नईदुनिया
इंदौर, गुरुवार 14 जुलाई 2016
www.naidunia.com

'दुश्मन देशों के सामरिक प्रतिष्ठानों को निशाना बना रहे सायबर अपराधी'

सायबर अपराध का दायरा बढ़ता जा रहा है। व्यक्तियों, वित्तीय संस्थाओं, प्रॉपर्टीज और सरकारों को निशाना बनाने के बाद सायबर अपराधी अब देश और उसके बड़े सामरिक प्रतिष्ठानों को निशाना बना रहे हैं। इस तरह के हमले जाहिर है कोई अकेले दम पर नहीं कर सकता है। इसके पीछे दुश्मन देश की साजिश होती है, जिसकी एजेंसियां सायबर अपराध करने वालों की मदद करने में अहम भूमिका निभाती है। कई मौकों पर दूसरे देशों के प्रतिष्ठानों में सायबर घुसपैठ करने वाले मित्र देश भी होते हैं, जो अपने ही दोस्त पर नजर रखते हैं। इसका मकसद उन देशों की आर्थिक नीतियों की जासूसी करना या उनकी इस आधार पर छवि खराब करना होता है। इसका सीधा असर उस देश के नागरिकों पर होता है और देश की अर्थव्यवस्था पटरी से उतर जाती है। दुनिया में इस तरह की सायबर घुसपैठ को बड़े खतरे के रूप में लिया जा रहा है और इसे सायबर युद्ध का नाम दे दिया।

वरुण कपूर
आईपीएस

किसी और देश द्वारा प्रायोजित इस सायबर युद्ध के पीछे मूल रुप से तीन कारण होते हैं। पहला- जासूसी, इसके पीछे उद्देश्य यह होता है कि दूसरे देश की गुप्त सूचनाएं हासिल करना, जिसे अपने देश की बेहतरी और सुरक्षा के लिए इस्तेमाल किया जा सके। दूसरा- तोड़-फोड़, हमला किए गए देश के सामरिक प्रतिष्ठानों और सैनिक ठिकानों में हो रही हलचल की जानकारी जुटाना और उसके मिलिट्री सिस्टम को प्रभावित करना। तीसरा-सेवाओं को बाधित करना। इसके जरिए देश के नागरिकों को इंटरनेट और सर्वर के माध्यम से मिल रही सेवाओं को बाधित करना है।

इसका बड़ा और सटीक उदाहरण है यूरोप का छोटा सा देश एस्टोनिया। 13 लाख की आबादी वाला यह देश बाल्टिक सागर के पास उत्तरी यूरोप में बसा है। अप्रैल 2007 को एस्टोनिया सरकार ने देश की आजादी में महत्वपूर्ण भूमिका निभाने वालों को सम्मान देने और याद करने का फैसला लिया। एस्टोनिया पर नाजी शासन से मुक्ति के बाद रूस का कब्जा था। सरकार के इस कदम से देश में वर्चुअल युद्ध शुरू हो गया और कई जगहों पर दंगे भड़क गए और इस सब में रूसियों का हाथ था। यह सब चल ही रहा था कि एक बड़ी घटना हो गई। दो रूसी युवक लंदन पहुंचे एक अनजान, छोटा होटल

बुक किया और अपने लैपटॉप के इस्तेमाल से उन्होंने एस्टोनिया के पॉवरग्रिड को हैक कर लिया। दुर्भाग्य से एस्टोनिया के पास एक ही पॉवरग्रिड था और वह भी बंद हो गया। रूसी लड़के यहीं नहीं रुके, उन्होंने ग्रिड के सिस्टम में वायरस भी डाल दिए जिससे सारा सिस्टम ठप पड़ गया। हालात यह हो गए कि पूरे देश में अंधेरा छा गया।

उन दिनों एस्टोनिया में कड़ाके की ठंड का मौसम था। बिजली सप्लाय बंद होने से देश में कम्प्युटर आधारित सभी नागरिक सेवाएं बंद हो गई। स्कूल, कॉलेज, हॉस्पिटल, उद्योग, ट्रैफिक सिग्नल, संचार साधन सारे बंद पड़ गए, लोगों की दिनचर्या गड़बड़ा गई और पूरा देश थम गया। एस्टोनिया तकनीकी तौर पर एडवांस देश है और स्काइप यहीं पर विकसित हुआ। इसके बावजूद एस्टोनिया में विशेषज्ञों को ग्रिड ठीक करने और उसके सिस्टम से वायरस बाहर करने में सात दिन लग गए। उसके बाद एक-एक करके देश की दूसरी सर्वर आधारित प्रणालियों को ठीक किया। सात दिनों में देश के नागरिकों का जीवन नर्क बन गया उन्हें कई दिक्कतों का सामना करना पड़ा और जो पैसों का नुकसान हुआ उसका आकलन करना भी कठिन है। इस घटना के बाद यह कहा जाने लगा कि रूस ने ऐसा किया जैसे उसने अपनी पूरी सेना के साथ एस्टोनिया पर हमला कर दिया हो और उसे बर्बाद करने की ठान ली हो। यह सब किया सिर्फ दो लड़कों की सेना ने जिसका हथियार एक लैपटॉप था।

सायबर पुलिस की तरह अब सायबर कमांडो

अमेरिका, चीन, ईरान, रूस, उत्तरी कोरिया, इजरायल जैसे देश एस्टोनिया जैसे सायबर हमले करने में सबसे आगे हैं। भारत में भी इस तरह के हमले लगातार होते रहते हैं और वो भी कई मौकों पर निशाना बना है और इसके खतरे बरकरार हैं। सायबर अपराध और घुसपैठ से बचने के लिए भारतीय सेना ने सायबर कमांड की शुरूआत की है। हाल ही में सेना ने एअरो-स्पेस कमांड की भी शुरू किया है। जिस तरह देश में सायबर पुलिस होती है उसी तरह अब सेना में सायबर कमांडो भी हैं।

(लेखक अतिरिक्त पुलिस महानिदेशक पद पर इंदौर में पदस्थ हैं और विचार उनके व्यक्तिगत हैं)
ईमेल: varunkapoor170@gmail.com