टिप्पणी

15

साईबर युद्ध

पिछले तीन अध्यायों में हमने परमाणु, जैविक और रसायनिक युद्धों के बारे में पढ़ा। सूचना प्रौद्योगिकी और साईबर स्पेस के अधिकाधिक प्रयोग से दुश्मनों द्वारा एक नए प्रकार के युद्ध का प्रयोग किया जा रहा है, जिसे साईबर युद्ध कहते हैं।

साईबर युद्ध का संबंध कंप्यूटर तकनालोजी से है, जिसका प्रयोग करके किसी राज्य अथवा संस्था की गतिविधियों को भंग किया जाता है। यह रणनीतिक अथवा सैन्य उद्देश्यों के लिए शत्रु के सूचना तंत्रों पर जान-बूझ कर किया गया आक्रमण होता है। इसका अभिप्राय शत्रु के सूचना और संचार तंत्र को भंग अथवा नष्ट करना तथा शत्रु के बारे में सब कुछ जानने की कोशिश एवं अपने बारे में कुछ भी जानने से शत्रु को दूर रखने का प्रयास होता है।

साईबर युद्ध में साईबर आक्रमण, जासूसी और तोड़-फोड़ के अनुरूप प्रहारात्मक और रक्षात्मक, दोनों प्रकार की कार्रवाईयाँ शामिल होती हैं। इस पर विवाद रहा है कि क्या इस प्रकार की गतिविधियों को युद्ध कहा जा सकता है? देश अपनी क्षमताओं को विकसित करने तथा साईबर युद्ध में एक आक्रमण अथवा रक्षाकर्ता अथवा दोनों रूपों में सलंग्न रहे हैं।

उद्देश्य

इस पाठ का अध्ययन करने के बाद, आप :

- साईबर युद्ध की व्याख्या कर सकेंगे;
- विभिन्न प्रकार के साईबर खतरों को पहचान सकेंगे;
- साईबर अपराधों, साईबर आक्रमणकर्ताओं और साईबर हथियारों की विभिन्न प्रकारों का वर्णन कर सकेंगे;
- साईबर घुसपैठ तथा बचाव के उपायों को स्पष्ट कर सकेंगे;
- साईबर सुरक्षा नीति की व्याख्या कर सकेंगे।

15.1 साईबर युद्ध की परिभाषा

साईबर युद्ध को किसी राज्य द्वारा किसी अन्य देशे के कंप्यूटर तंत्र को भंग अथवा नष्ट करने के उद्देश्य से उसमें हस्तक्षेप करने के लिए की गई घुसपैठ के रुप में परिभाषित कर सकते हैं। अन्य परिभाषाओं में गैर-राज्य अभिनेकर्ता भी शामिल हैं, जैसे आतंकवादी समूह, कंपनियां,

राजनीतिक या वैचारिक चरमपंथी समूह, और अंतरर्राष्ट्रीय आपराधिक संगठन। कुछ सरकारों ने इसको अपनी सकल सैन्य रणनीति का अभिन्न भाग बना लिया है और साईबर युद्ध में अपनी क्षमता को बढ़ाने के लिए भारी निवेश किया है।

साईबर युद्ध अनिवार्य रुप से किसी सरकार द्वारा युद्ध लड़ने की क्षमता में इसको सम्मिलित करने के कारण इसकी घुसपैठ करने की क्षमता का औपचारिक प्रारुप है। यह क्षमता एक ही प्रकार के घुसपैठ परीक्षण तरीकों का प्रयोग होता है परंतु रणनीतिक दृष्टि से उसका प्रयोग निम्नलिखित उद्देश्यों के लिए किया जाता है–

(a) महत्वपूर्ण संरचना (ढाँचों) पर साईबर आक्रमण को रोकना

(b) राष्ट्रीय स्तर पर साईबर आक्रमण की शंकाओं को कम करना

(c) साईबर आक्रमणों की क्षति को कम करने तथा पहले की अवस्था में आने में लगने वाले समय को कम करना

सरकारी स्तर पर घोषित युद्धों तथा देशों में घोषित युद्ध न होने पर भी युद्ध की स्थिति में उकसाने वाली कार्रवाईयाँ भी राष्ट्रीय स्तर की रणनीतियों का एक भाग हैं।

साईबर अपराध : ऐसा अपराध जिसमें क्षति पहुँचाने के लिए कंप्यूटर के प्रयोग का ज्ञान आवश्यक हो–उसे साईबर अपराध कहा जाता है।

साईबर सुरक्षा : साईबर सुरक्षा का अर्थ ऐसे नीतियों और प्रक्रियाओं को विकसित करना है जो हमारी सूचनाओं और सूचना प्रणाली की रक्षा कर सकें।

15.2 विभिन्न प्रकार के खतरे

(a) **साईबर आक्रमण :** ये आक्रमण ऐसे हैं जिनमें तत्कालिक क्षति और रुकावटें मुख्य चिन्ता होती है।

(b) **साईबर जासूसी :** साईबर जासूसी घुसपैठ की ऐसी कारवाई है जो शत्रु देश की आवश्यक जानकारी प्राप्त कर सकती है। पारंपरिक जासूसी युद्ध की कार्रवाई नहीं होती और न ही साईबर जासूसी युद्ध की कार्रवाई है। दोनों को ही प्रमुख शक्तियों के बीच निरंतर चलने वाली कार्रवाई माना जाता है। इस मान्यता के बावजूद कुछ घटनाएँ देशों की बीच गंभीर तनाव पैदा कर देती है, जिन्हें आक्रमण ही माना जाता है। उदाहरण के लिए–

(1) एडवर्ड स्नोडन द्वारा उद्घाटित अमरीका द्वारा कई देशों में बड़े स्तर पर की गई जासूसी

(2) जर्मनी की चांसलर एंजला मर्कल पर (एन एस ए) द्वारा की गई जासूसी का पर्दाफाश होने पर चांसलर ने एन एस ए की तुलना जर्मन लोकतांत्रिक गणराज्य की सरकारी सुरक्षा सेवा स्तासी (Stasi) से की थी।

(3) एन एस ए द्वारा बाहमास में सेलफ़ोन पर हर बातचीत की बाहमास सरकार की अनुमति बिना की गई रिकार्डिंग तथा इसी प्रकार से कीनिया, फिलीपींस, मेक्सिको और अफगानिस्तान में की गई गतिविधियाँ।

(4) 'टाईटन रेन' द्वारा 2003 से अमरीका में कंप्यूटर प्रणाली के रक्षा अनुबंधकों की जाँच पड़ताल करना।

(5) अमरीका में कर्मचारी प्रबंधन आँकड़ों की सुरक्षा का उल्लंघन जिसके लिए चीन युद्ध और इसके प्रकार को उत्तरदायी माना जाता है।

(c) **साईबर तोड़फोड़ :** अन्य गतिविधियों में सहयोग देने वाले कंप्यूटर और सेटेलाईट्स किसी सिस्टम तथा उपकरण को भंग कर सकने वाले संदिग्ध अवयव हैं। सैन्य प्रणालियों जैसे कमांड और कंट्रोल प्रणाली में समझौतों से उनमें अवरोध तथा संदिग्ध बदलाव पैदा हो सकते हैं। शक्ति, जल, इंधन, संचार और परिवहन ढाँचों-सभी में अवरोध की शंका उत्पन्न हो सकती है। साधारण नागरिकों की दुनिया में भी खतरा हो सकता है तथा कुछ खास ठिकाने जैसे-विद्युत पावर ग्रिड, रेल गाड़ियाँ अथवा स्टाक एक्सचेंज भी निशाने पर हो सकते हैं। सरकारी कर्मचारियों के अतिरिक्त गैर सरकारी कार्यकर्ता भी इस को भाग हो सकते हैं तथा उसके खतरनाक, विंध्वसकारी परिणाम हो सकते हैं। उच्च कौशल प्राप्त गैर सरकारी छोटे समूह वैश्विक रणनीति और साईबर युद्धों में बड़ी सरकारी एजेंसियों की भाँति अति प्रभावशाली प्रभाव डाल सकते हैं।

(d) **साईबर प्रचार :** प्रचार का उद्देश्य जनमत को प्रभावित करना तथा सूचनाओं को नियंत्रित करना होता है। साईबर प्रचार हर प्रकार की सूचनाओं को नियंत्रित करने तथा जनमत को प्रभावित प्रयास करते हैं। यह मानसिक युद्ध का एक तरीका है इसके अतिरिक्त यह सोशल मीडिया, झूठी खबरों तथा डिजिटल साधनों का प्रयोग करते हैं। प्रचार एक जानबूझ कर किया गया प्रयास है जिसका लक्ष्य अवधारणओं को निर्मित करना, मान्यताओं को बदलना तथा लोगों का ऐसा व्यवहार प्राप्त करना होता है जिससे उनका उद्देश्य पूरा हो सके।

इन्टरनेट संचार का एक विशेष माध्यम है। इसके द्वारा लोग अपना संदेश बहुत लोगों तक पहुँचा सकते हैं। आतंकवादी संगठन इस माध्यम का प्रयोग करके लोगों की प्रभावशली ढंग से सोच बदलते हैं तथा सक्रिय सदस्यों को भी मजबूत करते हैं।

पाठगत प्रश्न 15.1

1. रिक्त स्थान भरिए

   (a) अपनी सूचनाओं और संचार व्यवस्था की रक्षा के लिए विकसित नीतियों और प्रक्रियाओं को ..... कहते हैं।

   (b) ..... का उद्देश्य जनमत को प्रभावित करने तथा सूचनाओं को नियन्त्रित करना है।

2. साईबर युद्ध को परिभाषित कीजिए।

3. साईबर अपराध को साईबर सुरक्षा का क्या अभिप्राय है?

4. साईबर खतरे कितने प्रकार के हैं। उनका उल्लेख कीजिए।

15.3 साईबर अपराध, साईबर आक्रमणकर्त्ता और साईबर हथियार

15.3.1 साईबर अपराधों का उदय

आईए हम देखें कि साईबर अपराध कैसे पैदा होते हैं और उनके कारणों के बारे में जानें।

टिप्पणी

(a) इस संरचनात्मक केंद्रित वातावरण की दुनिया में इंटरनेट प्रयोग में उल्लेखनीय वृद्धि हुई और इससे साईबर स्पेस ने विभिन्न अपराधों के बारे में शंकाओं को जन्म दिया है।

(b) इलेक्ट्रानिक्स और प्रौद्योगिकी में प्रगति ने उन्नत कंप्यूटरों के प्रयोग को न केवल हमारे लिए बल्कि शत्रुओं के लिए भी सामान्य बना दिया है।

(c) साईबर अपराधों के शिकार लोगों में शिकार होने की बात मानने में झिझक की प्रवृति है। यह अफवाहों को फैलाने से रोकने के लिए तथा अपनी (व्याति को क्षतिग्रस्त होने से बचाने के लिए भी हो सकता है।

(d) हम अपने संसाधनों को बढ़ाने के लिए वाण्ज्यि और नेटवर्क आधारित समाधानों पर नाटकीय ढंग से अधिकाधिक निर्भर होते जा रहे हैं इससे साईबर अपराधों के लिए हम सदिंग्ध बनते जा रहे हैं।

15.3.2 साईबर अपराधों के प्रकार

आज की दुनिया में बहुत प्रकार के साईबर अपराध बढ़ रहे हैं क्योंकि मनुष्य का दिमाग और परिकल्पना अनेक साईबर अपराधों के बारे में सोच सकता है। इन अपराधों को व्यापक रूप से निम्नलिखित ढंग से वर्गीकृत किया जा सकता है।

(a) **फ्राड एवं धोखाधड़ी :** प्राथमिक रूप में यह अपराध प्राय: वाणिज्य और आर्थिक जगत में देखा जाता है।

(b) **कंप्यूटर प्रोग्राम अथवा आँकड़ों को क्षति अथवा सुधार :** यह निजी क्षेत्र, सार्वजनिक क्षेत्र अथवा रक्षा संस्थानों जैसे ए.टी.सी. और राडार सिस्टम के लिए हो सकता है।

(c) **कंप्यूटर सिस्टम और निगरानी तक अनाधिकृत पहुँच :** इसको प्राय: वाणिज्यिक वेबसाईट्स में जैसे फिशिंग, जासूसी उपकरणों और डाटा स्पूफिंग में देखा जाता है।

(d) **कंप्यूटर प्रोग्रामों का अनाधिकृत पुरुत्पादन :** इन्हें डकैती के मामलों में रखा जाता है।

15.3.3 साईबर आक्रमणकर्त्ता

साईबर आक्रमणकर्त्ता का उद्देश्य आपराधिक खतरे अथवा राष्ट्रीय सुरक्षा को खतरा पहुंचाना होता है।

कुछ साईबर आक्रमणकर्ता निम्नलिखित हैं-

(a) **हैक्कर :** कंप्यूटर प्रयोग करने वाला ऐसा व्यक्ति जो किसी कंप्यूटर सिस्टम तक अनाधिकृत रूप से पहुँचना चाहता है।

(b) **क्रैकर :** क्रैकर एक आपराधिक उद्देश्य वाला हैकर होता है जो बुरी नीयत से कंप्यूटर में तोड़-फोड़ करता है, सुरक्षित कंप्यूटर से सूचनाएँ चुराता है और व्यक्तिगत तथा राजनीतिक लाभ के लिए व्यवधान प्रस्तुत करता है।

(c) **अंदरुनी :** किसी संगगन का कोई नाराज़ अंदरुनी व्यक्ति (वर्तमान कर्मचारी अथवा भूतपूर्व कर्मचारी) साईबर अपराध का मुख्य स्त्रोत होता है। अंदरुनी व्यक्ति के पास संगठन के नेटवर्क की जानकारी होती है जिससे वह बिना रोक-टोक वहाँ पहुँच सकता है और सूचना तंत्र को क्षति पहँचा सकता है अथवा आँकड़ें चुरा सकता है।

(d) **आतंकवादी :** ऐसे साईबर आक्रमणकर्ता जो सूचना प्रौद्योगिकी और इंटरनेट का प्रयोग युद्ध और इसके प्रकार अपनी गतिविधियों की सूचना बनाने तथा लागू करने, पैसा एकत्र करने, प्रचार करने, आवश्यक राष्ट्रीय ढाँचें को ध्वस्त करने के लिए करते हैं- जैसे ऊर्जा, परिवहन अथवा सरकारी कार्यवाईयाँ, को किसी सरकार अथवा नागरिकों को डराने के उद्देश्य से करते है।

(e) **विदेशी खुफिया सेवाएं :** विदेशी खुफिया निगरानी जो अपने विरोधी के बारे में संवेदनशील जानकारी प्राप्त करने के लिए अपने जासूसी व्यापार शिल्प के हिस्से के रूप में साइबर उपकरणों का उपयोग करते हैं।

15.3.4 साईबर हथियार

अब तक आपने यह जाना है कि साईबर अपराध क्या हैं। अन्य अपराधों की भांति इस अपराध में भी कुछ हथियार प्रयोग किए जाते हैं। आइए हम उनके बारे में जानें-

(a) **वायरस और वर्मस :** हमारे दैनिक कंप्यूटर की जिन्दगी में यह शब्द प्रायः सुने जाते हैं। यह ऐसे कोड हैं जिन्हें होस्ट प्रोग्राम के अंदर लागू किया जाता है। जब भी कोई गलती दिखाई देती है तो हम वायरस को जिम्मेवार ठहराते हैं लेकिन कभी-कभी अधिक जटिल वर्मस का भी प्रयोग किया जाता है।

(b) **ट्रोजन होर्सिस :** ये ऐसे प्रोग्राम हैं जो कठिनाई में काम करते हैं। ट्रोजन होर्सिस किसी वैध प्रोग्राम में अनाधिकृत प्रोग्राम होता है। जो प्रयोगकर्ता की जानकारी से बाहर कार्य करता है। ट्रोजन होर्सिस द्वारा आक्रमण करने के संभावित स्थान है।

1) OS

2) इंटरनेट के साफ्टवेयर डाऊनलोड करना

(c) **लाजिक/नालेज बम :** यह छुपे हुए कार्य होते हैं जो शुरू करने पर काम करने लगते हैं।

(d) **लोबोट्स :** जिन्हें नालेज रोबोट्स भी कहते हैं-वे प्रोसेस किए गए आँकडों को स्टोर रखते हैं और नालेज को स्टोर करते रहते हें।

(e) **एडवेयर :** एडवेयर एक प्रोग्राम है जिसे उपयोग प्रोग्रामों के बीच बनाए रखा जा सकता है। ये जिस कंप्यूटर में होते हैं उसमें उभर आते हैं और इनकी बहुत नकारात्मक प्रवृत्ति होती है।

(f) **स्पाईवेयर :** स्पाईवेयर भी एक प्रोग्राम है जिसे उपयोगी प्रोग्रामों के बीच बनाए रखा जाता है। इन्हें प्रायः प्रयोगकर्ता के बारे में जानकारी एकत्र करने के लिए तैयार किया जाता है जैसे प्रयोगकर्ता की बेव सर्फिंग की आदत, प्राथमिकताएँ और ई-मेल इत्यादि। इस गतिविधि का अवैधानिक भाग यह है कि यह काम प्रयोगकर्ता की सहमति के हबना किया जाता है।

पाठगत प्रश्न 15.2

1. रिक्त स्थान भरिए

(a) नालेज रोबोट्स को ..... कहते हैं।

(b) किसी कंप्यूटर सिस्टम तक अनाधिकृत पहुँच पाने के इरादे से कंप्यूटर प्रयोगकर्ता को प्रयास को ..... कहते हैं।

टिप्पणी

(c) उस ..... को हैकर कहते हैं जो आपराधिक इच्छा से सुरक्षित कंप्यूटर में सुरक्षित जानकारी को बुरी नीयत से खराब अथवा चोरी करता है।

(d) बुरे समय में ..... प्रोग्राम काम आते हैं।

(e) एडवेसर और स्पाईवेयर एक ही चीज है। (सत्य/असत्य)

2. साईबर अपराध कितने प्रकार के होते हैं? उनका उल्लेख कीजिए।

3. विभिन्न प्रकार के साईबर हथियारों के नाम लिखिए।

15.4 साईबर घुसपैठ, उपचार के उपाय और राष्ट्रीय साईबर सुरक्षा नीति

15.4.1 साईबर घुसपैठ : कार्य शैली

हमारे दुश्मन किस प्रकार हमारे साईबर स्पेस (क्षेत्र) में घुसपैठ करते हैं। वे साईबर हैकिंग के लिए इंटरनेट प्रयोग करने वालों को अनेक ई-मेल भेजते हैं। प्राय: ऐसे मेल में स्पाईवेयरस होते हैं जो मेल प्राप्त करने वाले कंप्यूटर को हानि पहुँचाते हैं और उसकी हार्ड डिस्क में भंडारित आँकड़ों को प्राप्त कर लेते हैं। कई बार इससे कंप्यूटर काम करना बंद कर देता है। प्रयोग किए गए स्पाईवेयरस के कारण होस्ट कंप्यूटर को दूर बैठा हुआ व्यक्ति संचालक कर पाता है।

जब भी कोई हैकर किसी कंप्यूटर में घुसपैठ करता है, तो वह एक स्पाईवेयर स्थापित करने की कोशिश करता है, जिससे उसको होस्ट कंप्यूटर पर अपनी इच्छा से काम करने की पहुँच मिल जाती है। वह होस्ट कंप्यूटर में बदनीयती भरा प्रोग्राम भी स्थापित कर सकता है जो इंटरनेट के द्वारा उस कंप्यूटर की सारी जानकारी प्राप्त कर सकता है तथा सभी फाइलें तथा आई.पी. एड्रेस डाऊनलोड कर सकता है। इसके लिए केवल एंटीवायरस प्रोग्राम काफी नहीं हैं क्योंकि वायरस खुले में काम करता है परंतु स्पाईवेयर्स को इस प्रकार तैयार किया जाता है कि वे चोरी से काम करते हैं। इसलिए वापर्स और स्पाईवेयर्स को पहचानने की टैकनोलजी अलग-अलग है।

15.4.2 संकेत

मैं किस प्रकार जान सकता हूँ कि मेरे कंप्यूटर में संक्रमण है। कुछ बहुत ही प्रत्यक्ष संकेत हैं जो आपके कंप्यूटर के संक्रमण को दिखाते हैं। चौकन्ने रहिए और निम्नलिखित का ध्यान रखिए-

(a) सिस्टम के काम करने में सुस्ती आना

(b) सिस्टम का आसामान्य रूप से काम करना जैसे सिस्टम को बार-बार हैंग हो जाना।

(c) अज्ञात सेवाओं का संचालन

(d) काम करने की प्रक्रिया का अवरुद्ध होना

(e) फाईल के विस्तार अथवा सामग्री में परिवर्तन होना

(f) हार्ड डिस्क का व्यस्त होना अथवा इसकी लाईट का निरंतर जलते रहना

टिप्पणी

15.5.3 उपचारात्मक उपाय युद्ध और इसके प्रकार

आप कई बार अपने कंप्यूटर के संक्रमित होने के संकेत नहीं पकड़ पाते परंतु कुछ ऐसे उपाय हैं जिनसे आप अपने सिस्टम को किसी प्रकार के आक्रमण से बचा सकते हैं।

(a) OS तथा प्रयुक्त एप्लीकेशन्स के लिए किसी विश्वस्त वेबसाईट से नवीनतम पैचेज का प्रयोग करें। यदि कोई किसी एप्लीकेशन अथवा प्रोग्राम को इंटरनेट के द्वारा अपने पीसी. पर कनेक्ट करने की कोशिश कर रहा हो तो सर्तक करने के लिए एक अचछी फायरवाल रक्षा की दृष्टि से सबसे पहला उपचार होगा। हालांकि एक फायरवाल की निम्नलिखित सीमाएँ हैं-

1. यह आपके कंप्यूटर को किसी बदनीयत अंदरुनी आक्रमण जैसे स्नूफिंग आक्रमण से नहीं बचा सकती।
2. यह उन कनेक्शन्स की रक्षा नहीं कर सकती जो OS से न गुजरती हों।
3. ईमेल से पैदा हुए वायरस से रक्षा नहीं कर सकती।

(b) एक अच्छे इंटरनेट सिक्यूरिटी (सुरक्षा) स्वीट को लगाइए। आजकल बाज़ार में अनेक इंटरनेट सिक्यूरिटी सूट्स उपलब्ध हैं। वे एंटीवायर्स, एंटी स्पाईवेर, फायर वाल, पेरेंटल कंट्रोल के सभी कार्य करते हैं। विकल्प के रूप में आपको एंटीवायर्स तथा एंटीस्पाई वेयर प्रोग्राम स्थापित करने चाहिए तथा लगभग प्रतिदिन नवीनतम वापर्स सिग्नेचर डाऊनलोड करना चाहिए।

15.5 कंप्यूटर इमरजेंसी रिसपांस टीम (CERT) और राष्ट्रीय सुरक्षा नीति

सूचना प्रौद्योगिकी विभाग ने 2004 में भारत साईबर आक्रमणों को परास्त करने के लिए कंप्यूटर इमरजेंसी रिस्पांस टीम गठित की थी। उस वर्ष साईबर सुरक्षा भंग करने के 23 मामले सामने आए थे। वर्ष 2011 में 13,301 मामले हुए। इसके प्रत्युत्र में सरकार ने एक नया उप मंडल 'राष्ट्रीय क्रिटीकल इंर्फोमेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (NCIIPC) गठित किया था जिसका उद्देश्य बिजली, परिवहन (यातायात), बैंकिंग, टेलिकाम, रक्षा, अंतरिक्ष और अन्य संवेदनशील क्षेत्रों पर आक्रमणों को निष्फल करना था। भारत में 2013 से पहले कोई साईबर सुरक्षा नीति नहीं थी। सरकार ने 2 जुलाई 2013 के राष्ट्रीय साईबर सुरक्षा नीति शुरू की। राष्ट्रीय साईबर सुरक्षा नीति, इलेक्ट्रानिकस और सूचना प्रौद्योगिकी विभाग द्वारा प्रस्तुत किया गया नीति का एक ढाँचा है।

साईबर सुरक्षा नीति का उद्देश्य साईबर स्पेस में सूचना तंत्र की रक्षा करता है, जो विभिन्न शंकाओं को कम करने, साईबर खतरों को रोकने की क्षमता बढ़ाने तथा उनका मुकाबला करने तथा साईबर दुर्घटनाओं से होने वाली क्षति को कम करती है।

इसको विभिन्न संस्थानिक ढाँचों, लोगों, प्रक्रियाओं, प्रौद्योगिकी और सहयोग से प्राप्त किया जाता है। इस नीति का उद्देश्य एक सुरक्षित साईबर स्पेस, पारिस्थितिकी और नियामक ढाँचे को प्राप्त करना है।

कंप्यूटर इमरजेंसी रिस्पांस टीम (CERT-10) का गठन संकट प्रबंधन के प्रयासों में सहयोग की नोडल (सर्वोपरि) एजेंसी के रूप में किया गया है। यह एजेंसी सहयोगी कार्रवाईयों तथा क्षेत्रीय कंप्यूटर इमरजेंसी रिस्पांस टीमों के बड़े संगठन के रूप में भी कार्य करती है।

पाठगत प्रश्न 15.3

1. निम्नलिखित का विस्तृत रूप लिखिए-
   (a) CERT
   (b) ICT
   (c) NCIIPC
2. कंप्यूटर सिस्टम के संक्रमित होने के क्या संकेत होते हैं?
3. फायरवाल (Firewall) की क्या सीमाएँ हैं?
4. अच्छी फायरवाल को रक्षा की प्रथम पंक्ति क्यों कहा जाता है?

क्रियाकलाप 15.1

Zero Days वृत चित्र को https://topdocumentaryfilms.com/zero-days/ पर देखें।

आपने क्या सीखा

साईबर युद्ध के अध्याय में आपको निम्नलिखित पर अंतर्दृष्टि प्रदान की गई है -

- साईबर युद्ध से संबंधित कुछ परिभाषाएं
- साईबर खतरे जिनमें साईबर जासूसी, साईबर हमले और साईबर तोड़-फोड़ तथा साईबर प्रचार शामिल हैं। आपने साईबर अपराधों, साईबर हमलों (आक्रमण) और साईबर हथियारों के बारे में भी पढ़ा।
- साईबर घुसपैठ और उन संकेतों के बारे में भी पढ़ा जो हमें बताते हैं कि हमारे कंप्यूटर में संक्रमण आ गया है। साईबर आक्रमणों को रोकने के लिए किए जाने वाले उपचारात्मक उपाय।

पाठान्त प्रश्न

1. निम्नलिखित विषयों पर संक्षिप्त जानकारी दीजिए-
   (a) साईबर युद्ध
   (b) साईबर जासूसी
   (c) साईबर प्रहार (तोड़-फोड़)
   (d) CERT तथा राष्ट्रीय साईबर सुरक्षा नीति
   (e) साईबर घुसपैठ के बचने के लिए उपचारात्मक उपाय

2. एडवेयर और स्पाईवेयर के बीच अंतर कीजिए।

3. साईबर प्रचार क्या है?

4. साईबर अपराधों तथा उन्हें रोकने के उपायों को स्पष्ट कीजिए।

5. राष्ट्रीय साईबर सुरक्षा नीति की व्याख्या कीजिए।

पाठगत प्रश्नों के उत्तर

15.1

1. (a) साईबर सुरक्षा (b) प्रचार

2. साईबर युद्ध को 'किसी देश द्वारा किसी अन्य देश के कंप्यूटर अथवा ढाँचे में उसे क्षति पहुँचाने अथवा नष्ट करने की दृष्टि से घुसपैठ करना' के रूप में परिभाषित किया गया है।

3. साईबर अपराध तब किया जाता है जब क्षति पहुँचाने के लिए कंप्यूटर के ज्ञान का प्रयोग किया जाता है।

4. (i) साईबर आक्रमण

   (ii) साईबर जासूसी

   (iii) साईबर प्रहार (तोड़-फोड़)

   (iv) साईबर प्रचार

15.2

1. (a) नोबेट्स

   (b) हैकर

   (c) क्रैकर

   (d) ट्रोजन होर्सिस

   (e) असत्य

2. (i) फ्रॉड और धोखाधड़ी

   (ii) कंप्यूटर को क्षति अथवा बदलाव

3. वायर्सिस और वायरस, ट्रोजन होर्सिस, तर्क/नालेज बम, रोबोट्स, एडवेयर, स्पाईवेयर

टिप्पणी

15.3

1. (a) कंपयूटर इमरजेंसी रिस्पांस टीम (CERT)

   (b) सूचना एवं संचार-प्रणाली (ICT)

   (c) नेशनल क्रिटीकल इंफार्मेशन इंफ्रास्ट्रकचर प्रोटेक्शन सेंटर (NCIIPC)

2. (a) सिस्टम को निक्कमा प्रदर्शन

   (b) सिस्टम को असामान्य व्यवहार जैसे सिस्टम का बार-बार शुरू हो जाना या रुक जाना।

   (c) अज्ञात सेवाएँ चल रही हों

   (d) एप्लीकेशन का खराब हो जाना

   (e) फाईलों के विस्तार अथवा सामग्री का बदल जाना

   (f) हार्ड डिस्क का निरंतर व्यस्त रहना अथवा इसकी लाईट का निरंतर जलते रहना

3. (i) यह आपके कंप्यूटर को बदनीयत अंदरुनी व्यक्ति के प्रहार से नहीं बचा सकता।

   (ii) यह OS से न गुजरने वाले कनेक्शन्स की रक्षा नहीं कर सकता।

   (iii) ई-मेल से पैदा हुए वायर्स के विरुद्ध यह आपकी रक्षा नहीं कर सकता।

4. क्योंकि यह प्रयोगकर्ता को सचेत करता है यदि कोई एप्लीकेशन अथवा प्रोग्राम उसके कंप्यूटर से जुड़ने का प्रयास कर रहा हो।