ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

साइबर आतंकवाद और भारतीय सुरक्षा

डॉ. राम अवतार राम

एसोशिएट प्रोफेसर - रक्षा एवं स्त्रातेजिक अध्ययन विभाग, का. सु. साकेत स्नातकोत्तर महाविद्यालय , अयोध्या

सारांश

साइबर अपराध एक ऐसा अपराध है जिस में कंप्यूटर और नेटवर्क शामिल है। किसी भी कंप्यूटर का अपराधिक स्थान पर मिलना या कंप्यूटर से कोई अपराध करना कंप्यूटर अपराध कहलाता है। कंप्यूटर अपराध मे नेटवर्क शामिल नही होता है। किसी कि निजी जानकारी को प्राप्त करना और उसका गलत इस्तेमाल करना। किसी की भी निजी जानकारी कंप्यूटर से निकाल लेना या चोरी कर लेना भी साइबर अपराध है।

कंप्यूटर अपराध भी कई प्रकार से किये जाते है जैसे कि जानकारी चोरी करना, जानकारी मिटाना, जानकारी मे फेर बदल करना, किसी कि जानकारी को किसी और को देना या कंप्यूटर के भागो को चोरी करना या नष्ट करना। साइबर अपराध भी कई प्रकार के है जैसे कि स्पैम ईमेल, हैकिंग, फिशिंग, वायरस को डालना, किसी की जानकारी को ऑनलाइन प्राप्त करना या किसी पर हर वक़्त नजर रखना।

- राष्ट्रीय साइबर थ्रेट विश्लेषण यूनिट (TAU)
- राष्ट्रीय साइबर क्राइम रिपोर्टिंग
- संयुक्त साइबर क्राइम जांच टीम के लिए प्लेटफार्म
- राष्ट्रीय साइबर क्राइम फोरेन्सिक प्रयोगशाला (NCFL) पारिस्थितिकी
- राष्ट्रीय साइबर क्राइम प्रशिक्षण केन्द्र (NCTC)
- साइबर क्राइम पारिस्थितिकी प्रबंधन यूनिट
- राष्ट्रीय साइबर अनुसंधान एवं नवोन्मेषण केन्द्र

परिचय

कंप्यूटर अपराध के प्रकार

- जानकारी चोरी करना- किसी के भी कंप्यूटर से उसकी निजी जानकारी निकालना जेसे की उपयोगकर्ता नाम या पासवर्ड।
- जानकारी मिटाना- किसी के कंप्यूटर से जानकारी मिटाना ताकी उसे नुकसान हो या कोई जरूरी जानकारी को मिटाना।

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

- फेर बदल करना- जानकारी मे कुछ हटाना या जोड़ना उस जानकारी को बदल देना।
- बहारी नुकसान- भागो को नष्ट करना, उसे तोडना या भागो की चोरी करना भी कंप्यूटर अपराध मे आता है।[1,2]

साइबर अपराध के प्रकार

- स्पैम ईमेल- अनेक प्रकार के ईमेल आते है जिसमें एसे ईमेल भी होते है जो सिर्फ कंप्यूटर को नुकसान पहुचाते है। उन ईमेल से सारे कंप्यूटर में खराबी आ जाती हैं।

- हैकिंग- किसी की भी निजी जानकारी को हैक करना जेसे की उपयोगकर्ता नाम या पासवर्ड और फिर उसमे फेर बदल करना।

साइबरफिशिंग- किसी के पास स्पैम ईमेल भेजना ताकी वो अपनी निजी जानकारी दे और उस जानकारी से उसका नुकसान हो सके। यह इमेल आकार्षित होते है।

- वायरस फैलाना -साइबर अपराधी कुछ ऐसे सॉफ्टवेयर आपके कम्प्युटर पर भेजते हैं जिसमें वायरस छिपे हो सकते हैं, इनमें वायरस, वर्म, टार्जन हॉर्स, लॉजिक हॉर्स आदि वायरस शामिल हैं, यह आपके कंप्यूटर को काफी हानि पहुॅचा सकते हैं।

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

- सॉफ्टवेयर पाइरेसी - सॉफ्टवेयर की नकल तैयार कर सस्ते दामों में बेचना भी साइबर क्राइम के अन्तर्गत आता है, इससे साफ्टवेयर कम्पनियों को भारी नुकसान उठाना पड़ता है साथ ही साथ आपके कीमती उपकरण भी ठीक से काम नहीं करते हैं।

- फर्जी बैंक कॉल- आपको जाली ईमेल, मैसेज या फोन कॉल प्राप्त हो जो आपकी बैंक जैसा लगे जिसमें आपसे पूछा जाये कि आपके एटीएम नंबर और पासवर्ड की आवश्यकता है और यदि आपके द्वारा यह जानकारी नहीं दी गयी तो आपको खाता बन्द कर दिया जायेगा या इस लिंक पर सूचना दें। याद रखें किसी भी बैंक द्वारा ऐसी जानकारी कभी भी इस तरह से नहीं मॉगी जाती है और भूलकर भी अपनी किसी भी इस प्रकार की जानकारी को इन्टरनेट या फोनकॉल या मैसेज के माध्यम से नहीं बताये। [3,4]

- सोशल नेटवर्किग साइटों पर अफवाह फैलाना - बहुत से लोग सोशल नेटवर्किग साइटों पर सामाजिक, वैचारिक, धार्मिक और राजनैतिक अफवाह फैलाने का काम करते हैं, लेकिन यूजर्स उनके इरादें समझ नहीं पाते हैं और जाने-अनजाने में ऐसे लिंक्स को शेयर करते रहते हैं, लेकिन यह भी साइबर अपराध और साइबर-आतंकवाद की श्रेणी में आता है।

- साइबर बुलिंग - फेसबुक जैसी सोशल नेटवर्किंग पर अशोभनीय कमेंट करना, इंटरनेट पर धमकियॉ देना किसी का इस स्तर तक मजाक बनाना कि तंग हो जाये, इंटरनेट पर दूसरों के सामने शर्मिंदा करना, इसे साइबर बुलिंग कहते हैं। अक्सर बच्चे इसका शिकार हाेते हैं। इससे इनके सेहत पर भी असर पडता है

विचार – विमर्श

आई4सी को वर्ष 2018 में सीआईएस प्रभाग के तहत केंद्रीय स्तर पर समन्वय और साइबर अपराधों के खिलाफ लड़ाई में एक सामान्य रूपरेखा प्रदान करके राज्यों / केंद्र शासित प्रदेशों को आवश्यक सहयोग देने के लिए एक एजेंसी के रूप में स्थापित किया गया था।

आई4सी आम जनता को समय-समय पर साइबर सुरक्षा युक्तियां प्रदान करके 'साइबर दोस्त' के नाम से विभिन्न सोशल मीडिया हैंडल के माध्यम से जन जागरूकता बढ़ा रहा है।

साइबर क्राइम के विरुद्ध लड़ने में नोडल बिंदु के रूप में कार्य करना

एलईए की अनुसंधान समस्याओं/जरूरतों की पहचना करना और भारत एवं विदेश में शैक्षणिक अनुसंधान संस्थाओं के सहयोग से नई प्रौद्योगिकियां और फोरेन्सिक उपकरण विकसित करने में आर एंड डी कार्यकलाप शुरू करना

यह योजना 415.86 करोड़ रुपये के परिव्यय के साथ प्रस्तावित है और दो वर्ष तक चलती रहेगी

अतिवादियों और आंतकवादियो की गतिविधियों को रोकने के लिए साइबर स्पेस के दुरुपयोग को रोकना[5,6]

तेजी से बदलती हुई प्रौद्योगिकी और अन्तराष्ट्रीय सहयोग के साथ कदम मिलाकर चलने के लिए साइबर कानूनों में यथापेक्षित संशोधनों का सुझाव देने

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

गृह मंत्रालय में संबंधित नोडल प्राधिकारी के परामर्श से साइबर क्राइम से संबंधित अन्य देशों के साथ हुई पारस्परिक विधिक सहायता संधि (एमएलएटी) के कार्यान्वयन से संबंधित सभी गतिविधियों का समन्वय करना

साइबर अपराधियों ने 12 मई 2017 को ब्रिटेन जैसे विकसित देश की विशाल राष्ट्रीय स्वास्थ्य-सेवा (Cyber attack on United Kingdom's National Health Service) पर साइबर हमला करके चंद मिनट में उसकी चूलें हिला दीं थीं. ऐसे हमलों से बचने के लिए भारत सरकार दिन-रात जुटी है.

परिणाम

साइबर अपराधियों ने 12 मई 2017 को ब्रिटेन जैसे विकसित देश की विशाल राष्ट्रीय स्वास्थ्य-सेवा (Cyber attack on United Kingdom's National Health Service) पर साइबर हमला करके चंद मिनट में उसकी चूलें हिला दीं थीं. उस हमले से स्कॉटलैंड की स्वास्थ्य सेवाएं तहस-नहस हो गई थीं. ऐसे हमलों से बचने के लिए भारत सरकार दिन-रात जुटी है. हिंदुस्तानी हुकूमत भी ब्रिटेन में हुए उस जैसे घातक साइबर हमले से बचने के हर-संभव उपाय तलाश कर उन्हें अमल में लाने की कोशिशों में जुटी है.

इन्हीं कोशिशों के तहत केंद्रीय गृह मंत्रालय द्वारा तलाशा गया अचूक फार्मूला है 'आई4सी'. साइबर अपराधियों के एक्टिव होते ही उन्हें दबोच लेने के लिए. या अगर देश में यह साइबर अपराधी कहीं किसी वारदात को अंजाम दे भी दें तो, उन्हें तुरंत कानूनी शिकंजे में जकड़ा जा सके. केंद्रीय गृह मंत्रालय के उच्च पदस्थ सूत्रों की बात मानें तो, अब तक देश में मौजूद साइबर अपराधी खुद को सबसे ज्यादा शातिर और सरकारी मशीनरी को खुद के सामने बाहियाद मान रहे थे. लिहाजा इन अपराधियों को शुरू में ही पकड़ कर साइबर अपराधों पर लगाम लगाया जाना जरूरी था. इसी के चलते हाल-फिलहाल केंद्रीय गृह मंत्रालय ने 'आई4सी' फार्मूला तलाशा है.

'आई4सी' फार्मूले का पूरा नाम Indian Cyber Crime Co-ordination Centre है. इस फार्मूले की निगरानी और उसे गंभीरता से अमल में लाने की जिम्मेदारी भी हिंदुस्तान की हुकूमत ने केंद्रीय गृह मंत्रालय को ही सौंपी है. क्योंकि आई4सी फार्मूले की रुपरेखा (ब्लूप्रिंट) या इसकी परिकल्पना भी केंद्रीय गृह मंत्रालय की अपनी ही थी. देश के कोने-कोने में साइबर ठगों द्वारा आए दिन अंजाम दी जा रही 'ऑनलाइन-ठगी' की इन घटनाओं और साइबर अपराधियों को काबू करने में आई4सी फार्मूले के बेहद कामयाब साबित होने की उम्मीद है. साइबर अपराधियों से निपटने के लिए बने इस फार्मूले की खासियत है कि, इस पर अमल की जिम्मेदारी किसी व्यक्ति-विशेष या फिर राज्य विशेष अथवा किसी राज्य विशेष की किसी एजेंसी-विशेष को जिम्मेदारी नहीं दी गई है. साइबर अपराधियों को नेस्तनाबूद करने के लिए बनाए गए इस फार्मूले को अमल में लाने की जिम्मेदारी सामूहिक होगी. और यह सब संभव होगा Joint Cyber Crime Co-ordination Team (JCCT) के प्रयासों से. इन तमाम तथ्यों में से कई की पुष्टि शुक्रवार को उत्तराखण्ड राज्य के पुलिस महानिदेशक और देश के वरिष्ठ आईपीएस अधिकारी अशोक कुमार ने भी की. उत्तराखण्ड राज्य पुलिस महानिदेशक (Director General of Police Uttarakhand) के मुताबिक, "आई4सी फार्मूले को अमल में लाने के लिए दिन-रात युद्धस्तर पर काम जारी है. इस फार्मूले का बेहतरीन इस्तेमाल जल्दी से जल्दी कैसे किया जाए? इस पर मंत्रणा के लिए देश भर में Joint Cyber Crime Co-ordination Team (JCCT) मीटिंग्स/संयुक्त सम्मेलन चल रहे हैं."[7,8]

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

निष्कर्ष

यदि कोई देश की एकता, अखंडता, सुरक्षा या संप्रभुता को खतरा पहुंचाने के उद्देश्य से या लोगों में आतंक फैलाने के उद्देश्य से किसी कंप्यूटर सिस्टम को प्रभावित करता है, जैसे- कंप्यूटर सिस्टम पर जबरदस्ती कब्जा करना, उससे छेड़छाड़ करना, या उसे बिगाड़ना, और यह सब करते समय उसके कारण किसी की मृत्यु हो जाती है या हो सकती है, चोट लगती है, संपत्ति को नुकसान होता है, या आवश्यक जन सेवाओं को बाधा पहुंचती है तो उस व्यक्ति को साइबर आतंक आपराधिक माना जाएगा। यह अपराध देश में अशांति, अराजकता फैला कर किसी दूसरे देश या विदेशी गुट को लाभ पहुंचाने के लिए किया जाता है। ऐसा अपराध करने का षड्यंत्र भी अपराध है।[9,10]

संदर्भ

1) Alexander, Yonah Swetman, Michael S. (2001). Cyber Terrorism and Information Warfare: Threats and Responses. Transnational Publishers Inc.,U.S. आई°ऍस°बी°ऍन° 1-57105-225-9.
2) Colarik, Andrew M. (2006). Cyber Terrorism: Political and Economic Implications. Idea Group, U.S. आई°ऍस°बी°ऍन° 1-59904-022-0.
3) Verton, Dan (2003). Black Ice: The Invisible Threat of Cyber-terrorism. Osborne/McGraw-Hill, U.S. आई°ऍस°बी°ऍन° 0-07-222787-7.
4) Weimann, Gabriel (2006). Terror on the Internet: The New Arena, the New Challenges. United States Institute of Peace, U.S. आई°ऍस°बी°ऍन° 1-929223-71-4.
5) जॉन ब्लू, (2004 नवंबर) "साइबर टेरर के खिलाफ लड़ाई" नेटवर्कवर्ल्ड. 20 मार्च 2005 को वर्ल्ड वाइड वेब: https://web.archive.org/web/20041206204738/http://www.nwfusion.com/supp/2004/cybercrime/112904terror.html से पुनः प्राप्त
6) ग्रोस, ग्रांट (2003 नवंबर) "पिछले कीड़ों के मुकाबले साइबर हमले और अधिक परिष्कृत हैं, विशेषज्ञ कहते हैं। 17 मार्च 2005 को वर्ल्ड वाइड वेब: https://web.archive.org/web/20080315071926/http://www.computerworld.com/securitytopics/security/story/0,10801,86857,00.html से पुनः प्राप्त.
7) केविन पौल्सन, (अगस्त 2004) "दक्षिण ध्रुव 'साइबरआतंकवादी' हैक पहला नहीं था" सिक्युरिटीफोकस न्यूज़. 17 मार्च 2005 को वर्ल्ड वाइड वेब: https://web.archive.org/web/20110610224229/http://www.securityfocus.com/news/9356 से पुनः प्राप्त.
8) सिडरिक थेवेनेट, (नवम्बर 2005) "Cyberterrorisme, mythe ou réalité?". https://web.archive.org/web/20110716094802/http://www.terrorisme.net/pdf/2006_Thevenet.pdf: वर्ल्ड वाइड वेब से
9) अमेरिकी सेना साइबर संचालन और साइबर आतंकवाद पुस्तिका 1.02
10) Jacqueline Ching (2010). Cyberterrorism. Rosen Pub Group. आई°ऍस°बी°ऍन° 1435885325.