगठन के तत्वाधान में राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (CIIPC) की स्थापना की है। NCIIPC का लक्ष्य साइबर आतंकवाद, और अन्य खतरों के विरुद्ध CII की सुभेद्यता को कम करना है। इसे निम्नलिखित कार्य सौंपे गये हैं:
    - सभी CII तत्वों की पहचान करना;
    - सरकारों में सामरिक नेतृत्व और समन्वय प्रदान करना; और
    - नीति मार्गदर्शन, विशेषज्ञता साझाकरण और परिस्थितियों की जागरूकता के लिए CII को राष्ट्रीय स्तर के खतरों में समन्वय, साझाकरण, निगरानी, विश्लेषण और पूर्वानुमान लगाना।