Sampreshan
UGC CARE GROUP 1 **ISSN:2347-2979**
https://sampreshan.info/

Vol. 17, Issue No. 2, June 2024

सायबर युद्ध आणि भारताची राष्ट्रीय सुरक्षा: नवे आव्हान

प्रा. डॉ. दिनेश दयाराम माळी, विभाग प्रमुख - संरक्षण व सामरिक शास्त्र विभाग, कै. श्रीमती विमलबाई उत्तमराव पाटील कला आणि कै. डॉ. बी. एस. देसले विज्ञान महाविद्यालय, साक्री ता. साक्री, जि. धुळे

सारांश

सायबर युद्ध हा आधुनिक काळातील राष्ट्रीय सुरक्षेसमोरील सर्वात मोठ्या आव्हानांपैकी एक आहे. डिजिटल क्रांतीमुळे जगभरातील देश सायबर अवलंबित्वाकडे वाटचाल करत आहेत, मात्र त्याचबरोबर सायबर हल्ल्यांचा धोका प्रचंड वाढला आहे. भारतासारख्या विकसित होत असलेल्या देशासाठी हे आव्हान अधिक गंभीर बनले आहे. सायबर हल्ल्यांचे अनेक प्रकार आहेत, जसे की **सायबर हल्ले, DDoS हल्ले, मालवेअर आणि व्हायरस हल्ले, तसेच सामाजिक अभियांत्रिकी हल्ले.** सायबर हल्ल्यांद्वारे सरकारी यंत्रणा, बँकिंग क्षेत्र, संरक्षण विभाग, आणि इतर महत्त्वाच्या संस्था लक्ष्य केल्या जातात. उदाहरणार्थ, मालवेअर आणि व्हायरस हल्ल्यांमुळे संगणक प्रणाली निष्क्रिय होऊ शकते किंवा संवेदनशील डेटा चोरीला जाऊ शकतो. DDoS हल्ल्यांमुळे महत्त्वाच्या वेबसाइट्स किंवा ऑनलाइन सेवांवर भार टाकून त्या बंद पाडल्या जातात.

सामाजिक अभियांत्रिकी (Social Engineering) हा आणखी एक महत्त्वाचा सायबर धोका आहे, ज्यामध्ये हल्लेखोर लोकांचा विश्वास संपादन करून संवेदनशील माहिती मिळवतात. फिशिंग, व्हिशिंग आणि इतर फसवणुकीच्या पद्धतींमधून अनेक संस्थांना मोठे आर्थिक आणि सुरक्षा नुकसान झाले आहे. भारत सरकारने **"राष्ट्रीय सायबर सुरक्षा धोरण",** डिजिटल संरक्षा उपाय, आणि **संरक्षण व्यवस्थेमध्ये आत्मनिर्भरता** निर्माण करण्यावर भर दिला आहे. तथापि, प्रगत सायबर धोके टाळण्यासाठी **सायबर सुरक्षा उपायांची सुधारणा, तंत्रज्ञानावर आधारित मजबूत संरक्षण, आणि जनजागृती मोहिमा** राबवण्याची नितांत गरज आहे. सायबर युद्धाचा धोका टाळण्यासाठी भारताने आपल्या सुरक्षा यंत्रणेला अधिक सक्षम करणे आवश्यक आहे.

मुख्य संबोध: सायबर युद्ध, राष्ट्रीय सुरक्षा, सायबर सुरक्षा, सायबर हल्ले, भारताची सुरक्षा धोरण, डिजिटल इन्फ्रास्ट्रक्चर, सायबर धोके व जागतिक सहकार्य इ.

प्रस्तावना

वर्तमान काळातील युग डिजिटल क्रांतीचे आहे. इंटरनेट आणि तंत्रज्ञानाच्या झपाट्याने होणाऱ्या वृद्धीमुळे समाज, सरकार आणि अर्थव्यवस्थेच्या सर्व बाबी डिजिटल होत आहेत. परंतु, त्याचप्रमाणे तंत्रज्ञानाच्या या विकासामुळे सायबर सुरक्षा आणि सायबर युद्ध यासारखी नवीन आव्हानेदेखील उभी राहिली आहेत. सायबर युद्ध हे एक नवे प्रकारचे युद्ध आहे, जे परंपरागत युद्ध पद्धतींपेक्षा वेगळे आहे. त्यात शस्त्रास्त्रांची आवश्यकता नाही, पण ते इंटरनेटद्वारे विविध तंत्रज्ञानाचा उपयोग करून पारंपारिक युद्धाचे स्वरूप बदलवते. सायबर हल्ल्यांद्वारे परदेशी राष्ट्रे, आतंकी गट, किंवा सायबर गुन्हेगार राष्ट्रीय सुरक्षेला मोठा धोका निर्माण करू शकतात. भारतासाठी ही एक मोठी आव्हाने आहे, कारण आपल्या देशाची डिजिटल इन्फ्रास्ट्रक्चर, सरकारी पद्धती, आर्थिक प्रणाली आणि सैन्य यांचा मोठा भाग आता डिजिटल बनला आहे. म्हणूनच, भारतासाठी सायबर युद्ध आणि सायबर सुरक्षा एक महत्त्वाचे आणि आवश्यक प्रश्न बनले आहेत.

Sampreshan
UGC CARE GROUP 1 ISSN:2347-2979
https://sampreshan.info/
Vol. 17, Issue No. 2, June 2024

उद्दिष्टे

1. सायबर युद्धाची परिभाषा आणि त्याचे महत्त्व समजून घेणे.
2. सायबर युद्धाच्या स्वरूपातील नवे धोके ओळखणे आणि त्यांचा मुकाबला कसा करावा.
3. भारतातील सायबर सुरक्षा पद्धती आणि त्याची स्थिती विश्लेषित करणे.
4. सायबर युद्धाच्या संदर्भात भारताने घेतलेले धोरण आणि उपाय.
5. भविष्यातील सायबर युद्धाच्या आव्हानांना कशाप्रकारे सामोरे जावे, याबाबत धोरणाची आखणी करणे.
6. सायबर युद्धाच्या संदर्भातील जागतिक सहकार्य आणि त्याची महत्त्वता.

सायबर युद्धाचे स्वरूप

सायबर युद्ध हा एक अत्याधुनिक तंत्रज्ञानावर आधारित युद्ध प्रकार आहे, ज्यामध्ये शस्त्रास्त्रांचे वापर न करता, सायबर हल्ल्यांद्वारे विरोधकाला धोका दिला जातो. हे हल्ले इंटरनेटच्या माध्यमातून संगणक प्रणाली, नेटवर्क, डिव्हाइस, डेटा आणि डिजिटल इन्फ्रास्ट्रक्चरवर केली जातात. सायबर युद्धामध्ये विविध साधनांचा वापर केला जातो जसे की:

1. सायबर हल्ले: संगणक प्रणालीवर हल्ला करणे, ज्याद्वारे डेटा चोरी, सिस्टम क्रॅश करणे, किंवा इन्फ्रास्ट्रक्चरमध्ये गडबड निर्माण करणे. सायबर हल्ले हे संगणक प्रणाली किंवा नेटवर्कवर विविध प्रकारे हल्ला करण्याचे उपाय आहेत, ज्यामुळे विविध प्रकारे नुकसान होऊ शकते. हल्ला करणारे लोक किंवा गट संगणक प्रणालीवरील डेटा चोरी करू शकतात, सिस्टिममध्ये गडबड निर्माण करू शकतात, किंवा त्या प्रणालीच्या कार्यप्रणालीमध्ये विघ्न आणू शकतात.

डेटा चोरी: हॅकर्स विविध उपकरणे आणि सॉफ्टवेअरचा वापर करून संवेदनशील माहिती किंवा डेटा चोरू शकतात. उदाहरणार्थ, बँक खात्यांचे तपशील, व्यक्तिगत माहिती, किंवा व्यापारिक गुप्त माहिती.

सिस्टम क्रॅश करणे: हॅकर्स केवळ डेटा चोरी करण्यावर लक्ष केंद्रित करत नाहीत, तर ते सिस्टम क्रॅश करण्यासाठी किंवा त्यांच्या कार्यक्षमतेला थांबवण्यासाठी विशेष हल्ले तयार करू शकतात. यामुळे, कंपनी किंवा सरकारी प्रणालीचे संपूर्ण इन्फ्रास्ट्रक्चर ठप्प होऊ शकते.

इन्फ्रास्ट्रक्चरमध्ये गडबड निर्माण करणे: अनेक सायबर हल्ले इन्फ्रास्ट्रक्चर किंवा सर्व्हरला लक्ष्य करतात, ज्या ठिकाणी नेटवर्क किंवा संगणक प्रणाली जोडले जातात. हल्ला करणारे सायबर अपराधी डेटा सेंटरमध्ये प्रवेश करून, मुख्य प्रणाली थांबवू शकतात.

सायबर हल्ल्यांमुळे आर्थिक नुकसान, माहितीची चोरी, गुप्त माहिती उघड होणे, आणि कंपनीच्या इन्फ्रास्ट्रक्चरमध्ये महत्त्वाचे बदल घडवून आणले जाऊ शकतात.

2. डिस्ट्रिब्युटेड डिनायल-ऑफ-सर्व्हिस (DDoS) हल्ले: इंटरनेट सेवेवर लोड टाकून ती सेवा अस्थिर किंवा थांबवणे. DDoS हल्ले हे एक अत्यंत प्रभावी सायबर हल्ल्याचे प्रकार आहेत, ज्यामध्ये हल्लेखोर असंख्य संगणक किंवा नेटवर्क संसाधने एकाच वेळी इंटरनेट सेवा किंवा वेबसाइटवर पाठवतात. हल्ल्याचा उद्देश ही सेवा अस्थिर किंवा पूर्णपणे थांबवणे असतो.

हल्ल्याची कार्यप्रणाली: DDoS हल्ल्यांमध्ये, हल्लेखोर विविध प्रकारच्या संगणकांना नियंत्रणात घेतात, जे "झोम्बी संगणक" म्हणून ओळखले जातात. हे संगणक एकाच वेळी वेगवेगळ्या पॅकेट्स किंवा डेटा ओळख करून सर्व्हरवर पाठवतात. यामुळे सर्व्हरवरील ट्रॅफिक वधारणारी असंख्य विनंत्या होतात, आणि यामुळे इंटरनेट सेवा अचानक थांबते किंवा तोट्यात जाते.

आर्थिक परिणाम: DDoS हल्ल्यांमुळे इंटरनेट सेवा बंद होऊन किंवा मंद होऊन आर्थिक नुकसानीचा सामना करावा लागतो. ऑनलाइन व्यवसाय, बँकिंग सेवांमध्ये अडचणी येऊ शकतात, आणि यामुळे ग्राहकांची विश्वासार्हता कमी होऊ शकते.

हल्ल्याची इन्फ्रास्ट्रक्चरवरील परिणाम: या प्रकारच्या हल्ल्यांमुळे सामान्यत: जास्त ट्रॅफिकसाठी संसाधने संपुष्टात येतात. तसेच, मुख्य प्रणालीवर हल्ला होऊन व्यवसायाच्या ऑपरेशन्समध्ये गंभीर विघटन होऊ शकते.

3. मालवेअर आणि व्हायरस हल्ले: सायबर हल्ल्यांचा वापर करून संगणक प्रणाली किंवा डेटा चोरी करणे. मालवेअर आणि व्हायरस हल्ले हे सायबर हल्ल्यांचे अत्यंत सामान्य आणि धोकादायक प्रकार आहेत. मालवेअर किंवा व्हायरस हे असे सॉफ्टवेअर असतात, जे आपोआप संगणक किंवा नेटवर्कमध्ये प्रवेश करतात आणि त्याचे कार्य किंवा डेटा हल्लेखोरांच्या नियंत्रणात आणतात.

मालवेअर: मालवेअर म्हणजे "मालिशियस सॉफ्टवेअर" (Malicious Software). यामध्ये विविध प्रकारचा हल्ला समाविष्ट असतो, ज्यामध्ये ट्रोजन हॉर्सेस, रॅन्समवेयर, स्पायवेअर आणि कीलॉगरसारख्या सॉफ्टवेअरचा समावेश होतो. ट्रोजन हॉर्स एक हानिकारक सॉफ्टवेअर आहे जे एका सामान्य प्रोग्रॅमच्या रूपात लपवले जाते आणि त्याद्वारे हल्लेखोर प्रणालीवर नियंत्रण मिळवतो.

रॅन्समवेयर हल्ले: रॅन्समवेयर हल्ल्यांमध्ये हॅकर्स संगणक डेटा लॉक करून ठेवतात आणि त्याचे अनलॉक करण्यासाठी भरपाईची मागणी करतात. यामुळे, कंपन्या किंवा व्यक्ती मोठ्या प्रमाणात आर्थिक नुकसान करतात.

व्हायरस: व्हायरस हे सायबर हल्ल्यांच्या पारंपरिक प्रकारांपैकी एक आहेत. ते संगणक प्रणाली किंवा नेटवर्कमध्ये प्रवेश करून त्यांना प्रदूषित करतात. व्हायरस संगणकावर एकाधिक कामे करू शकतात, जसे की माहिती चोरी करणे, डेटा नष्ट करणे, किंवा सिस्टम क्रॅश करणे.

मालवेअर आणि व्हायरस हल्ल्यांमुळे कंपन्या आणि व्यक्तींना भारी वित्तीय नुकसान होऊ शकते. आणि यामुळे अनेक गोपनीय डेटा चोरीला जाऊ शकतो, ज्यामुळे गोपनीयता आणि सुरक्षा उल्लंघन होतात.

4. सामाजिक अभियांत्रिकी: लोकांचा विश्वास जिंकून संवेदनशील माहिती मिळवणे. सामाजिक अभियांत्रिकी हल्ले हे सायबर हल्ल्यांचे एक अत्यंत प्रभावी, परंतु भ्रामक साधन आहेत. यामध्ये हल्लेखोर लोकांना विश्वासात घेऊन संवेदनशील माहिती मिळवण्यासाठी विविध मनोवैज्ञानिक आणि धोरणात्मक तंत्रांचा वापर करतात.

फिशिंग हल्ले: फिशिंग हल्ल्यात, हल्लेखोर एखाद्या विश्वसनीय संस्थेचा किंवा व्यक्तीचा समान असलेला ईमेल किंवा संदेश तयार करतात आणि त्या माध्यमातून वापरकर्त्यांकडून संवेदनशील माहिती गोळा करतात. उदाहरणार्थ, बँक अकाउंट तपशील, पासवर्ड, किंवा क्रेडिट कार्ड माहिती.

प्रिस्किंग आणि व्हिशिंग: प्रिस्किंगमध्ये फोन कॉलद्वारे लोकांकडून माहिती मिळवली जाते, तर व्हिशिंग मध्ये व्हॉइस फोन कॉलद्वारे माहिती मिळवली जाते. हल्लेखोर व्यक्तीला खात्री देण्यासाठी त्या पद्धती वापरतात.

कन्सार टॅक्टिक्स: कधी कधी, हल्लेखोर कर्मचारी, संबंधित लोक, किंवा ग्राहकांना आपली माहिती देण्यासाठी दबाव आणतात, त्यांना मार्गदर्शन करत किंवा लहान फायद्यांची ऑफर देत.

सामाजिक अभियांत्रिकीचा मुख्य उद्देश लोकांना धोका देणे आणि त्यांच्याकडून संवेदनशील माहिती मिळवणे असतो, ज्याचा वापर पुढे सायबर हल्ल्यांसाठी केला जातो. सायबर हल्ले हे एक महत्त्वाचे आणि वेगाने वाढणारे धोका आहेत. प्रत्येक प्रकारच्या सायबर हल्ल्याने विशिष्ट धोके निर्माण केले आहेत आणि त्यांच्यावर लक्ष ठेवणे आवश्यक आहे. यासाठी सायबर सुरक्षा उपायांची अंमलबजावणी करणे आणि वापरकर्त्यांना सजग ठेवणे आवश्यक आहे, जेणेकरून सायबर हल्ल्यांपासून आपला डेटा आणि सुरक्षा संरक्षित राहील.

भारतासाठी सायबर युद्धाचे महत्त्व

भारत एक डिजिटल युगातील प्रमुख देश आहे. भारत सरकार अनेक डिजिटल पद्धती वापरत आहे ज्या नागरिकांच्या दैनंदिन जीवनाचा एक महत्त्वाचा भाग आहेत. यामध्ये डिजिटल पेमेंट, ऑनलाइन शिक्षा, सरकारच्या योजनांचा वापर, आणि सैन्याच्या डिजिटल तंत्रज्ञानाचा समावेश आहे. यामुळे, सायबर हल्ल्यांचा धोका अधिक वाढला आहे. सायबर युद्धात भारतासाठी काही महत्त्वाचे धोके समोर येतात:

1. **आंतरराष्ट्रीय वाद**: भारतावर सायबर हल्ले परदेशी राष्ट्रांकडून होऊ शकतात, ज्यामुळे राष्ट्रीय सुरक्षा धोक्यात येऊ शकते.
2. **आतंकी गट**: विविध दहशतवादी संघटनांनी सायबर हल्ले करून, नागरिकांचा डेटा चोरी करू शकतो किंवा देशाच्या अर्थव्यवस्थेला मोठा फटका देऊ शकतो.
3. **सायबर स्पायिंग**: विविध देशांच्या गुप्तचर संस्थांकडून सायबर हल्ले करून भारताची संवेदनशील माहिती चोरी केली जाऊ शकते.

भारताचे सायबर सुरक्षा धोरण

भारत सरकारने सायबर सुरक्षा धोरण आणि उपायांची आखणी केली आहे, ज्या अंतर्गत विविध कार्यप्रणाली विकसित केल्या आहेत:

1. **राष्ट्रीय सायबर सुरक्षा धोरण**: भारत सरकारने 2013 मध्ये राष्ट्रीय सायबर सुरक्षा धोरण (National Cyber Security Policy) घोषित केले. याचा मुख्य उद्देश सायबर हल्ल्यांपासून भारतीय इंटरनेट इन्फ्रास्ट्रक्चरचे संरक्षण करणे आहे.
2. **भारतीय संगणक आपत्ती प्रतिसाद यंत्रणा (CERT-In)**: हा भारत सरकारचा एक महत्त्वाचा यंत्रणा आहे, जी सायबर हल्ल्यांचा वेगाने प्रतिसाद देते आणि संरक्षण उपाययोजना करते.
3. **राष्ट्रीय सायबर सुरक्षा संस्थान (NICSI)**: हे संस्थान सायबर सुरक्षा धोरणांची अंमलबजावणी आणि सायबर क्षेत्रातील तज्ञांना प्रशिक्षित करते.
4. **संपूर्ण डिजिटल प्रणालीचे संरक्षण**: सरकार डिजिटल पेमेंट, ऑनलाइन डेटा संरक्षण, आणि इन्क्रिप्शन धोरणांचा अवलंब करत आहे.

Sampreshan
UGC CARE GROUP 1 ISSN:2347-2979
https://sampreshan.info/
Vol. 17, Issue No. 2, June 2024

सायबर युद्ध आणि राष्ट्रीय सुरक्षा

1. **सायबर युद्धाचे आधुनिक स्वरूप** : सायबर युद्ध परंपरागत युद्धापेक्षा वेगळं आहे. यामध्ये लष्करी हल्ले, हवाई हल्ले किंवा भूमिगत युद्धाची आवश्यकता नाही. परंतु सायबर हल्ल्यांद्वारे सरकारी प्रणाली, बँकिंग प्रणाली, आणि इतर महत्त्वाच्या सर्व्हिसेसमधून माहिती चोरणे, सेवा खंडित करणे, आणि नागरिकांचे नुकसान करणे शक्य आहे.
2. **सायबर हल्ल्यांमध्ये सॉफ्टवेअरचा वापर**: सायबर हल्ले साधारणतः सॉफ्टवेअर, व्हायरस, आणि मालवेअरच्या माध्यमातून केले जातात. या सॉफ्टवेअरने सरकारी आणि आस्थापनांच्या महत्त्वपूर्ण डेटाला धोका पोहोचवू शकतो.
3. **भारताच्या सायबर सुरक्षा सुधारणा** : भारत सरकार सायबर सुरक्षा आणि डिजिटल प्रणालीचे संरक्षण करण्यासाठी दरवर्षी नवीन धोरणे लागू करत आहे. भारतातील सुरक्षा एजन्सी आणि बडे बँक्स सायबर हल्ल्यांना त्वरित प्रतिसाद देण्यासाठी मजबूत यंत्रणा तयार करत आहेत.
4. **आंतरराष्ट्रीय सहकार्य** : सायबर युद्धाच्या आव्हानाला सामोरे जाण्यासाठी जागतिक सहकार्य महत्त्वाचे आहे. भारताने अनेक देशांसोबत सायबर सुरक्षा आणि डिजिटल धोरणावर करार केले आहेत.
5. **हॅकिंग आणि डिजिटल आपत्तीचे वाढते प्रमाण** : हॅकर्स, दहशतवादी गट, आणि आंतरराष्ट्रीय राज्ये यांचा सायबर हल्ल्यांमधील सहभाग वाढला आहे. यामुळे सायबर सुरक्षा उपाय वाढवले जात आहेत.
6. **सायबर युद्धाची भविष्यातील तंत्रज्ञानात्मक रूपरेषा** : भविष्यात सायबर हल्ल्यांच्या स्वरूपात नवे तंत्रज्ञान लागू होईल. आर्टिफिशियल इंटेलिजन्स, ब्लॉकचेन तंत्रज्ञान आणि क्वांटम कम्प्युटिंगचा वापर सायबर युद्धाच्या पद्धती बदलू शकतो.
7. **संपूर्ण डिजिटल तंत्रज्ञानाचे सामर्थ्य** : सायबर हल्ले जेव्हा पारंपारिक सैन्याने करणे शक्य नसते, तेव्हा ते डिजिटल पद्धतींवर आधारित असतात. भविष्यात सायबर युद्धाच्या किमती आणि प्रभावाचे मूल्यांकन तंत्रज्ञानाच्या दृष्टिकोनातून होईल.

निष्कर्ष

सायबर युद्ध हा एक अत्याधुनिक आणि डिजिटल युगातील नवा धोका आहे. भारतासाठी याचा धोका वाढत आहे, कारण देशाच्या डिजिटल इन्फ्रास्ट्रक्चरच्या वाढीमुळे त्यावर हल्ले करणे अधिक सोपे झाले आहे. भारताने सायबर सुरक्षा आणि सायबर युद्धाबाबत गंभीर पावले उचलली आहेत. सायबर हल्ल्यांचा प्रतिसाद वेगाने दिला जातो आणि यासाठी राष्ट्रीय सायबर सुरक्षा धोरण, विविध सुरक्षा यंत्रणा, आणि जागतिक सहकार्य महत्त्वाचे ठरते. भारताने सायबर सुरक्षा क्षेत्रात भविष्याच्या आव्हानांसाठी तयार रहाणे आवश्यक आहे.

संदर्भ

1. आचार्य, डी. (२०१८). सायबर सुरक्षा आणि भारताची राष्ट्रीय सुरक्षा. *भारतीय सुरक्षा अभ्यास* (१६), ५२-६८.
2. शर्मा, एस. (२०१९). सायबर युद्ध: नवा युद्धप्रकार. *राष्ट्रीय संरक्षण व अभ्यास* (२३), ४५-६१.

3. जोशी, पी. (२०२०). सायबर हल्ले आणि सुरक्षा धोरण. *भारत: सायबर सुरक्षा आणि धोक्यांचे विश्लेषण* (३४), १०१-११५.
4. गायकवाड, पी. (2021). **सायबर सुरक्षा आणि भारताच्या संरक्षण धोरणाचा विकास.** पुणे: राजहंस प्रकाशन.
5. देशमुख, आर. (2020). **डिजिटल भारत आणि सायबर गुन्हेगारी.** मुंबई: साकेत प्रकाशन.
6. कुलकर्णी, ए. (2019). **सायबर क्राईम आणि कायदे.** नागपूर: लोकवाङ्मय गृह.
7. जोशी, एस. (2018). **भारतातील सायबर सुरक्षा: संधी आणि आव्हाने.** औरंगाबाद: शीतल पब्लिकेशन्स.
8. शर्मा, आर. (2020). **भारत में साइबर सुरक्षा: एक अध्ययन.** नई दिल्ली: प्रभात प्रकाशन.
9. मिश्रा, वी. (2019). **साइबर अपराध और डिजिटल सुरक्षा.** वाराणसी: भारतीय विद्या प्रकाशन.
10. Singh, R. (2021). *Cyber Security and National Defense: India's Perspective*. New Delhi: Oxford University Press.