एक मज़बूत और सुरक्षित साइबर प्रणाली : वर्तमान की अपरिहार्य आवश्यकता!

सरकारी स्तर पर भले ही आज "डिजिटिल इंडिया" जैसे कार्यक्रमों की बदौलत इंटरनेट की तथा इससे जुड़े लाभों की चर्चा ज्यादा हो रही हो, किंतु भारत जैसे देश में भी बड़ी आबादी दशक भर से भी अधिक समय से इस प्रणाली को अपने दैनिक जीवन का अभिन्न हिस्सा बनाए हुए हैं। बात चाहे ईमेल के माध्यम से संदेश आदान-प्रदान करने की हो या अपने बिलों के भुगतान की, ऑनलाइन खरीदारी की हो या नौकरियों के लिये आवेदन की, बैंकिंग सुविधाओं का लाभ उठाने की हो अथवा रेलवे या हवाई जहाज़ों के टिकिट बुक करने की, सब चीजों में इंटरनेट का इस्तेमाल भारत में लंबे अरसे से हो रहा है। इसके अतिरिक्त, सोशल मीडिया व स्मार्ट फोन (विशेषकर कम कीमत वाले) के आने ने इस क्षेत्र में एक किस्म का समाजवाद सा ला दिया है तथा यह सुविधा निपट आम लोगों तक भी पैठ बनाने में सफल रही है।

कहना मुश्किल है कि यदि मात्र एक दिन के लिये भी फेसबुक अथवा व्हाट्सएप की सुविधा बंद कर दी जाए तो अधिक समस्या किस आयु वर्ग के लोगों को पेश आएगी, क्योंकि लगभग सभी आयुवर्ग के लोग सरलता और कुशलता से इसका खासा इस्तेमाल कर रहे हैं। कई मामलों में तो वे बच्चे जिन्होंने बमुश्किल अपनी टीनएज में जीवन में इस हद तक पैठ बना लेने के चलते असली संसार के साथ-साथ एक आभासी संसार ने भी आकार ले लिया है, जिसे इंटरनेट की भाषा में "वर्चुअल वर्ल्ड" की संज्ञा दी गई है।

अब चूँकि आमजन के सरोकार तथा निर्भरता इस प्रणाली पर संवेदनशीलता के स्तर तक बढ़ गई है, इसका मज़बूत और सुरक्षित होना भी उसी हद तक ज़रूरी हो गया है। आज एक ऐसा समय आ गया है जब साइबर प्रणाली में कुछ देर की गड़बड़ी भी अरबों-खरबों के नुकसान और अनेक अन्य जटिलताओं का कारण बन सकती है।

अपने आरंभिक दौर में विलासिता लगने वाली कोई चीज़ एक अरसे के बाद किसी भी अन्य सामान्य ज़रूरत की भाँति हमारे जीवन की आवश्यकता बन जाती है। ऐसा ही इंटरनेट और अन्य साइबर सुविधाओं के साथ भी है। हालाँकि भारत इस मामले में कुछ हद तक अभी भी संक्रमण काल से गुज़र रहा है, क्योंकि हमारे यहाँ अनेकों सुविधाओं का कुछ प्रतिशत भाग ही डिजिटिल हो पाया है तथा एक बड़ा तबका आज भी उन कार्यों को करने के लिये परंपरागत (अर्थात् ऑफलाइन) तरीकों का ही इस्तेमाल करता है। इसका एक कारण यह है कि एक बड़े तबके तक कंप्यूटर अथवा इंटरनेट तो छोड़िये, बिजली जैसी आधारभूत चीज़ भी हम अब तक नहीं पहुँचा पाए हैं। खैर, आज नहीं तो कल ऐसा कर देंगे तथा तब यह और भी ज्यादा आवश्यक हो जाएगा कि हमारी साइबर प्रणाली मज़बूत के साथ-साथ सुरक्षित भी हो।

कोई चीज हमारे लिये महत्त्वपूर्ण बन चुकी है, यह जानने के लिये ज़रूरी है कि एक बार उसके बिना जीवन की एक कच्ची सी कल्पना की जाए। ऐसी ही एक कल्पना मैं प्रस्तुत कर रही हूँ:

यदि हमारी साइबर प्रणाली किसी वजह से काम करना बंद कर दे तो-

- हमारी बैंकिंग व्यवस्था चरमरा जाएगी।
- हमारा शेयर बाज़ार पूरी तरह ठप हो जाएगा।
- हमारी संचार व्यवस्था (मोबाइल, टेलीफोन), प्रसारण व्यवस्था (रेडियो, टीवी, सिनेमा) काम करना बंद कर देगी।
- नौवहन प्रणाली के बिना हमारा रेल, वायु यातायात आदि संचालित नहीं हो पाएगा।
- कंपनियों द्वारा ऑनलाइन ट्रेडिंग संभव नहीं होगी।
- इस पर निर्भर अनुसंधान के हमारे कार्य (विशेषकर अंतरिक्ष अनुसंधान से जुड़े) रुक जाएंगे।

उपरोक्त बिंदुओं से साइबर प्रणाली के दुरूस्त रहने के महत्त्व का एक सामान्य अनुमान सहज ही लगाया जा सकता है। हालाँकि ये अनुमान साइबर प्रणाली के कार्य करना बंद कर देने से संबंधित थे, जबकि इसका एक अन्य पहलू है- किसी खराबी या अन्य गड़बड़ी के चलते इसका गलत ढंग से कार्य करने लगना, ऐसा होने पर परिणाम कितने भयानक हो सकते हैं इसका तो अनुमान भी कल्पना से परे लगता है।

साइबर प्रणाली में गड़बड़ी किसी तकनीकी खराबी का परिणाम भी हो सकती है तथा किसी बाहरी हस्तक्षेप का भी, जिसे कंप्यूटर की भाषा में साइबर हमला कहा जाता है।

अपने समय के प्रमुख रक्षा चिंतकों, जैसे मैकियावेली, ए.टी. माहन तथा डुहेट आदि ने क्रमशः थल, जल तथा गगन से होने वाले आक्रमणों से निपटने की रणनीतियाँ तो गढ़ीं, किंतु इस आभासी संसार में होने वाले युद्ध की तो उन्होंने अपने समय में कल्पना भी नहीं की होगी।

एक नियोजित तरीके से अंजाम दिया गया साइबर हमला बिना आवाज़ किये शत्रु को पस्त करने की ताकत रखता है। इस तरीके से अपनी लेशमात्र की जनहानि के

बिना हम शत्रु का एक बड़ा नुकसान करके "हींग लगे न फिटकरी, रंग चोखा का चोखा" वाली कहावत को चरितार्थ कर सकते हैं।

ईरान के यूरेनियम संवर्द्धन तथा परमाणु कार्यक्रम से जुड़े 5 संगठनों पर वर्ष 2010 (या उससे कुछ पहले) में 'स्टक्सनेट' वायरस से किये हमले का उदाहरण यहाँ लिया जा सकता है जिसने ईरान के सेंट्रीफ्यूज़ को नियंत्रण से बाहर कर उसके परमाणु कार्यक्रम को वर्षों पीछे धकेल दिया था। यहाँ शत्रु देश (संभवतः इज़राइल अथवा संयुक्त राज्य अमेरिका) को न तो कोई सेना भेजनी पड़ी और न ही कोई बम गिराना पड़ा। इसी प्रकार "डुकु" नामक वायरस को ईरान के परमाणु कार्यक्रम की रूपरेखा की नकल करने के लिये बनाया गया था।

हालिया दिनों में 'वानाक्राई' नामक मालवेयर का हमला काफी चर्चित रहा जो आपके कंप्यूटर की ज़रूरी सूचनाओं को एन्क्रिप्ट कर देता था तथा वापस उन तक पहुँच बनाने के बदले आपसे फिरौती मांगता था (जिसके चलते इसे 'रैनसमवेयर' की श्रेणी में रखा गया)। इस तरह का साइबर हमला व्यापक स्तर पर हानि पहुँचाने की क्षमता रखता है।

ये हमले यदि केवल आर्थिक हानि पहुँचाते हों तो एक दफा इन्हें सहन भी किया जा सकता है, किंतु आजकल साइबर जासूसी की अवधारणा ने लोगों की निजता और देशों की राष्ट्रीय सुरक्षा तक को खतरे में डाल दिया है। वर्ष 2006 से जारी "ऑपरेशन शेडी रैट" तथा भारत को लक्षित किया गया तथा वर्ष 2009 में पकड़ में आया 'घोस्टनेट' का हमला जिसने भारतीय सुरक्षा अभिकरणों की सूचनाओं तक पहुँच बना ली थी आदि इस श्रेणी में आते हैं।

साइबर संसार की चुनौतियों में एक और चुनौती सोशल मीडिया साइटों के बाद से पैदा हुई है, वह है झूठी अथवा तेज़ी से माहौल बिगाड़ने में सक्षम संवेदनशील खबरों का शीघ्रता से प्रसार। कितनी ही बार सोशल मीडिया पर वायरल हुई इन संवेदनशील खबरों के चलते देश का सांप्रदायिक माहौल बिगड़ने का खतरा पैदा हो चुका है। 2012 में ऐसी ही कुछ खबरों के चलते बंगलूरू में रह रहे पूर्वोत्तर भारत के लोगों का बड़ी संख्या में वहाँ से पलायन हुआ था।

अब बात करते हैं इन चुनौतियों से निपटने की जिसके लिये हमें साइबर सुरक्षा विशेषज्ञों की ज़रूरत होगी। यहाँ भी हालात कुछ संतोषजनक दिखाई नहीं देते। विश्व में भले ही भारत को एक आईटी सुपरपावर के तौर पर देखा जाता हो किन्तु वर्ष 2013 में राष्ट्रीय समाचार-पत्र में छपी एक खबर के मुताबिक भारत के पास कुल मिलाकर मात्र 556 साइबर सुरक्षा विशेषज्ञ हैं जबकि हमें ऐसे लाखों विशेषज्ञों की आवश्यकता है।

हमें समझना होगा कि जिस प्रकार हम अपने रक्षा बजट में किसी प्रकार की कोई कसर नहीं छोड़ते, उसी प्रकार सुरक्षा के लिहाज़ से इसे भी एक ऐसा मोर्चा मानना होगा जिसे अनदेखा छोड़ने के परिणाम घातक हो सकते हैं।

इस मोर्चे पर वीरता के स्थान पर तकनीक की समझ हमें बचाएगी और हमें इस तकनीकी समझ वाले लोगों की एक फौज उसी से तरह तैयार करने की ज़रूरत है जैसे चीन, अमेरिका अथवा रूस जैसे देशों ने तैयार की है, तभी हम चहुँओर से अपने सुरक्षित होने का दावा कर सकेंगे। हालाँकि ऐसा भी नहीं है कि भारत ने इस चुनौती को पूर्णतया अनदेखा छोड़ दिया हो। वर्ष 2004 में ही हमने साइबर सुरक्षा संबंधी चुनौतियों से निपटने के लिये "इंडियन कंप्यूटर एमरजेंसी रिस्पॉन्स टीम" (जिसे प्रचलित रूप से आईआरटी-इन के नाम से जाना जाता है) नाम के एक समर्पित अभिकरण का गठन कर लिया था जो समय-समय पर साइबर सुरक्षा से जुड़े विभिन्न उपायों को लागू करता रहता है। ऐसी ही एक पहल इस संस्था ने इस साल फरवरी में 'साइबर स्वच्छता केंद्र' की शुरुआत करके की। 'साइबर स्वच्छता केंद्र' का कार्य डेस्कटॉप और मोबाइल के लिये सिक्योरिटी सॉल्यूशन प्रदान करना है। इस संस्था व अन्य अभिकरणों के संयुक्त प्रयासों का ही फल था कि हाल में हुए 'वनाक्राई' नामक मालवेयर के हमले का भारत पर ज्यादा असर नहीं हुआ। इसके अलावा, एक श्रेणी एथिकल हैकर्स की भी है जो अपने तकनीकी ज्ञान व प्रतिभा का इस्तेमाल ऐसे हमलों को नाकाम करने में करते हैं। हालाँकि, ऐसे एथिकल हैकर्स की पहचान करना मुश्किल है किंतु भारत में इनकी एक मज़बूत उपस्थिति अवश्य है। अन्य सजग देशों की भाँति भारत को भी संभावित साइबर हमलों व इनसे जुड़ी अन्य गड़बड़ियों से निपटने के लिये और अधिक संस्थागत प्रयासों की ज़रूरत है तभी हम भरोसे के साथ डिजिटलीकरण के लाभों को व्यापक जनसमूह तक पहुँचा पाएंगे।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/a-strong-and-safe-cyber-system-the-inevitable-need-of-the-present