UGC Approved Journal
© INNOVATIVE RESEARCH THOUGHTS | Refereed | Peer Reviewed | Indexed
ISSN : 2454 – 308X | Volume : 03 , Issue : 1 | January - March 2017

साइबर युद्ध और भारत की राष्ट्रीय सुरक्षा: उभरते खतरे और रणनीतिक जवाबी उपायों पर अध्ययन

डॉ दीप कुमार श्रीवास्तव

एसोसिएट प्रोफेसर, रक्षा अध्ययन विभाग
एसएम कॉलेज चंदौसी

सार

राष्ट्रीय बुनियादी ढांचे में डिजिटल प्रौद्योगिकियों के बढ़ते एकीकरण ने भारत के राष्ट्रीय सुरक्षा एजेंडे में साइबर सुरक्षा के महत्व को बढ़ा दिया है। यह शोध राज्य प्रायोजित साइबर हमलों, साइबर आतंकवाद, रैंसमवेयर, बौद्धिक संपदा की चोरी और दुष्प्रचार अभियानों पर ध्यान केंद्रित करते हुए साइबर युद्ध से उत्पन्न उभरते खतरों की पड़ताल करता है। विश्लेषण से इन खतरों की बहुमुखी प्रकृति का पता चलता है और मजबूत जवाबी उपायों को लागू करने की तात्कालिकता पर जोर दिया जाता है। प्रमुख सिफारिशों में साइबर बुनियादी ढांचे को मजबूत करना, एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति विकसित करना, साइबर खुफिया और निगरानी को बढ़ाना, सार्वजनिक-निजी भागीदारी को बढ़ावा देना, कानूनी और नियामक ढांचे को अद्यतन करना, साइबर सुरक्षा जागरूकता और प्रशिक्षण को बढ़ावा देना और अंतरराष्ट्रीय सहयोग में शामिल होना शामिल है। इन रणनीतियों को अपनाकर, भारत साइबर खतरों के उभरते परिदृश्य के खिलाफ अपनी राष्ट्रीय सुरक्षा को बेहतर ढंग से सुरक्षित रख सकता है।

मुख्य शब्द: साइबर युद्ध, भारत, राष्ट्रीय सुरक्षा, खतरे, रणनीतिक जवाबी उपाय इत्यादि।

प्रस्तावना

डिजिटल प्रौद्योगिकी की तीव्र प्रगति ने दुनिया भर के समाजों को बदल दिया है, जिससे आर्थिक विकास, नवाचार और कनेक्टिविटी के अभूतपूर्व अवसर उपलब्ध हुए हैं। हालाँकि, इस डिजिटल क्रांति ने विशेष रूप से राष्ट्रीय सुरक्षा के क्षेत्र में महत्वपूर्ण कमजोरियाँ भी पेश की हैं। जैसे-जैसे राष्ट्र डिजिटल बुनियादी ढांचे पर अधिक निर्भर होते जा रहे हैं, साइबर युद्ध का खतरा एक गंभीर चिंता के रूप में उभरा है। साइबर युद्ध में अक्सर रणनीतिक, राजनीतिक या सैन्य उद्देश्यों को प्राप्त करने के इरादे से कंप्यूटर सिस्टम, नेटवर्क या डेटा को बाधित करने, क्षति पहुंचाने या अनधिकृत पहुंच प्राप्त करने के लिए राज्य या गैर-राज्य अभिनेताओं द्वारा डिजिटल हमलों का उपयोग शामिल होता है।

तेजी से बढ़ती डिजिटल अर्थव्यवस्था वाले तेजी से विकासशील देश के रूप में भारत इन खतरों के प्रति विशेष रूप से संवेदनशील है। दक्षिण एशिया में देश की रणनीतिक स्थिति, पड़ोसी देशों के साथ इसके भू-राजनीतिक तनाव के साथ मिलकर, साइबर हमलों के प्रति इसकी संवेदनशीलता को और बढ़ा देती है। हाल की घटनाओं ने भारत के महत्वपूर्ण बुनियादी ढांचे, रक्षा प्रणालियों, वित्तीय संस्थानों और निजी क्षेत्र के उद्यमों को लक्षित करने वाले साइबर खतरों की बढ़ती जटिलता और आवृत्ति को उजागर किया

है। ये खतरे न केवल राष्ट्रीय सुरक्षा के लिए महत्वपूर्ण जोखिम पैदा करते हैं बल्कि जनता के विश्वास और आर्थिक स्थिरता को भी कमजोर करने की क्षमता रखते हैं।

इन चुनौतियों के जवाब में, भारत के लिए साइबर खतरों का मुकाबला करने के लिए व्यापक रणनीति विकसित करना और लागू करना अनिवार्य है। इस पेपर का उद्देश्य भारत की राष्ट्रीय सुरक्षा के लिए साइबर युद्ध से उत्पन्न उभरते खतरों का पता लगाना और प्रभावी जवाबी उपाय प्रस्तावित करना है। चर्चा में राज्य प्रायोजित हमलों, साइबर आतंकवाद, रैंसमवेयर, बौद्धिक संपदा की चोरी और दुष्प्रचार अभियान सहित विभिन्न प्रकार के साइबर खतरों को शामिल किया जाएगा। इसके अलावा, पेपर भारत के साइबर लचीलेपन को बढ़ाने के लिए रणनीतिक उपायों की रूपरेखा तैयार करेगा, जिसमें साइबर बुनियादी ढांचे को मजबूत करना, राष्ट्रीय साइबर सुरक्षा रणनीति तैयार करना, सार्वजनिक-निजी भागीदारी को बढ़ावा देना, कानूनी ढांचे को अद्यतन करना, साइबर सुरक्षा जागरूकता को बढ़ावा देना और अंतर्राष्ट्रीय सहयोग को बढ़ाना शामिल है।

उभरते खतरे

जैसे-जैसे भारत तेजी से डिजिटल होता जा रहा है, साइबर खतरों का परिदृश्य विकसित हो रहा है, जो राष्ट्रीय सुरक्षा के लिए नई चुनौतियाँ पेश कर रहा है। ये खतरे विविध और परिष्कृत हैं, विभिन्न क्षेत्रों को लक्षित करते हैं और महत्वपूर्ण बुनियादी ढांचे में कमजोरियों का फायदा उठाते हैं। यह खंड भारत में साइबर युद्ध से उत्पन्न प्राथमिक उभरते खतरों की पड़ताल करता है।

- **राज्य प्रायोजित साइबर हमले**

राज्य-प्रायोजित साइबर हमले राष्ट्रीय सुरक्षा के लिए सबसे महत्वपूर्ण खतरों में से एक हैं। ये हमले विदेशी सरकारों द्वारा रणनीतिक लाभ हासिल करने, महत्वपूर्ण सेवाओं को बाधित करने या संवेदनशील जानकारी चुराने के लिए किए जाते हैं। चीन और पाकिस्तान जैसे उल्लेखनीय विरोधियों को भारत के खिलाफ कई साइबर जासूसी गतिविधियों में फंसाया गया है। ये हमले अक्सर राष्ट्रीय सुरक्षा से समझौता करने और भू-राजनीतिक दबाव बढ़ाने के उद्देश्य से रक्षा प्रणालियों, पावर ग्रिड और संचार नेटवर्क को निशाना बनाते हैं।

- **गैर-राज्य अभिनेता और साइबर आतंकवाद**

आतंकवादी संगठनों और हैक्टिविस्ट समूहों सहित गैर-राज्य अभिनेताओं ने अपने एजेंडे को आगे बढ़ाने के लिए साइबर उपकरणों को तेजी से अपनाया है। साइबर आतंकवाद में व्यवधान, भय और नुकसान पैदा करने के लिए डिजिटल साधनों का उपयोग करना शामिल है, जो अक्सर प्रतीकात्मक संस्थाओं या महत्वपूर्ण बुनियादी ढांचे को लक्षित करता है। ये अभिनेता दूर से हमले कर सकते हैं, जिससे उनकी गतिविधियों का पता लगाना और उन्हें कम करना चुनौतीपूर्ण हो जाता है। साइबर आतंकवाद द्वारा

आवश्यक सेवाओं को बाधित करने और व्यापक दहशत पैदा करने की क्षमता राष्ट्रीय सुरक्षा के लिए इसके खतरे को रेखांकित करती है।

- **रैंसमवेयर और वित्तीय साइबर अपराध**

विश्व स्तर पर रैनसमवेयर हमलों में वृद्धि हुई है, भारत भी इसका अपवाद नहीं है। इन हमलों में, दुर्भावनापूर्ण सॉफ़्टवेयर पीड़ित के डेटा को एन्क्रिप्ट करता है, डिक्रिप्शन के लिए फिरौती के भुगतान की मांग करता है। इस तरह के हमलों ने सरकारी एजेंसियों और निजी उद्यमों दोनों को निशाना बनाया है, जिससे महत्वपूर्ण वित्तीय नुकसान और परिचालन व्यवधान हुआ है। धोखाधड़ी और डेटा उल्लंघनों सहित वित्तीय साइबर अपराध, डिजिटल वित्तीय प्रणालियों में आर्थिक स्थिरता और सार्वजनिक विश्वास को भी खतरे में डालते हैं।

- **बौद्धिक संपदा की चोरी और औद्योगिक जासूसी**

बौद्धिक संपदा (आईपी) की चोरी और औद्योगिक जासूसी भारत की आर्थिक और तकनीकी प्रगति को कमजोर करती है। साइबर अपराधी और राज्य अभिनेता अक्सर नवाचारों, व्यापार रहस्यों और मालिकाना प्रौद्योगिकियों को चुराने के लिए अनुसंधान संस्थानों, निगमों और स्टार्टअप को लक्षित करते हैं। ये गतिविधियाँ प्रतिस्पर्धात्मक लाभ को ख़त्म करती हैं, आर्थिक विकास में बाधा डालती हैं, और रक्षा, फार्मास्यूटिकल्स और सूचना प्रौद्योगिकी जैसे महत्वपूर्ण क्षेत्रों में राष्ट्रीय हितों से समझौता करती हैं।

- **दुष्प्रचार और मनोवैज्ञानिक संचालन**

साइबर चैनलों के माध्यम से चलाए गए दुष्प्रचार अभियान और मनोवैज्ञानिक ऑपरेशन राष्ट्रीय सुरक्षा के लिए एक सूक्ष्म लेकिन गहरा खतरा पैदा करते हैं। इन ऑपरेशनों का उद्देश्य जनता की राय को प्रभावित करना, व्यवहार में हेरफेर करना और समाज के भीतर कलह पैदा करना है। दुष्प्रचार झूठी सूचना फैलाकर और संस्थानों में जनता के विश्वास को कम करके, चुनाव जैसी लोकतांत्रिक प्रक्रियाओं में हस्तक्षेप कर सकता है। सोशल मीडिया के प्रसार ने इन अभियानों के प्रभाव को बढ़ा दिया है, जिससे वे सामाजिक एकजुटता और राजनीतिक स्थिरता बनाए रखने के लिए एक महत्वपूर्ण चिंता बन गए हैं।

- **आपूर्ति श्रृंखला कमजोरियाँ**

आपूर्ति श्रृंखलाओं को लक्षित करने वाले साइबर हमले एक उभरते खतरे का प्रतिनिधित्व करते हैं जिसका कई क्षेत्रों पर व्यापक प्रभाव पड़ सकता है। आपूर्ति श्रृंखला हमलों में लक्ष्य के नेटवर्क तक पहुंच प्राप्त करने के लिए तीसरे पक्ष के विक्रेताओं या सेवा प्रदाताओं से समझौता करना शामिल है। ये हमले महत्वपूर्ण आपूर्ति श्रृंखलाओं को बाधित कर सकते हैं, जिससे आवश्यक वस्तुओं और सेवाओं की कमी हो सकती है और राष्ट्रीय सुरक्षा के लिए महत्वपूर्ण जोखिम पैदा हो सकते हैं।

- **उभरती प्रौद्योगिकियां और एआई-संचालित खतरे**

कृत्रिम बुद्धिमत्ता (एआई) और इंटरनेट ऑफ थिंग्स (आईओटी) जैसी उभरती प्रौद्योगिकियों को तेजी से अपनाने से नई कमजोरियां सामने आती हैं। एआई-संचालित साइबर हमले पारंपरिक साइबर खतरों

को स्वचालित और बढ़ा सकते हैं, जिससे उनका पता लगाना और उनका प्रतिकार करना अधिक कठिन हो जाता है।

साइबर खतरों की विविध और विकसित होती प्रकृति के कारण राष्ट्रीय सुरक्षा के लिए एक सक्रिय और व्यापक दृष्टिकोण की आवश्यकता है। इन उभरते खतरों को समझकर, भारत अपने डिजिटल बुनियादी ढांचे की सुरक्षा और राष्ट्रीय सुरक्षा बनाए रखने के लिए लक्षित रणनीतियाँ विकसित कर सकता है।

जवाबी उपाय

साइबर युद्ध से उत्पन्न उभरते खतरों को प्रभावी ढंग से संबोधित करने के लिए, भारत को एक बहुआयामी दृष्टिकोण अपनाना चाहिए जिसमें अपने साइबर रक्षा तंत्र को बढ़ाना, रणनीतिक नीतियां तैयार करना, सहयोग को बढ़ावा देना और साइबर सुरक्षा जागरूकता को बढ़ावा देना शामिल है। यह खंड साइबर खतरों के खिलाफ भारत की राष्ट्रीय सुरक्षा की सुरक्षा के लिए आवश्यक प्रमुख उपायों की रूपरेखा तैयार करता है।

साइबर इंफ्रास्ट्रक्चर को मजबूत बनाना

एक मजबूत साइबर बुनियादी ढांचा राष्ट्रीय साइबर रक्षा की रीढ़ है। प्रमुख उपायों में शामिल हैं:

- **नियमित सुरक्षा ऑडिट**: कमजोरियों की पहचान करने और उन्हें दूर करने के लिए महत्वपूर्ण बुनियादी ढांचे का लगातार और गहन सुरक्षा ऑडिट करना।
- **सिस्टम अपडेट और पैच प्रबंधन**: यह सुनिश्चित करना कि ज्ञात कमजोरियों से बचाने के लिए सभी सिस्टम और सॉफ़्टवेयर नियमित रूप से अपडेट और पैच किए जाते हैं।
- **उन्नत एन्क्रिप्शन प्रथाएँ**: संवेदनशील डेटा को अनधिकृत पहुंच और साइबर जासूसी से बचाने के लिए मजबूत एन्क्रिप्शन प्रोटोकॉल लागू करना।
- **अतिरेक और असफल-सुरक्षित**: साइबर हमले की स्थिति में संचालन की निरंतरता सुनिश्चित करने के लिए महत्वपूर्ण प्रणालियों में अतिरेक का निर्माण और असफल-सुरक्षित की स्थापना।

राष्ट्रीय साइबर सुरक्षा रणनीति

साइबर खतरों पर समन्वित प्रतिक्रिया के लिए एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति विकसित करना आवश्यक है। इस रणनीति में शामिल होना चाहिए:

- **नीति ढाँचे**: घटना की रिपोर्टिंग और प्रबंधन के लिए प्रोटोकॉल सहित साइबर रक्षा, प्रतिक्रिया और पुनर्प्राप्ति के लिए स्पष्ट नीतियां स्थापित करना।
- **आक्रामक और रक्षात्मक उपाय**: विरोधियों को रोकने और राष्ट्रीय हितों की रक्षा के लिए रक्षात्मक उपायों के साथ आक्रामक क्षमताओं को संतुलित करना।
- **सभी क्षेत्रों में सहयोग**: सामूहिक विशेषज्ञता और संसाधनों का लाभ उठाने के लिए सरकारी एजेंसियों, निजी क्षेत्र और शिक्षा जगत के बीच सहयोग को बढ़ावा देना।

साइबर इंटेलिजेंस और निगरानी

सक्रिय खतरे का पता लगाने और प्रतिक्रिया के लिए साइबर खुफिया क्षमताओं को बढ़ाना महत्वपूर्ण है:

- **उन्नत निगरानी प्रणाली**: वास्तविक समय में विसंगतियों और संभावित खतरों का पता लगाने के लिए परिष्कृत निगरानी और निगरानी प्रणाली तैनात करना।
- **खतरे की खुफिया जानकारी साझा करना**: उभरते खतरों से आगे रहने के लिए सार्वजनिक और निजी क्षेत्रों के बीच खतरे की खुफिया जानकारी साझा करने की सुविधा प्रदान करना।
- **प्रोएक्टिव थ्रेट हंटिंग**: नुकसान पहुंचाने से पहले साइबर खतरों को सक्रिय रूप से खोजने और बेअसर करने के लिए समर्पित टीमों की स्थापना करना।

साइबर सुरक्षा जागरूकता और प्रशिक्षण

- साइबर सुरक्षा जागरूकता और प्रशिक्षण को बढ़ावा देने से कमजोरियाँ काफी हद तक कम हो सकती हैं:
- **जन जागरूकता अभियान**: आम साइबर खतरों और सुरक्षित ऑनलाइन प्रथाओं के बारे में जनता को शिक्षित करने के लिए अभियान शुरू करना।
- **व्यावसायिक प्रशिक्षण कार्यक्रम**: साइबर सुरक्षा पेशेवरों के कौशल और ज्ञान को बढ़ाने के लिए प्रशिक्षण कार्यक्रम विकसित करना।
- **शिक्षा में साइबर सुरक्षा को शामिल करना**: साइबर सुरक्षा में कुशल भविष्य के कार्यबल का निर्माण करने के लिए साइबर सुरक्षा शिक्षा को स्कूल पाठ्यक्रम में एकीकृत करना।

अंतरराष्ट्रीय सहयोग

साइबर खतरे वैश्विक प्रकृति के हैं, जिनके प्रभावी शमन के लिए अंतर्राष्ट्रीय सहयोग की आवश्यकता है:

- **अंतर्राष्ट्रीय संवादों में संलग्न होना**: साइबर सुरक्षा मुद्दों पर अंतर्राष्ट्रीय मंचों और संवादों में सक्रिय रूप से भाग लेना।
- **संधियाँ और समझौते**: साइबर सुरक्षा सहयोग और मानदंडों को बढ़ावा देने वाली अंतर्राष्ट्रीय संधियों और समझौतों पर बातचीत करना और उनका पालन करना।
- **संयुक्त साइबर रक्षा पहल**: संयुक्त साइबर रक्षा पहल और सूचना साझाकरण समझौतों पर अन्य देशों के साथ सहयोग करना।

साइबर खतरों के उभरते परिदृश्य में राष्ट्रीय सुरक्षा की सुरक्षा के लिए एक व्यापक और सक्रिय दृष्टिकोण की आवश्यकता है। इन जवाबी उपायों को लागू करके, भारत अपनी साइबर लचीलापन बढ़ा सकता है, महत्वपूर्ण बुनियादी ढांचे की रक्षा कर सकता है और उभरते साइबर खतरों के सामने राष्ट्रीय सुरक्षा बनाए रख सकता है। अगला भाग निष्कर्षों का सारांश देगा और भारत की भविष्य की सुरक्षा के लिए एक मजबूत साइबर रक्षा रणनीति के महत्व को रेखांकित करेगा।

निष्कर्ष

डिजिटल क्रांति ने विकास और नवाचार के लिए अपार अवसर प्रदान करते हुए, विशेष रूप से राष्ट्रीय सुरक्षा के क्षेत्र में महत्वपूर्ण कमजोरियां भी पेश की हैं। साइबर युद्ध एक जटिल और उभरते खतरे का प्रतिनिधित्व करता है जो भारत के महत्वपूर्ण बुनियादी ढांचे, आर्थिक स्थिरता और सार्वजनिक सुरक्षा के लिए गंभीर जोखिम पैदा करता है। राज्य-प्रायोजित साइबर हमलों, गैर-राज्य अभिनेताओं, रैंसमवेयर, बौद्धिक संपदा की चोरी और दुष्प्रचार अभियानों के खतरे मजबूत साइबर रक्षा तंत्र की तत्काल आवश्यकता को रेखांकित करते हैं। इन चुनौतियों पर भारत की प्रतिक्रिया व्यापक और बहुआयामी होनी चाहिए। कमजोरियों को कम करने के लिए नियमित ऑडिट, अपडेट और उन्नत एन्क्रिप्शन प्रथाओं के माध्यम से साइबर बुनियादी ढांचे को मजबूत करना आवश्यक है। एक अच्छी तरह से परिभाषित राष्ट्रीय साइबर सुरक्षा रणनीति जिसमें आक्रामक और रक्षात्मक दोनों उपाय शामिल हैं, समन्वित कार्रवाई के लिए एक रूपरेखा प्रदान कर सकती है। साइबर इंटेलिजेंस और निगरानी क्षमताओं को बढ़ाने से सक्रिय खतरे का पता लगाने और प्रतिक्रिया करने में मदद मिलेगी, जबकि सार्वजनिक-निजी भागीदारी को बढ़ावा देने से विभिन्न क्षेत्रों की सामूहिक विशेषज्ञता और संसाधनों का लाभ उठाया जा सकता है।

सन्दर्भ ग्रन्थ सूची

1. क्लार्क, आर.ए., और नैक, आर.के. (2010)। साइबर युद्ध: राष्ट्रीय सुरक्षा के लिए अगला ख़तरा और इसके बारे में क्या करें। हार्परकोलिन्स।
2. गीयर्स, के. (2011)। सामरिक साइबर सुरक्षा. नाटो सहकारी साइबर रक्षा उत्कृष्टता केंद्र।
3. हैथवे, एम.ई., और क्लिम्बर्ग, ए. (2012)। साइबर तत्परता सूचकांक 1.0. नीति अध्ययन के लिए पोटोमैक संस्थान।
4. क्षेत्री, एन. (2013)। ग्लोबल साउथ में साइबर अपराध और साइबर सुरक्षा। पालग्रेव मैकमिलन.
5. लुईस, जे.ए. (2012)। साइबर सुरक्षा और साइबर युद्ध: हर किसी को क्या जानना आवश्यक है। ऑक्सफोर्ड यूनिवरसिटि प्रेस।
6. लिबिकी, एम.सी. (2009)। साइबरनिरोध और साइबरयुद्ध। रैंड कॉर्पोरेशन।
7. टिक, ई., कास्का, के., और विहुल, एल. (2010)। अंतर्राष्ट्रीय साइबर घटनाएँ: कानूनी विचार। सहकारी साइबर रक्षा उत्कृष्टता केंद्र।