1. साइबर सुरक्षा

- साइबर सुरक्षा **सिस्टम, नेटवर्क और प्रोग्राम को डिजिटल हमलों से बचाने** का अभ्यास है।
- ये साइबर हमले आमतौर पर संवेदनशील जानकारी तक पहुंचने, बदलने या नष्ट करने के उद्देश्य से होते हैं; रैंसमवेयर के माध्यम से उपयोगकर्ताओं से पैसे ऐंठना; या सामान्य व्यावसायिक प्रक्रियाओं को बाधित करना भी इसका उद्देश्य हो सकता हैं।

1.1. साइबर खतरों की अवधारणा

- साइबर खतरे को कानूनी अधिकार के बिना डेटा, किसी एप्लिकेशन या संघीय प्रणाली तक पहुंच, घुसपैठ, हेरफेर या अखंडता, गोपनीयता, सुरक्षा या उपलब्धता को नुकसान पहुंचाने के लिए निर्देशित किसी भी पहचाने गए प्रयास के रूप में परिभाषित किया गया है।
- साइबर खतरा अनजाने और जानबूझकर, लक्षित या गैर-लक्षित हो सकता है। यह विभिन्न स्रोतों से आ सकता है, जिसमें जासूसी और सूचना युद्ध में लगे विदेशी राष्ट्र, अपराधी, हैकर्स, वायरस प्रोग्राम लेखक और संगठन के भीतर काम करने वाले असंतुष्ट कर्मचारी और ठेकेदार शामिल हो सकते हैं।
- अनजाने खतरे असावधान या अप्रशिक्षित कर्मचारियों, सॉफ़्टवेयर अपग्रेड, रखरखाव प्रक्रियाओं और उपकरण विफलताओं के कारण हो सकते हैं जो अनजाने में कंप्यूटर सिस्टम को बाधित करते हैं या डेटा को दूषित करते हैं।
- जानबूझकर दी गई धमकियों में लक्षित और गैर-लक्षित दोनों तरह के हमले शामिल हो सकते हैं।
    - लक्षित हमला तब होता है जब कोई समूह या व्यक्ति विशेष रूप से एक महत्वपूर्ण बुनियादी ढांचा प्रणाली पर हमला करता है।
    - एक गैर-लक्षित हमला तब होता है जब हमले का इच्छित लक्ष्य अनिश्चित होता है, जैसे कि जब कोई वायरस, वर्म या मैलवेयर बिना किसी विशिष्ट लक्ष्य के इंटरनेट पर जारी किया जाता है।
- बार-बार सबसे चिंताजनक रूप में पहचाने जाने वाला खतरा "अंदरूनी सूत्र" है - जिसमें कोई व्यक्ति वैध रूप से किसी सिस्टम या नेटवर्क तक पहुंच को अधिकृत करता है।

1.2. साइबर खतरों के प्रकार

- **डिनायल-ऑफ-सर्विस (DoS) और डिस्ट्रिब्यूटेड डिनायल-ऑफ-सर्विस (DDoS) हमले:** सेवा से इनकार करने वाला (DoS) हमला सिस्टम के संसाधनों पर हावी हो जाता है ताकि वह सेवा अनुरोधों का जवाब न दे सके। DDoS हमला भी एक सिस्टम के संसाधनों पर हमला है, लेकिन यह बड़ी संख्या में अन्य होस्ट मशीनों से लॉन्च किया जाता है जो हमलावर द्वारा नियंत्रित दुर्भाविनापूर्ण सॉफ़्टवेयर से संक्रमित होते हैं।
- **मैन-इन-द-मिडिल (MitM) हमला:** MitM हमला तब होता है जब हैकर क्लाइंट और सर्वर के संचार के बीच खुद को सम्मिलित करता है।

- **फ़िशिंग और स्पीयर फ़िशिंग हमले:** फ़िशिंग हमला एक प्रकार का ईमेल हमला है जिसमें एक हमलावर संबंधित विश्वसनीय संगठन से होने का दिखावा करके इलेक्ट्रॉनिक संचार के माध्यम से उपयोगकर्ताओं की संवेदनशील जानकारी को धोखाधड़ी से ढूंढने का प्रयास करता है। स्पीयर फ़िशिंग विशिष्ट संगठनों या व्यक्तियों को लक्षित करती है, और गोपनीय डेटा तक अनधिकृत पहुंच की तलाश करती है।
- **ड्राइव-बाय आक्रमण:** ड्राइव-बाय डाउनलोड आक्रमण मैलवेयर फैलाने का एक सामान्य तरीका है। हैकर्स असुरक्षित वेबसाइटों की तलाश करते हैं और किसी एक पेज पर HTTP या PHP कोड में एक दुर्भाविनापूर्ण (malicious) स्क्रिप्ट डालते हैं। यह स्क्रिप्ट साइट पर आने वाले किसी व्यक्ति के कंप्यूटर पर सीधे मैलवेयर इंस्टॉल कर सकती है, या यह पीड़ित को हैकर्स द्वारा नियंत्रित साइट पर पुन: निर्देशित कर सकती है।
- **पासवर्ड हमला:** ब्रूट-फोर्स पासवर्ड अनुमान लगाने का अर्थ है अलग-अलग पासवर्ड आज़माकर एक यादृच्छिक दृष्टिकोण का उपयोग करना और यह उम्मीद करना कि कोई काम करेगा।
- **SQL इंजेक्शन हमला:** डेटाबेस-संचालित वेबसाइटों के साथ SQL इंजेक्शन एक आम समस्या बन गई है।
- **क्रॉस-साइट स्क्रिप्टिंग (XSS) हमला:** XSS हमले किसी वेबसाइट के डेटाबेस में दुर्भाविनापूर्ण जावास्क्रिप्ट को इंजेक्ट करने के लिए तीसरे पक्ष के वेब संसाधनों का उपयोग करते हैं।
- **चोरी छुपे सुनना (eavesdropping) हमला:** यह नेटवर्क ट्रैफ़िक के अवरोधन के माध्यम से होता है। छिपकर, एक हमलावर पासवर्ड, क्रेडिट कार्ड नंबर और अन्य गोपनीय जानकारी प्राप्त कर सकता है जिसे उपयोगकर्ता नेटवर्क पर भेज सकता है।
- **मैलवेयर हमला:** मैलवेयर को अवांछित सॉफ़्टवेयर के रूप में वर्णित किया जा सकता है जो किसी सिस्टम में सहमति के बिना इंस्टॉल किया जाता है। यह खुद को वैध कोड से जोड़ सकता है और इंटरनेट पर खुद को प्रचारित या दोहरा सकता है।
- **रैनसमवेयर:** रैनसमवेयर एक प्रकार का मैलवेयर हमला है जिसमें हमलावर पीड़ित के डेटा को लॉक या एन्क्रिप्ट करता है और फिरौती का भुगतान न करने पर डेटा को प्रकाशित करने या उस तक पहुंच को ब्लॉक करने की धमकी देता है।

1.3. साइबर खतरों के स्रोत

- **बॉटनेट ऑपरेटर:** बॉटनेट ऑपरेटर हमलों को समन्वित करने और फ़िशिंग योजनाओं, स्पैम और मैलवेयर हमलों को वितरित करने के लिए समझौता किए गए, दूर से नियंत्रित सिस्टम के एक नेटवर्क या बॉटनेट का उपयोग करते हैं। इन नेटवर्कों की सेवाएँ कभी-कभी भूमिगत बाज़ारों में उपलब्ध कराई जाती हैं।
- **आपराधिक समूह:** आपराधिक समूह मौद्रिक लाभ के लिए सिस्टम पर हमला करना चाहते हैं। विशेष रूप से, संगठित आपराधिक समूह आइडेंटिटी चोरी और ऑनलाइन धोखाधड़ी करने के लिए स्पैम, फ़िशिंग और स्पाइवेयर/मैलवेयर का उपयोग करते हैं। अंतर्राष्ट्रीय कॉर्पोरेट जासूस और आपराधिक संगठन भी औद्योगिक जासूसी और बड़े पैमाने पर मौद्रिक चोरी करने और हैकर

प्रतिभा को काम पर रखने या विकसित करने की अपनी क्षमता के माध्यम से खतरा पैदा करते हैं।

- **विदेशी राष्ट्र:** विदेशी ख़ुफ़िया सेवाएँ अपनी सूचना एकत्र करने और जासूसी गतिविधियों के हिस्से के रूप में साइबर उपकरणों का उपयोग करती हैं। साथ ही, कई राष्ट्र सूचना युद्ध सिद्धांत, कार्यक्रम और क्षमताओं को विकसित करने के लिए आक्रामक रूप से काम कर रहे हैं। ऐसी क्षमताएं सैन्य शक्ति का समर्थन करने वाली आपूर्ति, संचार और आर्थिक बुनियादी ढांचे को बाधित करके एक इकाई को महत्वपूर्ण और गंभीर प्रभाव डालने में सक्षम बनाती हैं।
- **हैकर्स:** हैकर्स बदला लेने, दूसरों का पीछा करने और मौद्रिक लाभ के लिए नेटवर्क ब्रेक करते हैं। जबकि अनधिकृत पहुंच प्राप्त करने के लिए पहले उचित मात्रा में कौशल या कंप्यूटर ज्ञान की आवश्यकता होती थी, हैकर्स अब इंटरनेट से हमले की स्क्रिप्ट और प्रोटोकॉल डाउनलोड कर सकते हैं और उन्हें पीड़ित साइटों के खिलाफ लॉन्च कर सकते हैं।
- **हैक्टिविस्ट:** जो सार्वजनिक रूप से प्रवेश्य वेब पेजों या ई-मेल सर्वर पर राजनीति से प्रेरित हमले करते हैं। ये समूह और व्यक्ति राजनीतिक संदेश भेजने के लिए ई-मेल सर्वर को ओवरलोड करते हैं और वेबसाइटों को हैक करते हैं।
- **अंदरूनी सूत्र:** किसी संगठन के भीतर से काम करने वाला असंतुष्ट अंदरूनी सूत्र, कंप्यूटर अपराधों का एक प्रमुख स्रोत हो सकता है। अंदरूनी सूत्र सिस्टम को नुकसान पहुंचा सकते है या सिस्टम से डेटा चुरा सकते है। अंदरूनी खतरे में ठेकेदार कर्मी भी शामिल हैं।
- **अंतर्राष्ट्रीय कॉर्पोरेट जासूस:** अंतर्राष्ट्रीय कॉर्पोरेट जासूस आर्थिक और औद्योगिक जासूसी और बड़े पैमाने पर मौद्रिक चोरी करने और हैकर प्रतिभा को काम पर रखने या विकसित करने की अपनी क्षमता के माध्यम से खतरा पैदा करते हैं।
- **फ़िशर:** व्यक्ति, या छोटे समूह, मौद्रिक लाभ के लिए पहचान या जानकारी चुराने के प्रयास में फ़िशिंग योजनाओं को अंजाम देते हैं। फ़िशर अपने उद्देश्यों को पूरा करने के लिए स्पैम और स्पाइवेयर/मैलवेयर का भी उपयोग कर सकते हैं।
- **स्पैमर:** व्यक्ति या संगठन उत्पादों को बेचने, फ़िशिंग योजनाओं का संचालन करने, स्पाइवेयर/मैलवेयर वितरित करने, या संगठनों पर हमला करने (यानी, सेवा हमले से इनकार करने) के लिए छिपी या झूठी जानकारी के साथ अनचाहे ई-मेल वितरित करते हैं।
- **स्पाइवेयर/मैलवेयर लेखक:** दुर्भावनापूर्ण इरादे वाले व्यक्ति या संगठन स्पाइवेयर और मैलवेयर का उत्पादन और वितरण करके उपयोगकर्ताओं के खिलाफ हमले करते हैं। मेलिसा वायरस, एक्सप्लोर.ज़िप वर्म, CIH (चेरनोबिल) वायरस, निमडा वर्म, कोड रेड, स्लैमर वर्म और ब्लास्टर वर्म सहित कई विनाशकारी कंप्यूटर वायरस और वर्म फाइलों और हार्ड ड्राइव को नुकसान पहुंचाते है।
- **आतंकवादी:** आतंकवादी राष्ट्रीय सुरक्षा को खतरे में डालने, सैन्य उपकरणों से समझौता करने, अर्थव्यवस्था को बाधित करने और बड़े पैमाने पर हताहत करने के लिए महत्वपूर्ण इन्फ्रास्ट्रक्चर को नष्ट करने, घुसपैठ करने या शोषण करने के लिए साइबर हमले करते हैं।

2. भारत में साइबर सुरक्षा परिदृश्य

- भारत में, भारतीय व्यवसायों और सरकारी संस्थानों पर साइबर हमलों की बढ़ती संख्या के कारण हाल के वर्षों में साइबर सुरक्षा सर्वोच्च प्राथमिकता बन गई है।
- भारत में हाल के वर्षों में फ़िशिंग हमले बढ़ रहे हैं। एक उल्लेखनीय उदाहरण भारतीय रिज़र्व बैंक पर 2017 का फ़िशिंग हमला है जिसके परिणामस्वरूप $1 मिलियन से अधिक की चोरी हुई।
- भारत में मैलवेयर हमले भी आम हैं। 2016 में, WannaCry रैंसमवेयर हमले ने आंध्र प्रदेश पुलिस बल और भारत संचार निगम लिमिटेड (BSNL) सहित कई भारतीय संगठनों को प्रभावित किया।
- भारत में 2022 में 13.91 लाख साइबर सुरक्षा घटनाएं देखी गईं। संख्याएं अभी भी देश पर साइबर हमलों की पूरी तस्वीर नहीं देती हैं क्योंकि इन आंकड़ों में केवल CERT-In द्वारा रिपोर्ट की गई और ट्रैक की गई जानकारी शामिल है।
- इन चुनौतियों के बावजूद, जब साइबर सुरक्षा की बात आती है तो भारत में सकारात्मक रुझान उभर रहे हैं।
- भारत सरकार ने देश की साइबर सुरक्षा स्थिति में सुधार के लिए कई कदम उठाए हैं, जिसमें राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre-NCIIPC) की स्थापना और राष्ट्रीय साइबर समन्वय केंद्र (National Cyber Coordination Centre-NCCC) बनाना शामिल है।
- इसके अलावा, सरकार ने नागरिकों को साइबर सुरक्षा खतरों के बारे में शिक्षित करने और खुद को सुरक्षित रखने के तरीके के बारे में शिक्षित करने के लिए विभिन्न जागरूकता अभियान शुरू किए हैं।
- भारतीय साइबर स्पेस को सुरक्षित करने के लिए भारत में अनुसंधान एवं विकास, कानूनी ढांचा, सुरक्षा घटनाएं, प्रारंभिक चेतावनी और प्रतिक्रिया, सर्वोत्तम सुरक्षा नीति अनुपालन और आश्वासन, अंतर्राष्ट्रीय सहयोग और सुरक्षा प्रशिक्षण जैसे दृष्टिकोण भी अपनाए जाते हैं।

2.1. सूचना प्रौद्योगिकी (IT) अधिनियम, 2000

- 2000 का IT अधिनियम भारत की संसद द्वारा अधिनियमित किया गया था और भारतीय साइबर सुरक्षा कानून का मार्गदर्शन करने, डेटा सुरक्षा नीतियों को स्थापित करने और साइबर अपराध को नियंत्रित करने के लिए **भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम** (Indian Computer Emergency Response Team-CERT-In) **द्वारा प्रशासित** किया गया था।
- यह ई-गवर्नेंस, ई-बैंकिंग, ई-कॉमर्स और निजी क्षेत्र सहित कई अन्य की भी सुरक्षा करता है।
- हालाँकि भारत के पास कोई विशिष्ट, एकात्मक साइबर सुरक्षा कानून नहीं है, यह साइबर सुरक्षा मानकों को बढ़ावा देने के लिए IT अधिनियम और कई अन्य क्षेत्र-विशिष्ट नियमों का उपयोग करता है। यह भारत में महत्वपूर्ण सूचना बुनियादी ढांचे के लिए एक कानूनी ढांचा भी प्रदान करता है।

- इस अधिनियम को **सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 के माध्यम से संशोधित** किया गया था। संशोधन लागू किए गए और महत्वपूर्ण अनुभागों के नियम अक्टूबर, 2009 में अधिसूचित किए गए थे जो राष्ट्रीय साइबर सुरक्षा की जरूरतों को संबोधित करते हैं।
- संशोधन में अन्य बातों के साथ-साथ साइबर अपराधों के नए रूपों से निपटने के लिए IT अधिनियम, 2000 में प्रावधान जोड़े गए, जैसे इलेक्ट्रॉनिक रूप में स्पष्ट यौन सामग्री को प्रचारित करना, वीडियो ताक-झांक और गोपनीयता का उल्लंघन और मध्यस्थ और ई-कॉमर्स धोखाधड़ी द्वारा डेटा का रिसाव।
- 2008 का IT अधिनियम किसी भी व्यक्ति, कंपनी या संगठन (मध्यस्थों) पर लागू होता है जो भारत में कंप्यूटर संसाधनों, कंप्यूटर नेटवर्क या अन्य सूचना प्रौद्योगिकी का उपयोग करता है।

2.2. राष्ट्रीय साइबर सुरक्षा नीति, 2013

- भारत सरकार ने 1 जुलाई 2013 को साइबर हमलों को रोकने के लिए सूचना की सुरक्षा और क्षमताओं का निर्माण करने के उद्देश्य से राष्ट्रीय साइबर सुरक्षा नीति 2013 लॉन्च की।
- इस नीति का उद्देश्य सरकारी और गैर-सरकारी संस्थाओं सहित सूचना और संचार प्रौद्योगिकी उपयोगकर्ताओं और प्रदाताओं के व्यापक स्पेक्ट्रम को पूरा करना है।
- राष्ट्रीय साइबर सुरक्षा नीति 2013 देश की भौतिक और व्यावसायिक संपत्तियों की सुरक्षा के लिए है।

राष्ट्रीय साइबर सुरक्षा नीति 2013 की मुख्य विशेषताएं

- यह नीति देश के साइबर सुरक्षा मुद्दों से निपटने के लिए व्यापक, सहयोगात्मक और सामूहिक जिम्मेदारी के लिए एक रूपरेखा तैयार करती है।
- नीति में **14 उद्देश्य** बताए गए हैं जिनमें क्षमता निर्माण, कौशल विकास और प्रशिक्षण के माध्यम से अगले पांच वर्षों में 5,00,000 मजबूत पेशेवर, कुशल कार्यबल का निर्माण शामिल है।
- नीति में ICT इन्फ्रास्ट्रक्चर के खतरों के संबंध में रणनीतिक जानकारी प्राप्त करने, प्रभावी, पूर्वानुमानित, निवारक, सक्रिय प्रतिक्रिया और पुनर्प्राप्ति कार्यों के माध्यम से प्रतिक्रिया, समाधान और संकट प्रबंधन के लिए परिदृश्य बनाने के लिए राष्ट्रीय और क्षेत्रीय स्तर पर 24×7 तंत्र बनाने की योजना है।
- यह नीति एक सुरक्षित साइबर इको-सिस्टम बनाने के लिए आठ अलग-अलग रणनीतियों की पहचान करती है, जिसमें विभिन्न उत्पादों या सेवाओं के बीच अंतरसंचालनीयता और डेटा विनिमय की सुविधा के लिए खुले मानकों को प्रोत्साहित करने के अलावा एक आश्वासन ढांचा बनाने की आवश्यकता भी शामिल है।

अन्य लक्ष्य में शामिल हैं

- व्यक्तियों, संगठनों और सरकार के लिए एक लचीला और सुरक्षित साइबरस्पेस बनाना।
- साइबर घटनाओं और साइबर खतरों को कम करने, तेजी से रोकने या प्रतिक्रिया देने के लिए रूपरेखा, क्षमताएं और भेद्यता प्रबंधन रणनीतियां बनाना।

- संगठनों को ऐसी साइबर सुरक्षा नीतियां विकसित करने के लिए प्रोत्साहित करना जो रणनीतिक लक्ष्यों, व्यावसायिक वर्कफ़्लो और सामान्य सर्वोत्तम प्रथाओं के अनुरूप हों।
- साथ ही साइबर अपराध से होने वाले नुकसान को कम करने के लिए संस्थागत संरचनाएं, प्रक्रियाएं, प्रौद्योगिकी और सहयोग बनाना।

2.3. सूचना प्रौद्योगिकी नियम

- केंद्र सरकार द्वारा फरवरी 2021 में सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021 ('2021 नियम') जारी किए गए थे।
- 2021 नियम **सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 69ए(2), 79(2)(सी) और 87 के तहत** पारित किए गए हैं।
- 2021 के नियम को पहले से अधिनियमित सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश) नियम 2011 के स्थान पर लाया गया।
- 2021 नियम सोशल मीडिया के सामान्य उपयोगकर्ताओं को सशक्त बनाने और एक सुरक्षित और भरोसेमंद ऑनलाइन वातावरण के लिए सोशल मीडिया मध्यस्थों (Social Media Intermediaries-SMIs) और महत्वपूर्ण सोशल मीडिया मध्यस्थों (Significant Social Media Intermediaries-SSMI) पर दायित्व डालने के लिए नियामक ढांचे को अद्यतन करने के लिए पेश किए गए थे।
- यह सोशल मीडिया पर यौन अपराधों से महिलाओं और बच्चों की सुरक्षा पर विशेष जोर देता है।

सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) संशोधन नियम, 2023 ('2023 संशोधन')

- 6 अप्रैल, 2023 को, इलेक्ट्रॉनिक्स और आईटी मंत्रालय (Ministry of Electronics and IT-MeitY) ने आईटी नियम 2021 में संशोधन करने के लिए सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) संशोधन नियम 2023 को अधिसूचित किया।
- यह संशोधन केंद्र सरकार को केंद्र सरकार के किसी भी व्यवसाय के संबंध में "फर्जी या गलत या भ्रामक" जानकारी की पहचान करने के लिए "तथ्य जांच इकाई" नामित करने के लिए अधिकृत करता है।
- प्रारंभ में, इस संशोधन में केवल ऑनलाइन गेमिंग कंपनियों को विनियमित करने के प्रावधान शामिल थे। लेकिन बाद में MeitY ने एक नया मसौदा प्रकाशित किया जिसमें "तथ्य-जाँच शक्तियाँ" शामिल थीं।
- तथ्य जांच इकाई सरकारी अधिकारियों और मंत्रालयों के बारे में किसी भी ऑनलाइन टिप्पणी, समाचार रिपोर्ट या राय की जांच कर सकती है और फिर इसकी सेंसरशिप के लिए ऑनलाइन मध्यस्थों को सूचित कर सकती है।
- ऐसे मध्यस्थों में न केवल ऑनलाइन सोशल मीडिया कंपनियां शामिल हैं, बल्कि इंटरनेट सेवा प्रदाता और फ़ाइल होस्टिंग कंपनियां जैसे सेवा प्रदाता भी शामिल हैं।

- यदि कोई मध्यस्थ अनुपालन करने में विफल रहता है, तो उन्हें IT अधिनियम, 2000 की **धारा 79 के तहत** अपनी सुरक्षित हार्बर स्थिति खोने का जोखिम होगा।
    - सुरक्षित हार्बर प्रावधान में कहा गया है कि "एक मध्यस्थ उसके द्वारा उपलब्ध या होस्ट की गई किसी भी तीसरे पक्ष की जानकारी, डेटा या संचार लिंक के लिए उत्तरदायी नहीं होगा"।

2.4. राष्ट्रीय साइबर सुरक्षा रणनीति 2020

- राष्ट्रीय साइबर सुरक्षा रणनीति 2020 को मार्च 2021 में राष्ट्रीय सुरक्षा परिषद सचिवालय में राष्ट्रीय साइबर सुरक्षा समन्वयक के कार्यालय द्वारा तैयार किया गया था।
- रणनीति का उद्देश्य **साइबर सुरक्षा ऑडिट गुणवत्ता में सुधार करना** है ताकि संगठन अपने साइबर सुरक्षा वास्तुकला और ज्ञान की बेहतर समीक्षा कर सकें।
- योजना का मुख्य लक्ष्य साइबर घटनाओं, साइबर आतंकवाद और साइबरस्पेस में जासूसी को रोकने के लिए हितधारकों, नीति निर्माताओं और कॉर्पोरेट नेताओं के लिए आधिकारिक मार्गदर्शन के रूप में कार्य करना है।
- इसमें साइबर तैयारियों के सूचकांक और प्रदर्शन की निगरानी की भी आवश्यकता है।

2.5. भारतीय रिज़र्व बैंक अधिनियम, 2018

- भारतीय रिजर्व बैंक ने 2018 में RBI अधिनियम पेश किया, जिसमें **UCBs** (urban co-operative banks-शहरी सहकारी बैंक) **और भुगतान ऑपरेटरों के लिए साइबर सुरक्षा** दिशानिर्देश और ढांचे का विवरण दिया गया है। 2018 के RBI अधिनियम का लक्ष्य है:
    - ऐसे मानक बनाना जो बैंकों और भुगतान ऑपरेटरों के सुरक्षा ढांचे को नई प्रौद्योगिकियों और डिजिटलीकरण के अनुकूल बनाने के तरीके के अनुसार समान बने।
    - बैंकों को अपनी साइबर संकट प्रबंधन योजनाएँ बनाने और प्रस्तुत करने का आदेश देना।
    - बैंकों को नियमित रूप से खतरा मूल्यांकन ऑडिट शेड्यूल करने के लिए प्रोत्साहित करना।
    - बैंकों को एंटी-फ़िशिंग और एंटी-मैलवेयर तकनीक के साथ अपने स्वयं के ईमेल डोमेन को लागू करने में सहायता करना।
    - सभी भारतीय बैंकों को भुगतान प्रसंस्करण साइबर सुरक्षा के लिए ढांचे को मानकीकृत करने और डिजिटल वातावरण में लगातार बढ़ती व्यावसायिक जटिलताओं से निपटने के लिए इन दिशानिर्देशों का पालन करना चाहिए।

2.6. भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In)

- **2004 में** आधिकारिक बनाया गया, CERT-In सूचना प्रौद्योगिकी अधिनियम, 2000 की **धारा 70बी के तहत** स्थापित **राष्ट्रीय नोडल एजेंसी** है, जो कंप्यूटर सुरक्षा संबंधी घटनाओं के घटित होने पर प्रतिक्रिया देती है।

- CERT-In अपनी वेबसाइट पर सूचना के प्रसार के माध्यम से सुरक्षा मुद्दों पर जागरूकता पैदा करता है और 24x7 घटना प्रतिक्रिया सहायता डेस्क संचालित करता है।
- यह घटना निवारण और प्रतिक्रिया सेवाओं के साथ-साथ सुरक्षा गुणवत्ता प्रबंधन सेवा भी प्रदान करता है।
- CERT-In साइबर सुरक्षा के क्षेत्र में निम्नलिखित कार्य करता है:
    - साइबर घटनाओं पर सूचना का संग्रहण, विश्लेषण और प्रसार;
    - साइबर सुरक्षा घटनाओं का पूर्वानुमान और अलर्ट;
    - साइबर सुरक्षा घटनाओं से निपटने के लिए आपातकालीन उपाय;
    - साइबर घटना प्रतिक्रिया गतिविधियों का समन्वय;
    - साइबर घटनाओं की सूचना सुरक्षा, प्रथाओं, प्रक्रियाओं, रोकथाम, प्रतिक्रिया और रिपोर्टिंग से संबंधित दिशानिर्देश, सलाह, भेद्यता नोट और श्वेतपत्र जारी करना; और
    - साइबर सुरक्षा से संबंधित ऐसे अन्य कार्य जो निर्धारित किये जा सकते हैं।

2.7. राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Center-NCIIPC)

- NCIIPC की स्थापना **16 जनवरी 2014 को IT अधिनियम, 2000 की धारा 70ए के तहत** भारत सरकार द्वारा की गई थी।
- **नई दिल्ली में स्थित,** NCIIPC को महत्वपूर्ण सूचना अवसंरचना संरक्षण के मामले में राष्ट्रीय नोडल एजेंसी के रूप में नियुक्त किया गया था।
- इसके अतिरिक्त, NCIIPC को **राष्ट्रीय तकनीकी अनुसंधान संगठन** (National Technical Research Organization-NTRO) की एक इकाई माना जाता है और इसलिए यह प्रधान मंत्री कार्यालय के अंतर्गत आता है।
- NCIIPC को महत्वपूर्ण सूचना बुनियादी ढांचे के लिए राष्ट्रीय स्तर के खतरों की निगरानी और रिपोर्ट करना आवश्यक है। महत्वपूर्ण क्षेत्रों में शामिल हैं:
    - शक्ति और ऊर्जा
    - बैंकिंग, वित्तीय सेवाएँ और बीमा
    - दूरसंचार और सूचना
    - परिवहन
    - सरकार
    - सामरिक और सार्वजनिक उद्यम
- NCIIPC ने इन महत्वपूर्ण क्षेत्रों, विशेष रूप से बिजली और ऊर्जा में, संगठनों के लिए नीति मार्गदर्शन, ज्ञान साझाकरण और साइबर सुरक्षा जागरूकता के लिए कई दिशानिर्देशों को सफलतापूर्वक लागू किया है।

2.8. साइबर विनियम अपीलीय न्यायाधिकरण (Cyber Regulations Appellate Tribunal-CRAT)

- **IT अधिनियम, 2000, धारा 62 के तहत,** भारत की केंद्र सरकार ने तथ्य-खोज, साइबर साक्ष्य प्राप्त करने और गवाहों की जांच करने के लिए एक मुख्य शासी निकाय और प्राधिकरण के रूप में साइबर विनियमन अपीलीय न्यायाधिकरण बनाया।
- सिविल न्यायालय और सिविल प्रक्रिया संहिता, 1908 के अनुसार, CRAT के पास यह शक्ति है:
    - शपथपत्रों पर साक्ष्य प्राप्त करना।
    - सुनिश्चित करना कि सभी इलेक्ट्रॉनिक और साइबर साक्ष्य और रिकॉर्ड अदालत के लिए प्रस्तुत किए जाएं।
    - गवाहों, दस्तावेजों और शपथ के तहत लोगों की जांच के लिए नियमित कमीशन लागू करना, बुलाना और जारी करना।
    - घटनाओं और मामलों को सुलझाने के लिए न्यायालय के अंतिम निर्णयों की समीक्षा करना।
    - डिफॉल्टर के आवेदनों को एकपक्षीय रूप से स्वीकृत, खारिज या घोषित करना।

3. डिजिटल व्यक्तिगत डेटा संरक्षण (Digital Personal Data Protection-DPDP) अधिनियम, 2023

- 11 अगस्त, 2023 को डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 (अधिनियम) को भारत के राष्ट्रपति की सहमति प्राप्त हुई और इसे आधिकारिक राजपत्र में प्रकाशित किया गया।
- DPDP अधिनियम **भारत का पहला डेटा संरक्षण अधिनियम** है, और यह **भारत में व्यक्तिगत डेटा के प्रसंस्करण के लिए एक रूपरेखा** स्थापित करता है।
- यह डिजिटल व्यक्तिगत डेटा के प्रसंस्करण के लिए इस तरह से प्रावधान करता है जो व्यक्तियों के अपने व्यक्तिगत डेटा की सुरक्षा के अधिकारों और वैध उद्देश्यों के लिए और उससे जुड़े या प्रासंगिक मामलों के लिए ऐसे व्यक्तिगत डेटा को संसाधित करने की आवश्यकता दोनों को पहचानता है।
- यह अधिनियम संक्षिप्त और सरल है, यानी सरल, सुलभ, तर्कसंगत और कार्रवाई योग्य कानून है, और संसदीय कानून बनाने में महिलाओं को स्वीकार करने के लिए "he" के बजाय "she" शब्द का इस्तेमाल किया गया है।

सात सिद्धांत

यह अधिनियम निम्नलिखित सात सिद्धांतों पर आधारित है:

- व्यक्तिगत डेटा के सहमतिपूर्ण, वैध और पारदर्शी उपयोग का सिद्धांत;
- उद्देश्य सीमा का सिद्धांत (व्यक्तिगत डेटा का उपयोग केवल डेटा प्रिंसिपल की सहमति प्राप्त करने के समय निर्दिष्ट उद्देश्य के लिए);

- डेटा न्यूनीकरण का सिद्धांत (केवल उतना ही व्यक्तिगत डेटा एकत्र करना जितना निर्दिष्ट उद्देश्य को पूरा करने के लिए आवश्यक है);
- डेटा सटीकता का सिद्धांत (सुनिश्चित करना कि डेटा सही और अद्यतन है);
- भंडारण सीमा का सिद्धांत (डेटा को केवल तब तक संग्रहीत करना जब तक कि निर्दिष्ट उद्देश्य के लिए इसकी आवश्यकता हो);
- उचित सुरक्षा उपायों का सिद्धांत; और
- जवाबदेही का सिद्धांत (डेटा उल्लंघनों और विधेयक के प्रावधानों के उल्लंघनों के निर्णय और उल्लंघनों के लिए दंड लगाने के माध्यम से)।

डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 की मुख्य विशेषताएं

प्रयोज्यता

- यह अधिनियम भारत के भीतर डिजिटल व्यक्तिगत डेटा के ऐसे प्रसंस्करण पर लागू होता है जहां ऐसा डेटा ऑनलाइन एकत्र किया जाता है, या ऑफ़लाइन एकत्र किया जाता है और डिजिटलीकृत किया जाता है।
- यह भारत के बाहर व्यक्तिगत डेटा के प्रसंस्करण पर भी लागू होगा यदि यह भारत में वस्तुओं या सेवाओं की पेशकश के लिए है तो। व्यक्तिगत डेटा को किसी व्यक्ति के बारे में किसी भी डेटा के रूप में परिभाषित किया जाता है जो ऐसे डेटा के आधार पर या उसके संबंध में पहचाना जा सकता है।

सहमति

- व्यक्तिगत डेटा को व्यक्ति की सहमति प्राप्त करने के बाद केवल वैध उद्देश्य के लिए संसाधित किया जा सकता है। सहमति लेने से पहले एक नोटिस दिया जाना चाहिए।
- नोटिस में एकत्र किए जाने वाले व्यक्तिगत डेटा और प्रसंस्करण के उद्देश्य के बारे में विवरण होना चाहिए। सहमति किसी भी समय वापस ली जा सकती है।
- निम्नलिखित सहित 'वैध उपयोगों' के लिए सहमति की आवश्यकता नहीं होगी:
    - निर्दिष्ट उद्देश्य जिसके लिए डेटा किसी व्यक्ति द्वारा स्वेच्छा से प्रदान किया गया है,
    - सरकार द्वारा लाभ या सेवा का प्रावधान,
    - चिकित्सा आपातकाल, और
    - रोज़गार।
- 18 वर्ष से कम आयु के व्यक्तियों के लिए, माता-पिता या कानूनी अभिभावक द्वारा सहमति प्रदान की जाएगी।

डेटा प्रिंसिपल के अधिकार

- डेटा प्रिंसिपल वह व्यक्ति होता है जिसका डेटा संसाधित किया जा रहा है। उसे इसका अधिकार होगा:
    - प्रसंस्करण के बारे में जानकारी प्राप्त करना,
    - व्यक्तिगत डेटा में सुधार और उसे मिटाने की मांग करना,

- मृत्यु या अक्षमता की स्थिति में अधिकारों का प्रयोग करने के लिए किसी अन्य व्यक्ति को नामांकित करना, और
- शिकायत निवारण।

डेटा प्रिंसिपल के कर्तव्य

- डेटा प्रिंसिपलों के कुछ कर्तव्य होंगे। उन्हें यह नहीं करना चाहिए:
  - झूठी या तुच्छ शिकायत दर्ज करना, और
  - निर्दिष्ट मामलों में कोई गलत विवरण प्रस्तुत करना या किसी अन्य व्यक्ति का प्रतिरूपण करना।
- कर्तव्यों का उल्लंघन करने पर **10,000 रूपये तक का जुर्माना** लगाया जाएगा।

डेटा फ़िडुशियरी के दायित्व

- डेटा प्रत्ययी वह इकाई है जो प्रसंस्करण के उद्देश्य और साधन का निर्धारण करती है। डेटा प्रत्ययी को यह करना होगा:
  - डेटा की सटीकता और पूर्णता सुनिश्चित करने के लिए उचित प्रयास करना,
  - डेटा उल्लंघन को रोकने के लिए उचित सुरक्षा उपाय बनाना,
  - उल्लंघन की स्थिति में भारतीय डेटा संरक्षण बोर्ड और प्रभावित व्यक्तियों को सूचित करना, और
  - उद्देश्य पूरा होते ही व्यक्तिगत डेटा मिटा दें और कानूनी उद्देश्यों के लिए इसे बनाए रखना आवश्यक नहीं है।
- सरकारी संस्थाओं के मामले में, भंडारण सीमा और डेटा प्रिंसिपल का मिटाने का अधिकार लागू नहीं होगा।

भारत के बाहर व्यक्तिगत डेटा का स्थानांतरण

- अधिनियम अधिसूचना के माध्यम से केंद्र सरकार द्वारा प्रतिबंधित देशों को छोड़कर, भारत के बाहर व्यक्तिगत डेटा के हस्तांतरण की अनुमति देता है।

छूट

- डेटा प्रिंसिपल के अधिकार और डेटा फिड्यूशियरीज़ के दायित्व (डेटा सुरक्षा को छोड़कर) निर्दिष्ट मामलों में लागू नहीं होंगे। इसमे शामिल है:
  - अपराधों की रोकथाम और जांच, और
  - कानूनी अधिकारों या दावों का प्रवर्तन।
- केंद्र सरकार, अधिसूचना द्वारा, कुछ गतिविधियों को अधिनियम के लागू होने से छूट दे सकती है। इसमे शामिल है:
  - राज्य की सुरक्षा और सार्वजनिक व्यवस्था के हित में सरकारी संस्थाओं द्वारा प्रसंस्करण, और
  - अनुसंधान, संग्रह, या सांख्यिकीय उद्देश्य।

भारतीय डेटा संरक्षण बोर्ड

- केंद्र सरकार भारतीय डेटा संरक्षण बोर्ड की स्थापना करेगी। बोर्ड के प्रमुख कार्यों में शामिल हैं:
    - अनुपालन की निगरानी करना और जुर्माना लगाना,
    - डेटा ब्रीच की स्थिति में आवश्यक उपाय करने के लिए डेटा फिड्यूशियरीज़ को निर्देशित करना, और
    - प्रभावित व्यक्तियों द्वारा की गई शिकायतों को सुनना।

दंड

- अधिनियम की अनुसूची विभिन्न अपराधों के लिए दंड निर्दिष्ट करती है जैसे:
    - बच्चों के लिए दायित्वों को पूरा न करने के लिए 200 करोड़ रुपये, और
    - डेटा उल्लंघनों को रोकने के लिए सुरक्षा उपाय करने में विफलता के लिए 250 करोड़ रुपये।

महत्वपूर्ण मुद्दे

- राष्ट्रीय सुरक्षा जैसे आधारों पर राज्य द्वारा डेटा प्रोसेसिंग में छूट से डेटा संग्रह, प्रसंस्करण और आवश्यकता से अधिक प्रतिधारण हो सकता है। इससे निजता के **मौलिक अधिकार का उल्लंघन** हो सकता है।
- अधिनियम व्यक्तिगत डेटा के प्रसंस्करण से उत्पन्न होने वाले नुकसान के जोखिमों को विनियमित नहीं करता है।
- अधिनियम डेटा पोर्टेबिलिटी का अधिकार और डेटा प्रिंसिपल को भूल जाने का अधिकार नहीं देता है।
- अधिनियम केंद्र सरकार द्वारा अधिसूचित देशों को छोड़कर, **भारत के बाहर व्यक्तिगत डेटा के हस्तांतरण की अनुमति** देता है। यह तंत्र उन देशों में डेटा सुरक्षा मानकों का पर्याप्त मूल्यांकन सुनिश्चित नहीं कर सकता है जहां व्यक्तिगत डेटा के हस्तांतरण की अनुमति है।
- भारतीय डेटा संरक्षण बोर्ड के सदस्यों की नियुक्ति दो साल के लिए की जाएगी और वे पुनर्नियुक्ति के लिए पात्र होंगे। पुनर्नियुक्ति की गुंजाइश वाला अल्पावधि बोर्ड के स्वतंत्र कामकाज को प्रभावित कर सकता है।

1. इंटरनेट ऑफ थिंग्स (Internet of Things-IoT)

- इंटरनेट ऑफ थिंग्स शब्द का तात्पर्य जुड़े हुए उपकरणों और प्रौद्योगिकी के सामूहिक नेटवर्क से है जो **उपकरणों और क्लाउड के साथ-साथ स्वयं उपकरणों के बीच संचार की सुविधा** प्रदान करता है।
- मूल रूप से, IoT रोजमर्रा की "चीजों" को इंटरनेट के साथ एकीकृत करता है।

1.1. IoT का कार्य

- IoT सिस्टम वास्तविक समय में डेटा के संग्रह और आदान-प्रदान के माध्यम से काम करते हैं। एक IoT प्रणाली में तीन घटक होते हैं: **स्मार्ट डिवाइस, IoT एप्लिकेशन और एक ग्राफिकल यूजर इंटरफ़ेस।**
- स्मार्ट डिवाइस एक उपकरण है, जैसे टेलीविजन, सुरक्षा कैमरा, या व्यायाम उपकरण जिसे कंप्यूटिंग क्षमताएं दी गई हैं। यह अपने वातावरण, उपयोगकर्ता इनपुट या उपयोग पैटर्न से डेटा एकत्र करता है और अपने IoT एप्लिकेशन से इंटरनेट पर डेटा संचार करता है।
- IoT एप्लिकेशन सेवाओं और सॉफ़्टवेयर का एक संग्रह है जो विभिन्न IoT उपकरणों से प्राप्त डेटा को एकीकृत करता है। यह इस डेटा का विश्लेषण करने और सूचित निर्णय लेने के लिए मशीन लर्निंग या कृत्रिम बुद्धिमत्ता (Artificial Intelligence-AI) तकनीक का उपयोग करता है।
- निर्णय वापस IoT डिवाइस को सूचित कर दिए जाते हैं और IoT डिवाइस फिर इनपुट पर समझदारी से प्रतिक्रिया करता है।
- IoT डिवाइस को ग्राफिकल यूजर इंटरफ़ेस के माध्यम से प्रबंधित किया जा सकता है।

1.2. IoT उपकरणों के उदाहरण

कनेक्टेड कारें

- ऐसे कई तरीके हैं जिनसे वाहनों, जैसे कारों, को इंटरनेट से जोड़ा जा सकता है। यह स्मार्ट डैशकैम, इंफोटेनमेंट सिस्टम या यहां तक कि वाहन के कनेक्टेड गेटवे के माध्यम से भी हो सकता है।
- वे ड्राइवर के प्रदर्शन और वाहन दोनों की निगरानी के लिए एक्सीलेटर, ब्रेक, स्पीडोमीटर, ओडोमीटर, पहियों और ईंधन टैंक से डेटा एकत्र करते हैं।

कनेक्टेड घर

- स्मार्ट होम डिवाइस मुख्य रूप से घर की दक्षता और सुरक्षा में सुधार के साथ-साथ घरेलू नेटवर्किंग में सुधार पर केंद्रित हैं।
- स्मार्ट आउटलेट जैसे उपकरण बिजली के उपयोग की निगरानी करते हैं और स्मार्ट थर्मोस्टेट बेहतर तापमान नियंत्रण प्रदान करते हैं।
- हाइड्रोपोनिक सिस्टम बगीचे के प्रबंधन के लिए IoT सेंसर का उपयोग कर सकते हैं जबकि IoT स्मोक डिटेक्टर तंबाकू के धुएं का पता लगा सकते हैं।

- दरवाज़े के ताले, सुरक्षा कैमरे और पानी रिसाव डिटेक्टर जैसी घरेलू सुरक्षा प्रणालियाँ खतरों का पता लगा सकती हैं और उन्हें रोक सकती हैं, और घर के मालिकों को अलर्ट भेज सकती हैं।

स्मार्ट शहर

- IoT अनुप्रयोगों ने शहरी नियोजन और इन्फ्रास्ट्रक्चर के रखरखाव को अधिक कुशल बना दिया है।
- IoT अनुप्रयोगों का उपयोग वायु गुणवत्ता और विकिरण के स्तर को मापने, स्मार्ट प्रकाश व्यवस्था के साथ ऊर्जा बिल को कम करने, महत्वपूर्ण इन्फ्रास्ट्रक्चर के लिए रखरखाव की जरूरतों का पता लगाने और कुशल पार्किंग प्रबंधन के माध्यम से मुनाफा बढ़ाने के लिए किया जा सकता है।

उत्पादन

- IoT एप्लिकेशन मशीन की विफलता होने से पहले ही उसका अनुमान लगा सकते हैं, जिससे उत्पादन डाउनटाइम कम हो जाता है।
- श्रमिकों को संभावित खतरों के बारे में चेतावनी देने के लिए हेलमेट और रिस्टबैंड में पहनने योग्य उपकरणों के साथ-साथ कंप्यूटर विज़न कैमरों का उपयोग किया जाता है।

रसद एवं परिवहन

- वाणिज्यिक और औद्योगिक IoT उपकरण इन्वेंट्री प्रबंधन, विक्रेता संबंध, फ्लीट प्रबंधन और निर्धारित रखरखाव सहित आपूर्ति श्रृंखला प्रबंधन में मदद कर सकते हैं।
- शिपिंग कंपनियाँ परिसंपत्तियों पर नज़र रखने और शिपिंग मार्गों पर ईंधन की खपत को अनुकूलित करने के लिए औद्योगिक IoT अनुप्रयोगों का उपयोग करती हैं।

1.3. IoT के लाभ

- वास्तविक समय संसाधन दृश्यता।
- लागत में कमी।
- परिचालन दक्षता में सुधार।
- त्वरित निर्णय लेने के लिए डेटा-संचालित अंतर्दृष्टि।
- शुरू से अंत तक, परिसंपत्तियों/संसाधनों की दूरस्थ निगरानी और प्रबंधन।
- वास्तविक समय, पूर्वानुमानित और अनुदेशात्मक अंतर्दृष्टि।
- अंतिम-ग्राहक अनुभव में सुधार।