साइबर युग के युद्ध में निशाने पर हम

किसी जमाने में यह काम विषकन्याएं किया करती थीं और फिर सैंकड़ों साल तक यह जिम्मेदारी जासूसों के कंधों पर रही। लेकिन प्रतिद्वंद्वी देशों के गुप्त राज इकट्ठे करने और उनके प्रशासनिक तंत्र को छिन्न-भिन्न करने का दायित्व अब साइबर जासूसों और हैकरों की ऐसी फौज़ ने संभाल लिया है जिसे सामने आने की जरूरत ही नहीं। इंटरनेट युग में दूरी का को अर्थ नहीं रहा। हजारों किलोमीटर दूर बैठे कुछ दक्ष कंप्यूटर विशेषज्ञ दुनिया की बड़ी से बड़ी शक्तियों पर साइबर हमले कर इतनी सफाई से निकल जाते हैं कि सबूत ढूंढे से भी नहीं मिलते। इन हमलों में कभी राष्ट्रीय सुरक्षा से जुड़े बेशकीमती राज चुरा लिए जाते हैं, कभी तकनीकी प्रणालियों को नुकसान पहुंचाकर कंप्यूटर नेटवर्क ठप कर दिए जाते हैं और कभी प्रतिद्वंद्वी राष्ट्र के सर्वरों पर कब्ज़ा जमा लिया जाता है। साइबर अपराध, साइबर आतंकवाद, साइबर जासूसी और हैकिंग अब को तकनीकी शब्द नहीं रहे। लगभग रोजाना ही सरकार, प्रशासन और कारोबार के किसी न किसी अहम हिस्से को हैकिंग के हमलों से गुजरना पड़ रहा है, फिर भले ही वह हमारा रक्षा मंत्रालय हो, सेना हो, मिसाइल प्रणालियां हों, विदेश मंत्रालय हो या फिर खुद प्रधानमंत्री का कार्यालय। जिस साइबर वार का जिक्र पहले विज्ञान कथाओं में होता था, वह शीतयुद्ध-पश्चात के इस दौर में हमारी राष्ट्रीय सुरक्षा के प्रति सबसे बड़ी चुनौती बन चुका है।

नए दौर का युद्ध हथियारों, मिसाइलों और परमाणु बमों से नहीं लड़ा जाएगा। ऐसे हथियारों से तो दोनों ही पक्ष लैस हैं और नुकसान भी दोनों ही पक्षों का होता है, जो कभी नहीं चाहेंगे कि अर्थव्यवस्थाओं की प्रधानता के युग में उनके सामने कोई आर्थिक व्यवधान आए। नए जमाने की लड़ाई अप्रत्यक्ष रूप से लड़ी जानी है जिसमें हथियारों का इस्तेमाल किए बीना ही प्रतिद्वंद्वी राष्ट्र के सुरक्षा, संचार, ऊर्जा, बैंकिंग, कारोबारी तथा प्रशासनिक ढांचे को पंगु बना दिया जाए। कंप्यूटर, इंटरनेट और संचार के शक्तिशाली साधन इस तरह के विध्वंसक एजेंडा को लागू करने के उपयोगी औजार बन गए हैं। ऐसे अनजान हमलावरों की पहचान बहुत मुश्किल है, जवाबी कार्रवाई की तो बात ही छोड़ दीजिए। पिछले डेढ़ साल के भीतर भारत ने जो कुछ झेला है, वह आने वाली चुनौतियों का अनुमान लगाने के लिए काफी है।

- जुलाई २०१०: एक साइबर सुरक्षा विशेषज्ञ जैफ़री कार ने यह सिद्ध करके सबको सकते में डाल दिरा था कि भारत के उपग्रह इनसैट ४बी को स्टक्सनेट वायरस के जरिए नुकसान पहुंचाया गया था ताकि उसके जरिए चलने वाले टेलीविजन चैनल चीनी उपग्रह के ट्रांसपोंडर किराए पर ले लें। बाद में यही हुआ भी।

- अप्रैल २०१०: रक्षा मंत्रालय और कई भारतीय दूतावासों के कंप्यूटर सिस्टम हैक कर लिए गए। संदेह है कि इस साइबर हमले में भारतीय सुरक्षा प्रणालियों और मिसाइलों के गोपनीय डेटा चुरा लिए गए।

- जुलाई २०११: चीनी हैकरों ने केंद्र सरकार के कंप्यूटरों को नियंत्रित करके रक्षा मंत्रालय, विदेश मंत्रालय और दलाई लामा से जुड़ी संवेदनशील सूचनाओं को खंगाल डाला था। भारत के सरकारी ठिकानों, अमेरिका, दक्षिण कोरिया, विरातनाम, आसियान, आई ओसी और संयुक्त राष्ट्र के जिनेवा कार्यालरा सहित कुल ७२ लक्ष्यों को भेदने वाली इस कार्रवाई को अब तक का सबसे बड़ा साइबर हमला करार दिया गया है।

- जुलाई २०११: विदेश मंत्रालय तथा प्रधानमंत्री कार्रालय के कंप्यूटरों को हैक कर लिया गया। पता चला कि हैक किए गए कुछ कंप्यूटर तो पिछले दो साल से गुप्त सूचनाएं बाहर भेज रहे थे।

- नवंबर २०११: भारत सरकार ने आधिकारिक रूप से बताय कि नेशनल इन्फॉरमेटिक्स सेन्टर (एनआईसी) के कुछ सर्वरों पर दूसरे देशों के हैकरों ने कब्जा जमा रखा था और वे इनका इस्तेमाल तीसरे देशों के विरुद्ध साइबर हमलों के लिए कर रहे थे। एनआईसी भारत सरकार और राज्य सरकारों को इंटरनेट से जुड़ी सेवाएं देने वाली सबसे बड़ी एजेंसी है।

चुनौती बहुत गंभीर

जिस स्टक्सनेट वायरस का इस्तेमाल भारत पर साइबर हमले करने के लिए किया गया, उसी ने पिछले साल ईरान के एक परमाणु संयत्र को बंद करने पर मजबूर कर दिया था। सन २००७ में एस्तोनिया पर हुए साइबर हमलों ने वहां की सरकार, बैंकों, सुरक्षा प्रणालियों, अखबारों, संसद और मंत्रालयों को पंगु बना दिया था। वहां सामान्य व्यवस्था बहाल होने में कई दिन लगे। भारत के साथ भी ऐसा हो सकता है। परमाणु हथियारों के युग में किसी सुरक्षा प्रणाली को भेद देने के कितने भीषण नतीजे हो सकते हैं, इसका अनुमान लगाना मुश्किल नहीं है। और तो और महज दो शेरार बाजारों के सिस्टम ठप करने भर से कारोबारी क्षेत्र में कोहराम मच सकता है और बैंकिंग प्रणाली निशाने पर आई तो राष्ट्रव्यापी अव्यवस्था तथा अराजकता फैल सकती है। अरबों का नुकसान अलग से।

अफसोस की बात है कि आई टी की बहुत बड़ी ताकत होने के बावजूद हम साइबर सुरक्षा के मामले में न तो जागरूक हैं और न ही तैयार। इतने बड़े ठिकानों पर इतनी आसानी से सालों-साल होने वाले विदेशी हैकरों के क्या हमारी आई-टी विशेषज्ञता पर सवालिया निशान खड़ा नहीं करते? और क्या वे एक उभरती हुई अंतरराष्ट्रीरा ताकत होने के हमारे दावे की कल नहीं खोलते?

कैस्परस्की नामक एंटीवायरस कंपनी के संस्थापक यूजीन कैस्परस्की ने हाल ही में कहा था कि भारत सरकार और यहां के संगठनों के विरुद्ध विशाल साइबर हमले होना रोजमर्रा की बात है। और इनमें से ज्यादातर हमले सफल रहते हैं। जाने-माने एंटी वाररस विशेषज्ञ मिक्को हिप्पोनेन का कहना है- मुझे नहीं लगता कि भारत सरकार को इस बात का अहसास भी है कि उसके सामने साइबर हमलों की चुनौती कितनी बड़ी है!

ऐसे में आश्चर्रा नहीं होना चाहिए कि २०१०-११ में यहां २.९९ करोड़ लोग साइबर हमलों के शिकार हुए और इनसे लगभग ३४,११० करोड़ रुपए का नुकसान हुआ।

अगर यह पूछा जाए कि इन हमलों के पीछे कौन है तो परिस्थितियां चिल्ला-चिल्लाकर चीन की ओर इशारा कर रही हैं। पूरी दुनिरा चीन के साइबर आचरण से त्रस्त हैं, जो इंटरनेट विश्व का बेताज खलनायक माना जाता है। व्हाइट हाउस से लेकर नाटो तक और ब्रिटिश गुप्तचर एजेंसी से लेकर आस्ट्रेलिया संसद तक चीन से होने वाले हमलों के शिकार हो चुके हैं। साइबर हमलों की निगरानी रखने वाले टोरंटो विश्वविद्यालय के शोधकर्ताओं ने पता लगाया था कि पिछले साल भारतीय ठिकानों पर हुए साइबर हमले चीन के चेंगदू शहर से किए गए थे। और इस साल अगस्त में मैकेफी ने भारत तथा ७२ दूसरे ठिकानों की हैकिंग के बारे में जो रपट पेश की है वह भी चीन को ही हमलावर करार देती है। रपट के अनुसार इसके पीछे कम से कम एक सरकारी संगठन की भी भूमिका है।

चीनी खंडन और सबूत

हालांकि चीन इससे इंकार करता है। उसका तो यह भी दावा है कि अमेरिका और भारत से खुद चीन के विरुद्ध पिछले एक साल में करीब पांच लाख साइबर हमले हुए हैं और उसे निशाना बनाने के मामलों में से आठ फीसदी भारत की सरजमीन से जन्म लेते हैं। लेकिन कुछ अरसा पहले चीन के झूठ का उसी के सरकारी टेलीविजन पर पर्दाफाश हो गया जब एक कार्यक्रम में कुछ सैकंड की ऐसी क्लिप दिखा दी गई जिसमें चीनी सेना की देखरेख में होने वाली हैकिंग की कार्रवाइरों की एक झलक दिखा दी गई थी। बाद में यह वीडियो तुरत-फुरत हटा दिया गया। हैकिंग के मामलों की जांच करने वाले अनेक विशेषज्ञों ने पाया है कि सरकारों को निशाना बनाने वाले वायरसों और इंटरनेट हमलों का कोड चीनी भाषा में लिखा गया है। हमला करने वाले कंप्यूटरों के आई पी एड्रेस (इंटरनेट से जुड़े कंप्यूटरों की पहचान बताने वाला एक नंबर) भी चीन से जुड़े थे। और फिर जिन देशों को निशाना बनाया गया, वे वही थे जिनके प्रति चीन का रवैया शत्रुतापूर्ण है, जैसे भारत, अमेरिका, जापान, वियतनाम आदि।

सवाल उठता है कि इस चुनौती के बरक्स हमारा जवाब क्या है? भारत में कई एजेंसियों को कंप्यूटर प्रणालियों, इंटरनेट, दूरसंचार और सुरक्षा संचार प्रणालियों को महफूज़ रखने का जिम्मा दिया गया है। प्रधानमंत्री कार्यालय के तहत काम करने वाला नेशनल टेक्निकल रिसर्च अएर्गनाइजेशन (एनटीआरओ), केंद्र सरकार की नोडल एजेंसी इंडिरान कंप्यूटर इमरजेंसी रेस्पोंस टीम (सीईआरटी-इन), सेना से जुड़े कुछ संगठन, एनआईसी, पुलिस की साइबर अपराध शाखाएं आदि इंटरनेट सुरक्षा को अभेद्य बनाने की कोशिशों में जुटी हैं। कहने को तो संस्थाएं बहुत हैं लेकिन उनके बीच तालमेल की कमी कहिए, सरकारी लालफीताशाही की समस्याएं कहिए या फिर योग्य पेशेवरों तथा आधुनिक सुविधाओं का अभाव कि जमीनी स्तर पर परिणाम निराशाजनक ही रहे हैं। दूसरी ओर अमेरिका को देखिए जहां इंटरनेट सुरक्षा के लिए बाकारादा फौजी कमान का गठन किया गया है। यह साइबर कमांड (यूएससाइबरकॉम) वहां नेशनल सिक्यूरिटी एजेंसी के साथ मिलकर मुस्तैदी से राष्ट्रीय हितों को अंजाम दे रही हैं। प्रधानमंत्री डॉ. मनमोहन सिंह ने भी देश में साइबर कमांड के गठन का संकेत दिया था लेकिन अब तक उसके दर्शन नहीं हुए हैं और न ही उस मजबूत राष्ट्रीय साइबर सुरक्षा नीति का ही को अता-पता है जिसकी इंटरनेट से जुड़े करीब १२ करोड़ भारतीयों को तलाश है।