AL-QALAM القلم

ISSN 2071-8683 e-ISSN 2707-0077

Volume 25, Issue, 2, 2020

Published by Institute of Islamic Studies,
University of the Punjab, Lahore, Pakistan.

سائبر کرائمز کا تعارف، تاریخ، خطرات و نقصانات اور چیلنجز

Introduction, history, dangers and challenges of cyber crimes

***Hafiz Samiullah**

****Dr. Muhammad Hammad Lakhvi**

* PhD Scholar, Department of Islamic Studies, Punjab University, Lahore, Pakistan, Lecturer in Islamic Studies, Government Post Graduate College, Sahiwal

**Dean Faculty of Islamic Studies, Punjab University, Lahore, Pakistan

Abstract

With the invention of the Internet, the world has become a universal village as the Internet has brought people from all over the world closer together. While modern technology, cyberspace, and the Internet are a great source of blessing and development for human civilization, there are many opportunities for criminals to commit crimes. Those who use information technology for negative purposes are called cybercriminals and all criminal activities, committed by the computer; the Internet, cyberspace and the World Wide Web are called cybercrimes. The first recorded cybercrime occurred in 1820 (1). Cybercriminals freed from geographical boundaries can commit their crimes from anywhere in the world. Today, cybercriminals have access to various systems of the countries of the world, including security, defense, communications, education, economic and ground and air transportation, and they also have access to the private information of individuals and the entire record of various institutions. At present, the world faces technical, legal, operational and general challenges regarding cybercrimes both domestically and internationally. This article explains: What are cybercrimes? When did they start? What are the types of cybercrime? Who are the cybercriminals and what are their goals? What are the risks and challenges of cybercrime?

سائبر کرائمز کا تعارف:

"سائبر ورلڈ" ایک ایسی دنیا ہے جہاں آن لائن ہو کر لوگ بغیر کسی مخصوص سرحد کے پوری دنیا دیکھ سکتے

ہیں، جس سے چاہے بات کر سکتے ہیں، ایک دوسرے کے ساتھ تبادلہ خیال کر سکتے ہیں، معلومات دے اور لے سکتے ہیں، کاروبار کر سکتے ہیں، رقوم کی منتقلی کر سکتے ہیں اور اس کے علاوہ کسی جگہ جائے بغیر گھر بیٹھے ہی بہت ساری سہولیات سے مستفید ہو سکتے ہیں۔ لیکن تصویر کا دوسرا رخ یہ ہے کہ موجودہ دور میں جدید ٹیکنالوجی، سائبر سپیس اور انٹرنیٹ جہاں انسانی تہذیب کے لئے ایک بہت بڑی نعمت اور ترقی کا ذریعہ ہیں وہاں ان میں تخریب کارانہ ذہن کے حامل لوگوں کے لئے جرائم کا ارتکاب کرنے کے لئے بہت سارے مواقع بھی موجود ہیں۔ موجودہ دور میں سائبر کرائم ایسے عفریت کی شکل اختیار کر چکا ہے جس کے لئے جغرافیائی سرحدیں کوئی معنی نہیں رکھتیں یہی وجہ ہے کہ سائبر کریمینلز دنیا میں کہیں بھی بیٹھ کر اپنے جرائم کا ارتکاب کر سکتے ہیں۔

سائبر کرائم دو انگریزی الفاظ "سائبر" اور "کرائم" کا مرکب ہے جن کی الگ الگ وضاحت مختلف انگریزی ڈکشنریوں کے اعتبار سے مندرجہ ذیل ہے:

سائبر:

کیمبرج ڈکشنری میں "سائبر" کی وضاحت ان الفاظ میں کی گئی ہے: کمپیوٹر خصوصاً انٹرنیٹ سے منسلک ہونا یا ان کا استعمال کرنا۔(2) ویبسٹر ڈکشنری میں سائبر کو یوں بیان کیا گیا ہے: کمپیوٹرز یا کمپیوٹر نیٹ ورکس سے منسلک ہونا۔(3) آکسفورڈ ڈکشنری کے مطابق سائبر سے مراد: برقی کمیونیکیشن نیٹ ورکس اور قیاسی حقیقت سے منسلک ہونا ہے۔(4)

کرائم:

کرائم سے مراد ایسا غیر قانونی کام ہے جس کے لئے کوئی شخص حکومت کی طرف سے سزا دیا جا سکتا ہو۔(5)

سائبر کرائم:

سائبر کرائم کی بطور اصطلاح مختلف تعریفات کی گئی ہیں جن میں سے چند ایک مندرجہ ذیل ہیں:

سائبر کرائم سے مراد ایسی تمام مجرمانہ سرگرمیاں ہیں جن کا ارتکاب کمپیوٹر، انٹرنیٹ، سائبر سپیس اور ورلڈ وائڈ ویب کے ذریعے کیا جاتا ہے۔(6) سائبر کرائم سے مراد ایسے غیر قانونی کام ہیں جن میں کمپیوٹر یا تو ایک آلہ ہوتا ہے، یا ہدف ہوتا ہے یا آلہ اور ہدف دونوں ہوتا ہے۔(7) کوئی بھی ایسی مجرمانہ سرگرمی جو کمپیوٹر کو ایک آلے، ہدف یا مزید جرائم کے ارتکاب میں ایک ذریعے کے طور پر استعمال کرے، وہ سرگرمی سائبر کرائم کے

دائرے میں آتی ہے۔(8)ایسے جرائم جن کا ارتکاب جدید ٹیلی کمیونیکیشن نیٹ ورکس جیسا کہ انٹرنیٹ اور موبائل فونز(وغیرہ) کا استعمال کرتے ہوئے مجرمانہ ارادے کے ساتھ افراد یا افراد کے گروہوں کے خلاف کیا جاتا ہے تاکہ نشانہ بننے والے کی ساکھ کو بالارادہ نقصان پہنچایا جائے، یا اسے جسمانی یا ذہنی نقصان پہنچایا جائے، یا اسے بلا واسطہ یا بالواسطہ خسارے میں ڈالا جائے۔(9) سائبر کرائم سے مراد ایسا جرم ہے جو ایک کمپیوٹر اور ایک نیٹ ورک پے مشتمل ہوتا ہے۔(10)

مذکورہ بالا تعریفات کی روشنی میں سائبر کرائم کو آسان الفاظ میں اسطرح بیان کیا جاسکتا ہے: سائبر کرائم سے مراد ایسا جرم ہے جس کا ارتکاب کمپیوٹر اور انٹرنیٹ کا استعمال کرتے ہوئے کیا جاتا ہے۔ یہاں یہ بات سمجھنی ضروری ہے کہ سائبر کرائم کی تعریف میں کمپیوٹر کی جو اصطلاح استعمال ہوئی ہے اس سے مراد مروجہ ڈیسک ٹاپ یا لیپ ٹاپ کمپیوٹر ہی نہیں ہے بلکہ اس اصطلاح کے ضمن میں پرسنل ڈیجیٹل اسسٹنس(PDA)، سیل فونز، پیچیدہ گھڑیاں اور مشینوں کی ایک بڑی تعداد آتی ہے۔(11)

سائبر کرائم کے مترادفات:

سائبر کرائم کے مترادف کمپیوٹر کرائم، انٹرنیٹ کرائم، ای کرائم، ڈیجیٹل کرائم، ہائی ٹیک کرائم، آن لائن کرائم ، الیکٹرانک کرائم اورانفارمیشن ٹیکنالوجی کرائم کی اصطلاحات بھی استعمال کی جاتی ہیں البتہ سائبر کرائم کی اصطلاح موجودہ دور میں ذیادہ مستعمل ہے۔

سائبر کرائم سائبر ورلڈ کی ایک جدید اور پیچیدہ اصطلاح ہے جس کے خطرات نے دنیا کو تیزی سے اپنی لپیٹ میں لے لیا ہے۔ سائبر کرائم، کمپیوٹر کرائم، انفارمیشن ٹیکنالوجی کرائم اور ہائی ٹیک کرائم کی اصطلاحات جرائم کی اقسام میں سے دو بڑی اقسام کو ظاہر کرنے کے لئے عام طور پے ایک دوسری کی جگہ استعمال کی جاتی ہیں۔ پہلی قسم کے جرم میں نشانہ کمپیوٹر ہوتا ہے جس میں اس کے نیٹ ورک کے اخفاء، سالمیت اور دستیابی کے اوپر حملہ کیا جاتا ہے۔ دوسری قسم روایتی جرائم پر مشتمل ہے(جیسا کہ چوری، فراڈ اور جعلسازی وغیرہ) جن کا ارتکاب کمپیوٹر کی مدد، کمپیوٹر کے ذریعے، کمپیوٹر نیٹ ورک اور متعلقہ معلوماتی اور مواصلاتی ٹیکنالوجی کی مدد سے کیا جاتا ہے۔(12)

سائبر کرائمز کی تاریخ:

1820ء میں جوزف میری جیکوارڈ، جو کہ فرانس کا ایک ٹیکسٹائل مینوفیکچرر تھا، نے ایک لوم بنائی۔ یہ ایک ایسی مشین تھی جس نے خاص کپڑا بننے کے مراحل کے تسلسل کو دہرانا ممکن بنا دیا (یہ لوم ڈیزائن کو محفوظ بھی کر سکتی تھی)۔ اس لوم کی وجہ سے جیکوارڈ کے ملازم خوفزدہ ہو گئے کہ ان کا روزگار خطرے میں پڑ گیا ہے، لہذا انہوں نے جیکوارڈ کو مزید نئی ٹیکنالوجی کے استعمال سے روکنے کے لئے تخریب کاری کی اور مشین کو توڑ دیا۔ یہ پہلا سائبر کرائم ہے جسے ریکارڈ کیا گیا۔(13)

آسٹریلین انسٹیٹیوٹ آف کریمنالوجی نے سائبر کرائم ریسرچ کے نام سے کی گئی اپنی تحقیق میں سائبر کرائم کی مختلف اقسام کو ان کے وقوع پذیر ہونے کی زمانی ترتیب کے اعتبار سے اس طرح بیان کیا ہے:

کسی چیز کو وقوع پذیر ہونے سے روکنا (Interception):	1867
منظم جرائم (Organized Crime):	1920
کمپیوٹر نیٹ ورک کو غیر قانونی طور پر توڑنا (Phreaking):	1961
ٹیلی مارکیٹنگ فراڈ (Telemarketing Scam):	1965
کسی دوسرے کے کمپیوٹر میں غیر قانونی رسائی (Computer Hacking):	1970
کریپر وائرس (Creeper Virus):	1971
ڈینیئل آف سروس (Denial of Service):	1980
بالجبر رشوت ستانی (Extortion):	1980
دھوکے سے رقوم کی منتقلی (Funds Transfer Fraud):	1985
اے۔ ٹی۔ ایم فراڈ (A.T.M Fraud):	1985
بچوں کا استحصال (Child Exploitation):	1990
کمپیوٹر کا ایسا مجموعہ جسے وائرس زدہ پروگرام سے کنٹرول کیا جائے (Botnets):	1993
انٹرنیٹ پر کسی دوسرے کے کام یا خیالات کی چوری (Online Piracy):	1995

کسی کی شناخت سے منسلک جرائم(Identity Crime):	1995
کسی کو اس کی مرضی کے بغیر ای۔ میل بھیجنا(Spam):	1995
کمپیوٹر اور انٹرنیٹ کا استعمال کرتے ہوئے دہشت گردانہ حملہ(Cyber terrorism attack):	1997
انٹرنیٹ پر کسی کو ہراساں(Cyber Stalking):	1998
کسی کی نجی معلومات حاصل کرنے کیلئے کسی اصل ویب پیج کی نقل بنانا(Phishing):	2002
ایم۔کامرس اٹیک (M-commerce Attacks):	2006
وائرلیس عدم تحفظ (Wireless vulnerabilities):	2007
کلاوَڈ کمپیوٹنگ خطرات (Cloud Computing): (14)	2009

سائبر کرائمز کی تقسیم:

کمپیوٹر اور انٹرنیٹ پر ہونے والے جرائم کئی شکلیں اختیار کرتے ہیں جنہیں سائبر کرائم کی مختلف اقسام کہا جاتا ہے۔ ذیل میں ان مختلف اقسام کی وضاحت کی جاتی ہے:

(الف) نشانہ بننے والوں کے اعتبار سے سائبر کرائمز کی اقسام: سائبر کرائمز کا نشانہ بننے والوں کے اعتبار سے سائبر کرائمز کی مندرجہ ذیل اقسام ہیں:

1۔افراد کے خلاف ہونے والے سائبر کرائمز: ان کو آگے مزید دو اقسام میں بانٹا جا سکتا ہے:

I. شخص یا اشخاص سے متعلقہ جرائم

II. شخص یا اشخاص کی ملکیت سے متعلقہ جرائم

شخص یا اشخاص سے متعلقہ جرائم: ان سے مراد وہ جرائم ہیں جو کسی فرد کی شخصیت کو متاثر کریں یا اسے براہ راست نقصان پہنچائیں۔ اس قسم کے تحت مندرجہ ذیل جرائم آتے ہیں:

کمپیوٹر سسٹم تک غیر قانونی رسائی (Unauthorized access over computer system)

فحش مواد کا پھیلاؤ (Dissemination of obscene material)

سائبر سٹالکنگ (کمپیوٹر اور انٹرنیٹ کے ذریعے کسی کو ہراساں کرنا) (Cyber Stalking)

غیر مہذب تشہیر (Indecent Exposure)

ای۔ میل کے ذریعے ہراساں کرنا(E-mail Harassment)

رسوائی یابدنامی (Defamation)

دھوکا اور فراڈ (Cheating and Fraud)

ای۔ میل کے ذریعے دھوکا دینا (E-mail Spoofing)(15)

شخص یا اشخاص کی ملکیت سے متعلقہ جرائم: ان سے مراد وہ جرائم ہیں جو افراد کی ملکیت کو متاثر کرتے ہیں۔ اس قسم کے تحت مندرجہ ذیل جرائم آتے ہیں:

کمپیوٹر کی بربادی اور غارتگری (Computer Vandalism)

وائرس بھیجنا (Transmitting Virus)

نیٹ میں مداخلت (Net Trespass)

کمپیوٹر سسٹم پر غیر قانونی قبضہ یا رسائی (Unauthorized Access/Control over Computer system)

ایجادات اور خیالات کی ملکیت سے منسلک جرائم (Intellectual Property Crimes)

انٹرنیٹ کے وقت کی چوری (Internet Time Theft)(16)

2۔ حکومتوں یا تنظیموں کے خلاف ہونے والے سائبر کرائمز:

کچھ مخصوص جرائم ایسے ہیں جنکا ارتکاب مختلف گروہوں نے انٹرنیٹ کی سہولیات کا استعمال کرتے ہوئے عالمی سطح پر حکومتوں، کمپنیوں اور افراد کے گروہوں کو دھمکانے اور خوفزدہ کرنے کے لئے کیا ہے۔ ایسے سائبر کرائمز تنظیموں کے خلاف سائبر کرائمز شمار ہوتے ہیں۔اس قسم کے تحت مندرجہ ذیل جرائم آتے ہیں:

سائبر ٹیررازم (Cyber Terrorism)

غیر قانونی معلومات پر قبضہ (Possession of Unauthorized information)

کمپیوٹر سسٹم پر غیر قانونی کنٹرول (Unauthorized control over computer system)

پائریٹڈ سافٹ ویئرز کی تقسیم (Distribution of pirated softwares)

کمپیوٹر کی بربادی اور غارتگری (Computer Vandalism)

وائرس (Virus)

نیٹ میں مداخلت (Net Trespass)

ایجادات اور خیالات کی ملکیت سے منسلک جرائم (Intellectual Property Crimes)

سائبر تھیفٹ (کمپیوٹر سسٹم سے معلومات وغیرہ کی چوری) (Cyber Theft)(17)

صنعتی جاسوسی (Industrial Espionage)

3۔ معاشرے کے خلاف ہونے والے سائبر کرائمز:

ایسے جرائم جو بڑے پیمانے پر معاشرے کے مفادات پر اثر ڈالیں، معاشرے کے خلاف سائبر کرائمز کے طور پر جانے جاتے ہیں۔ اس قسم کے تحت مندرجہ ذیل جرائم آتے ہیں:

سائبر پورنوگرافی (انٹرنیٹ پر تحریری، تصویری، فلمی فحش نگاری) (Cyber Pornography)

آن لائن گیمبلنگ (انٹرنیٹ پر جوا کھیلنا) (Online Gambling)

فنانشل سائبر کرائمز (مالی سائبر کرائمز) (Financial cybercrimes)

سائبر ٹریفکنگ (غیر قانونی طور پے اشیاء کا لین دین) (Cyber Trafficking)

سائبر جعلسازی (انٹرنیٹ پر جعلسازی کرنا) (Cyber Forgery)

بے حیائی کی تشہیر سے نوجوانوں کو خراب کرنا (Polluting the Youth through indecent exposure)

غیر قانونی اشیاء کی خرید و فروخت (Sale of illegal article)(18)

(ب) کمپیوٹر کے کردار کے حوالے سائبر کرائمز کی تقسیم:

کمپیوٹر کے کردار کے حوالے سے سائبر کرائمز کی مندرجہ ذیل اقسام ہیں:

1۔ ایسے سائبر کرائمز جن کے ارتکاب میں کمپیوٹر ایک آلہ ہوتا ہے: سائبر کرائمز کی اس قسم میں جرم کا ارتکاب کرنے کیلئے کمپیوٹر ایک آلے کے طور پر استعمال ہوتا ہے۔ کمپیوٹر کے پروگراموں کو دوسروں کو دھوکا دینے کیلئے غلط انداز میں پیش کیا جاتا ہے۔ اس قسم کے تحت مندرجہ ذیل جرائم آتے ہیں:

i- اے۔ٹی۔ ایم کارڈز اور اکاؤنٹس کا دھوکے پر مبنی استعمال

ii- کریڈٹ کارڈ فراڈ

iii- الیکٹرانک فنڈز ٹرانسفر فراڈ

iv- ای کامرس فراڈ

v- ٹیلی کمیونیکیشن فراڈ

vi- سٹاک ٹرانسفر فراڈ(19)

2۔ ایسے سائبر کرائمز جن کے ارتکاب میں کمپیوٹر ہدف ہوتا ہے: اس قسم کے سائبر کرائمز کا ارتکاب مخصوص سائبر کریمینلز ہی کرتے ہیں کیونکہ اس قسم کے جرائم، ان جرائم کی نسبت جن میں کمپیوٹر ایک آلہ ہوتا ہے، زیادہ تکنیکی علم کا تقاضا کرتے ہیں۔ اس قسم کے جرائم کا بڑا مقصد کمپیوٹر سسٹم کو نقصان پہنچانا ہوتا ہے یا اس اہم ڈیٹا تک رسائی حاصل کرنا یا اسے چوری کرنا ہوتا ہے جو کمپیوٹر میں محفوظ ہو۔ اس قسم کے تحت مندرجہ ذیل جرائم آتے ہیں:

i- کمپیوٹر اور کمپیوٹر سسٹم یا کمپیوٹر نیٹ ورکس کی تخریب کاری

ii- ڈیٹا اور معلومات کی چوری

iii- ایجادات اور خیالات کی ملکیت کی چوری جیسا کہ کمپیوٹر سافٹ ویئر کی چوری

iv- قابل فروخت معلومات کی چوری

v- ایسی بلیک میلنگ (افشائے راز کی دھمکی دے کر مال وغیرہ لینا) جو کمپیوٹر فائلوں سے حاصل شدہ معلومات پر مبنی ہو جیسا کہ طبی معلومات، ذاتی معلومات، جنسی ترجیحات اور مالی ڈیٹا وغیرہ۔

vi- کریمینل جسٹس اور حکومتی ریکارڈ تک غیر قانونی رسائی

(ج) ایسے سائبر کرائمز جن کے ارتکاب میں کمپیوٹرز کا کردار کم ہوتا ہے: سائبر کرائمز کی اس تقسیم میں جرم کا ارتکاب کرنے میں کمپیوٹر کا کردار کم ہوتا ہے۔ اس کی مزید دو اقسام ہیں:

1۔ انٹرنیٹ کرائم

2۔ ویب کی بنیاد پر ہونے والے جرائم

انٹرنیٹ کرائم: انٹرنیٹ کرائمز ایسے جرائم پر مشتمل ہیں جو انٹرنیٹ انفراسٹرکچر کا مجرمانہ استعمال کرتے ہیں اور ان جرائم میں مندرجہ ذیل جرائم شامل ہیں:

i- ہیکنگ (معلومات کی چوری، پاس ورڈز کی چوری، کریڈٹ کارڈز نمبرز کی چوری، وائرس زدہ پروگرام لانچ کرنا)

ii- جاسوسی

iii- سپیمنگ (غیر مطلوبہ ای۔میلز بھیجنا)

ویب کی بنیاد پر ہونے والے جرائم: ویب کی بنیاد پر ہونے والے جرائم کو مزید چار اقسام میں بانٹا گیا ہے:

i- ویب سائٹ سے منسلک جرائم

- دھوکہ دہی
- انشورینس فراڈ
- جوا
- فحش نگاری کی تقسیم
- پائریٹڈ سافٹ ویئرز کی فروخت

ii- ای۔میل کے ذریعے جرائم

- دھمکیاں
- بالجبر رشوت ستانی
- ساکھ خراب کرنا
- وائرس زدہ پروگرام لانچ کرنا

iii- یوز نیٹ(20) سے منسلک جرائم

- فحش مواد کی تقسیم و فروخت
- پائریٹڈ سافٹ ویئرز کی تقسیم و فروخت
- ہیکنگ کے طریقوں پر تبادلہ خیال کرنا

- چوری شدہ کریڈٹ کارڈز کے نمبروں کی فروخت
- چوری شدہ ڈیٹا کی فروخت

iv- انٹرنیٹ ری لے (relay) چیٹ کرائم

سائبر سٹالکنگ وغیرہ (21)

(د) سائبر کریمینلز کے حوالے سے سائبر کرائمز کی اقسام: سائبر کرائمز کا ارتکاب عام طور پر کئی طرح کے لوگوں کی طرف کی سے کیا جاتا ہے۔ سائبر کریمینلز فرد یا افراد بھی ہوسکتے ہیں، گروہ بھی ہوسکتے ہیں اور ریاستیں یا پھر حکومتیں بھی ہوسکتی ہیں جیسا کہ طالبعلم، شوقین کمپیوٹر پروگرامر، کاروباری مخالفین اور دہشت گرد اور منظم مجرم گروہ کے اراکین۔ مجرمین کی عمریں 10 سال سے 60 سال تک ہوسکتی ہیں اور ان کی مہارتیں ایک نوآموز سے لیکر ایک پیشہ ورتک کی ہوسکتی ہیں۔(22) سائبر کریمینلز کو تین بنیادی اقسام میں تقسیم کیا جاسکتا ہے:

1۔ ہیکرز اور فریکس (ٹیلیفون ہیکرز)

2۔ معلومات کے سوداگر اور زرخرید

3۔ دہشت گرد، انتہا پسند اور راہ سے بھٹکے ہوئے

1۔ ہیکرز اور فریکس (ٹیلیفون ہیکرز): کمپیوٹر ہیکرز اور فریکس کھوج، معلومات اور تجسس کے مقاصد کے پیش نظر غیر قانونی طور پہ کمپیوٹر سسٹم میں داخل ہونے کیلئے انفارمیشن ٹیکنالوجی کا استعمال کرتے ہیں۔ ان کے جرم اگرچہ غیر قانونی ہوتے ہیں مگر عموما ان سے ان کا ارادہ ڈیٹا کو نقصان پہنچانے یا مالی مفاد کے حصول کا نہیں ہوتا۔ اکثر ہیکرز اور فریکس شرارتیں کرتے ہیں جیسا کہ فون کالز کا پتہ بدلنا یا ویب پیجز کو دوبارہ ترتیب دے دینا۔ اگرچہ ان کے افعال سے افراد، تنظیموں یا صنعتوں کو مالی نقصان ہوتا ہو مگر ان کا بنیادی مقصد اپنے جرائم سے فائدہ اٹھانا نہیں ہوتا۔

2۔ معلومات کے سوداگر اور زرخرید: ہیکرز کے برخلاف معلومات کے سوداگر اور زرخرید مجرمین معلومات کی خرید و فروخت کا کاروبار کرتے ہیں۔ یہ لوگ جن جرائم میں ملوث ہوتے ہیں ان میں کاروباری جماعتوں کی جاسوسی اور تخریب کاری، شناخت کی معلومات کی فروخت اور چوری، کمپیوٹر اور نیٹ ورکس میں نقب زنی اور بڑے پیمانے پر سافٹ ویئر پائریسی شامل ہیں۔ اگرچہ یہ لوگ بھی اسی طرح کے آلات اور تکنیکیں استعمال کریں جسطرح کے

ہیکرز استعمال کرتے ہیں مگر ان کا بنیادی مقصد فائدہ اٹھانا ہوتا ہے۔ وہ لوگ جو معلومات کے حصول اور فروخت میں ملوث ہوتے ہیں، اکثر مقابلے میں ہونے والی کاروباری جماعتوں کی طرف سے کرائے پر لئے گئے ہوتے ہیں، یا پھر وہ خود ان کمپنیوں اور ایجنسیوں کے سابقہ ملازم ہوتے ہیں جن سے وہ معلومات حاصل کرتے ہیں۔

3۔ دہشت گرد، انتہا پسند اور منحرف: سائبر کریمینلز کے تیسرے گروپ میں وہ لوگ شامل ہیں جو سائبر سپیس کو غیر قانونی، سیاسی یا سماجی سرگرمی کے لئے استعمال کرتے ہیں۔ پہلی دو اقسام کے سائبر مجرمین کے مقابلے میں اس قسم کے سائبر مجرمین دہشت گردی، نفرت یا غیر قانونی سرگرمیوں کی ترویج یا غیر قانونی سماجی رویوں میں ملوث ہونے کے لئے، جیسا کہ چائلڈ پورنوگرافی (بچوں کی فحش نگاری) کی ترسیل یا آن لائن پیڈوفیلیا (بڑوں کا بچوں کی طرف جنسی میلان) ہیں، انٹرنیٹ کا استعمال کرتے ہیں۔ یہ گروپ ان لوگوں پر مشتمل ہے جو جنگ و جدل کی معلومات میں ملوث ہوتے ہیں اور اسی طرح ان لوگوں پر بھی مشتمل ہے جو انفارمیشن ٹیکنالوجی کا استعمال غیر قانونی سیاسی سرگرمی یا دہشت گردی کو منظم کرنے کے لئے کرتے ہیں۔(23)

سائبر کرائمز کی ایک اور تقسیم: ایک اور لحاظ سے سائبر کرائمز کو دو اقسام میں بانٹا جا سکتا ہے:

1۔ کمپیوٹر کی مدد سے کئے جانے والے جرائم

2۔ کمپیوٹر سے منسلک جرائم

کمپیوٹر کی مدد سے کئے جانے والے جرائم: ان سے مراد وہ جرائم ہیں جن کے ارتکاب کیلئے کمپیوٹر کو براہ راست استعمال کیا جاتا ہے۔ سائبر کرائمز کی یہ قسم کمپیوٹر کے ذریعے کی جانے والی خیانت و خرد برد، خدمات کی چوری، معلومات کی چوری، فراڈ اور منظم جرائم کو شامل ہے۔(24)

کمپیوٹر سے منسلک جرائم: ان سے مراد وہ جرائم ہیں جن کا ارتکاب کرنے کیلئے کمپیوٹر بالواسطہ استعمال ہوتا ہے (مثلاً غیر قانونی اسلحے کا سودا کرنے کیلئے ڈیٹا کا ریکارڈ وغیرہ)۔(25)

سائبر کرائم کے خطرات و نقصانات:

سائبر کرائمز کا دائرہ کار معاشی جرائم (فراڈ، چوری، صنعتی جاسوسی، تخریب کاری، حصول بالجبر اور اخفاء) سے لے کر رازداری کی خلاف ورزی، غیر قانونی اور نقصان دہ مواد کی نشر و اشاعت، بدکاری اور دوسرے اخلاقی جرائم میں

سہولت کاری اور منظم جرائم تک پھیلا ہوا ہے۔ سائبر کرائم کی سب سے بڑی سنگینی یہ ہے کہ یہ دہشت گردی سے ملحق ہے اور یہ انسانی زندگی کے تحفظ، قومی تحفظ، اہم بنیادی ڈھانچوں اور دیگر ضروری معاشرتی اجزاء کے خلاف حملوں پر محیط ہے۔(26) سائبر سپیس مسلسل حملوں کی زد میں ہے۔ سائبر جاسوس، چور، تباہی اور تھرتھلی مچانے والے کمپیوٹر سسٹمز میں نقب لگا کر ذاتی معلومات کو چوری کرتے ہیں، ویب سائٹس کو نقصان پہنچاتے ہیں، سروس میں خلل ڈالتے ہیں، سسٹم اور ڈیٹا میں تخریب کاری کرتے ہیں، کمپیوٹر میں وائرس بھیجتے ہیں، دغابازی پر مبنی کاروباری معاملات کرتے ہیں اور افراد اور کمپنیوں کو ہراساں کرتے ہیں۔(27) انٹیلی جنس ایجنسیاں ایسے سائبر حملوں کے خلاف تیاریاں کر رہی ہیں جو ریل اور ہوائی کنٹرول، بجلی کے ترسیلی نیٹ ورکس، سٹاک مارکیٹس، بینکاری اور انشورنس سسٹم کو تہ و بالا کر سکتے ہیں۔ بدقسمتی سے سائبر کرائم کے حقیقی معاشرتی اور معاشی اثرات کا اندازہ لگانا ممکن نہیں ہے، اس کی وجہ یہ ہے کہ بہت سے جرائم ایسے ہوتے ہیں جنہیں رپورٹ ہی نہیں کیا جاتا۔(28) 2008 میں ماہرین نے اندازہ لگایا کہ (صرف) ایک سال میں سائبر کریمینلز نے 100 بلین ڈالر اکٹھے کئے۔(29)

سیمانٹک کارپوریشن کمپنی کا سائبر سیکورٹی کے حوالے ہونے والی بے قاعدگیوں کا ڈیٹا بیس سب سے زیادہ مکمل ہے جس میں 66,400 کے قریب ریکارڈ شدہ خلاف ورزیوں کی نشاندہی کی گئی ہے۔ کارپوریشن کے اپنے انٹیلی جنس نیٹ ورک کے مطابق 157 ممالک میں 57.6 ملین سائبر حملے ہوئے اور 2014ء میں 6,549 نئی خلاف ورزیوں کی نشاندہی کی گئی۔ کارپوریشن کی رپورٹ میں بتایا گیا ہے کہ چھوٹی بڑی کوئی کمپنی انٹرنیٹ سیکورٹی خطرات سے محفوظ نہیں ہے۔ ہر چھ میں سے پانچ کمپنیاں جن کے ملازمین کی تعداد 2500 سے زیادہ ہے انہیں فشنگ (Phishing) حملوں کا سامنا کرنا پڑا۔ ان حملوں میں گزشتہ سال کے مقابلے میں 40 فیصد اضافہ ہوا۔ چھوٹے اور درمیانے درجے کے کاروبار میں 26 سے 30 فیصد سائبر حملوں میں اضافہ ہوا ہے، اس کے معنی ہیں کہ چھوٹے اور درمیانے درجے کے کاروبار پر حملے 60 فیصد تک پہنچ گئے ہیں۔(30)

بنگلا دیش کے مرکزی بینک کے گورنر عطیع الرحمان نے دنیا کی تاریخ میں سب سے بڑی سائبر چوری ہونے پر 15 مارچ 2016ء کو اپنا استعفیٰ پیش کر دیا۔ اسی سال فروری میں فیڈرل ریزرو بنک آف نیویارک سے بھی 81 ملین ڈالر چرا لئے گئے۔ میڈیا رپورٹس کے مطابق نامعلوم ہیکروں نے بنگلا دیش بینک کے کمپیوٹر سسٹم کو توڑتے ہوئے اس

کے اکاؤنٹ سے پہلے نیویارک فیڈرل بنک میں پھر سری لنکا اور فلپائن کے بنکوں میں رقم منتقل کی۔ بنگلا دیش کے بینک سائبر حملے نے ثابت کر دیا ہے کہ معلومات کے اس دور میں ترقی یافتہ، ترقی پذیر یا کم ترقی یافتہ ممالک میں سے کوئی بھی سائبر خطرات سے نمٹنے کیلئے پوری طرح سے تیار نہیں۔(31)

نومبر 2014ء میں کئے گئے سائبر حملے نے کارپوریٹ دنیا کو ہلا کر رکھ دیا۔ بڑے سٹور سے کریڈٹ کارڈ نمبرز چوری کئے گئے، ہیکرز نے سونی پکچرز انٹرٹینمنٹ کی خفیہ سروسز کا کھوج لگالیا، حساس کاروباری رپورٹس قبضے میں لے لیں، اہم شخصیات کی ای میلز، عام صارفین کا ہیلتھ ڈیٹا حتیٰ کہ ریلیز سے قبل فلموں کو بھی ویب سائٹس پر ڈال کر عام کر دیا۔ اس سے ثابت ہوتا ہے کہ سائبر حملوں سے بچاؤ کے لئے موجودہ دور میں استعمال کی جانیوالی ٹیکنالوجیز اتنی موثر نہیں ہیں جتنا کہ انہیں ہونا چاہیے۔ 2015ء میں امریکی پرسنل مینجمنٹ کے ادارے کو ہیک کیا گیا جس کے نتیجے میں 21.5 ملین شہریوں کے ریکارڈ افشا ہو گئے۔ ان ریکارڈز میں شہریوں کی ذاتی معلومات بھی شامل تھیں اور 56لاکھ شہریوں کے انگلیوں کے نشانات بھی ہیکرز نے حاصل کر لئے۔(32)

سنہ 2016 کی نسبت سنہ 2017 میں عالمی سطح پر ایک آرگنائزیشن کو ہونے والا اوسط نقصان 23 فیصد اضافے کے ساتھ 11.7 ملین ڈالر تک پہنچ گیا ہے، جو کہ سنہ 2016 میں 9.5 ملین ڈالر تھا۔(33) سنہ 2017 میں امریکہ میں مختلف کمپنیوں پر سائبر حملوں سے ہونے والا نقصان 21.22 ملین ڈالر ہے۔(34) سنہ 2017 میں سائبر کرائمز سے ہونے والا عالمی نقصان 600 بلین ڈالر تھا جو کہ سنہ 2014 میں 445 بلین ڈالر تھا۔(35)

موجودہ دور میں سائبر کرائم ایسے عفریت کی شکل اختیار کر چکا ہے جس کے لئے جغرافیائی سرحدیں کوئی معنی نہیں رکھتیں، یہی وجہ ہے کہ مختلف ایجنسیاں اس کو قابو میں کرنے کے لئے سر توڑ کوششیں کر رہی ہیں۔ سائبر کرائم امریکی ایجنسی ایف بی آئی کی تیسری بلند ترین ترجیح ہے۔(36) عالمی سطح پر ہائی ٹیکنالوجی کرائم انٹرپول کی پہلی پانچ ترجیہات میں سے ایک ہے۔(37)

سائبر کرائم سے ہونے والے نقصانات کا اصل اندازہ لگانا تقریباً ناممکن ہے کیونکہ سائبر کرائم کے زیادہ تر کیسز رپورٹ نہیں ہوتے، اور جو رپورٹ ہوتے ہیں وہ آٹے میں نمک کے برابر ہیں۔

سائبر کرائمز کے چیلنجز:

سائبر سپیس کی کوئی جغرافیائی حد بندی نہیں ہے۔ یہ ان مجرمین کیلئے جنت ہے جو انٹر نیٹ پر شناخت ہونے کے خوف سے آزاد انٹر نیٹ پر غیر قانونی سر گرمیاں کرتے ہیں۔ قانون نافذ کرنے والی ایجنسیوں کی طرف سے انٹر نیٹ کے کام کرنے کی حقیقت کے بارے میں کم علمی معاملے کو مزید الجھا دیتی ہے۔ اس وقت ملکی اور عالمی سطح پے سائبر کرائمز کے چیلنجز مندرجہ ذیل ہیں:

1۔ **قانونی چیلنجز:** سائبر کرائمز کو کنٹرول کرنے اور ان کی تفتیش کرنے کیلئے قوانین محدود ہیں۔

2۔ **آپریشنل چیلنجز:** تفتیش کاروں کی ایک ایسی متحدہ، تربیت یافتہ اور مطلوبہ ساز و سامان سے آراستہ فورس کی ضرورت ہے جو قومی اور بین الاقوامی سطح پر کام اور تعاون کر سکے۔

3۔ **ٹیکنیکل چیلنجز:** آن لائن مجرموں کو پکڑنے اور ان کے خلاف قانونی چارہ جوئی کرنے کی قانون نافذ کرنے والے اداروں کی کوششیں تکنیکی مہارتیں نہ ہونے کی وجہ سے ضائع ہو جاتی ہیں۔(38)

4۔ **عمومی چیلنجز:** سائبر کرائمز پر قابو پانے کے حوالے سے ایک بہت بڑا مسئلہ یہ ہے کہ یہ بہت کم رپورٹ ہوتے ہیں جس کی بڑی وجوہات سائبر کرائمز کے حوالے سے عوامی عدم واقفیت اور بہت سے ممالک میں سائبر کرائمز کے حوالے سے مناسب قانون سازی نہ ہونا ہیں۔ سائبر کرائمز کے بارے میں عوام میں آگہی کم پائی جاتی ہے اس لئے سائبر کرائمز کے حوالے سے تحقیقی مواد بھی بہت کم پایا جاتا ہے۔

سائبر کرائمز کے لئے عدالتی دائرہ اختیار بھی ایک بہت بڑا عالمی مسئلہ ہے جسے حل کرنے کی اشد ضرورت ہے۔ نیز سائبر کرائمز، سائبر قوانین، کمپیوٹر فرانزک اور سائبر کرائمز کی تحقیق و تفتیش کی سمجھ بوجھ رکھنے والے ماہرین کی بھی بہت زیادہ کمی ہے۔ پولیس افسران، وکلاء، پراسیکیوٹرز اور جج حضرات سائبر کرائمز کے فنی اور تکنیکی پہلوؤں کے بارے میں بہت کم جانتے ہیں۔

موجودہ صورتحال یہ ہے کہ روایتی جرائم کے لئے قانون سازی تقریبا دنیا کے ہر ملک میں موجود ہے۔ مگر سائبر کرائمز کے لئے کافی ممالک میں یا تو قانون سازی ہوئی ہی نہیں یا اگر ہوئی ہے تو وہ مطلوبہ معیار کی نہیں ہے۔ چونکہ سائبر کریمینلز اور سائبر کرائمز کے لئے جغرافیائی حدود کوئی معنی نہیں رکھتیں اس لئے سائبر کرائم ایک

ایسا مسئلہ ہے جس کے بارے میں کسی ایک ملک کی قانون سازی مکمل طور پے کافی نہیں ہو سکتی، اس مسئلے کے مستقل حل کے لئے ملکی سطح کے ساتھ ساتھ بین الاقوامی سطح پے ممکنہ حد تک مشترکہ قانون سازی کی بھی ضرورت ہے جس کے لئے ابھی تک کوئی سنجیدہ کوشش نہیں کی جارہی۔

خلاصہ:

سائبر کرائم سے مراد ایسی تمام مجرمانہ سرگرمیاں ہیں جن کا ارتکاب کمپیوٹر، انٹرنیٹ، سائبر سپیس اور ورلڈ وائڈ ویب کے ذریعے کیا جاتا ہے۔ سائبر کرائمز کا آغاز 1820 سے ہوا۔ اس وقت سائبر کرائمز کی، نشانہ بننے والوں کے اعتبار سے، کمپیوٹر کے کردار کے اعتبار سے، سائبر کریمینلز کے اعتبار سے اور کمپیوٹر کی مدد یا کمپیوٹر سے تعلق کے اعتبار سے مختلف اقسام ہیں۔ اسی طرح سائبر کریمینلز بھی پیشہ ور اور منظم ہیکرز، باغی ملازمین، جاسوس، کمپیوٹر پائریٹس، دہشتگرد اور انتہا پسندوں سمیت مختلف اقسام میں منقسم ہیں۔ سائبر کرائم موجودہ دور کا ایک سنگین، اہم اور بڑھتا ہوا مسئلہ بن چکا ہے۔ آج جہاں دنیا کے ممالک کے حفاظتی، دفاعی، مواصلاتی، تعلیمی، معاشی اور زمینی و فضائی نقل و حمل سمیت مختلف نظام سائبر کریمینلز کی پہنچ میں ہیں، وہاں افراد کی نجی معلومات اور مختلف اداروں کا سارا ریکارڈ بھی ان کی رسائی میں ہے۔ سائبر کرائم سے ہونے والے نقصانات کا اصل اندازہ لگانا تقریباً ناممکن ہے کیونکہ سائبر کرائم کے زیادہ تر کیسز رپورٹ نہیں ہوتے، اور جو رپورٹ ہوتے ہیں وہ آٹے میں نمک کے برابر ہیں۔ اس وقت دنیا کو ملکی اور بین الاقوامی سطح پر سائبر کرائمز کے حوالے سے تکنیکی، قانونی، عملی اور عمومی قسم کے چیلنجز کا سامنا ہے۔ ضرورت اس بات کی ہے کہ ان چیلنجز سے نمٹنے کے لئے ملکی اور بین الاقوامی سطح پے کوششیں تیز تر کی جائیں۔

حوالہ جات

(1) Mali, Parshant, A Text BOOK OF CYBER CRIME AND PENALTIES [AS PER ITA A 2008 AND IPC] (Draft Version), p4.available at: https://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt

(2) https://dictionary.cambridge.org/dictionary/english/cyber?a=british (visited on 21-7-2018)

(3) https://www.merriam-webster.com/dictionary/cyber (visited on 21-7-2018)

(4) https://en.oxforddictionaries.com/definition/cyber- (visited on 21-7-2018)

(5) https://www.merriam-webster.com/dictionary/crime (visited on may4, 2018)

(6) A Text BOOK OF CYBER CRIME AND PENALTIES, p4

(7) Kamini Dashora, Cyber Crime in the Society: Problems and Preventions, Journal of Alternative Perspectives in the Social Sciences, 2011, Vol 3, No 1, p 242

(8) Ibid

(9) Debarati Holder, K. Jaishankar, Victimization of Women: Cyber Laws, Rights and regulation, Information Science Reference,USA, 2012, p14

(10) Moore, Roobert, Cybercrime Investigating High-Technology Computer Crime, Second edition, Routledge New York, 2015, p4

(11) A Text BOOK OF CYBER CRIME AND PENALTIES, p7

(12) Atul Jain, Cybercrime Issues Threats and Management, ISHA Books Dehli, 2005, p4-5

(13) A Text BOOK OF CYBER CRIME AND PENALTIES, p6

(14) Smith RG., Trajectories of Cybercrime, in Smith RG, Cheung RC-C & Lau LY-C (eds) Cybercrime Risks and Responses: Eastern and Western Perspectives, Palgrave Macmillan: London, 2015,p 13-34

(15) Ritu, Cyber Crimes: National and International Perspective, Department of Law, Kuruksheta University, 2017, p 88

(16) Cyber Crime in the Society: Problems and Preventions, p248

(17) Cyber Crimes: National and International Perspective, p 89

(18) Cyber Crimes: National and International perspective, p 90; Zibber Mohiuddin, Cyber Laws in Pakistan; A situational Analysis and Way Forward, 2006, p 9 (Available at: www.supreme court.gov.pk/ijc/articles/10/5.pdf visited on 22-6-2018)

(19) Verma,Amita, Cybercrimes: An analytical Study of International and National Legal Regimes, Punjab University, Chandigarh, 2004, p 59

(20) یوزنیٹ ایک نیٹ ورک ہوتا ہے جو انٹرنیٹ کے ذریعے ڈسکشن گروپ مہیا کرتا ہے۔

(21) Cybercrimes: An Analytical Study of International and National Legal Regimes, p 59, 60; Cybercrimes: National and International perspective, p 91

(22) Cybercrimes: An Analytical Study of International and National Legal Regimes, p 61

(23) Thomas, Douglas and Loader, Brain., Cybercrime Law and enforcement, security and surveillance in the information age, Routledge New York, 2000, p 6-8

(24) Bhaskar,S.M. Ahson,S.I, Information Security A Practical Approach, Alfa Science, 2009,p 212

(25) Stamatellos,Giannis, Computer Ethics: A Global Perspective, Jones and Bartlett Learning, 2007, p 11

(26) Cybercrime Issues Threats and Management, p5

(27) A Text BOOK OF CYBER CRIME AND PENALTIES, p5-6

(28) Ibid, p7

(29) Byron Acohido, Meet A–Z: The Computer Hacker behind a Cybercrime Wave, USA Today, August 5, 2008. Available at: http://www.usatoday.com/tech/news/ Computersecurity/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm.

(30) Ahmad Raza, Securing Cyberspace for Pakistan, Available at: http: //www. Technology review.pk/securing-cyberspace-for-pakistan/ (Visited on 26-5-2018 at: 4 pm)

(31) Ibid

(32) David Talbot, Cyber security: The Age of the Mega breach, 2016 Available at: https: // www. technologyreview.com/s/545616/cybersecurity-the-age-of-the-megabreach / (Visited on 26-5-2018 at 3 pm)

(33) http://www.4-traders.com/ACCENTURE-11521/news/CORRECTING-and-REPLACING-Accenture-and-Ponemon-Institute-Report-Cyber-Crime-Drains-11-7-Million-Pe-25175624/ (Visited on 26-5-2018 at 3 pm)

(34)https://www.google.com.pk/search?q=year+wise+ratio+of+cyber+crime&tbm=isch &source (visited on 23-6-2018 at 12 pm)

(35) https://www.forbes.com/sites/forbestechcouncil/2018/05/15/cyberthreats-a-10-year-perspective/#1ba2872a5e9e (visited on 15-07-2019)

(36) Kshetri, N., The economics of Cybercrime, IEEE Security and Privacy, 2006, p 33-39

(37) Broadhurst, R. and P. Grabosky, eds. Cyber-crime: The challenge in Asia, Hong Kong University Press, 2005, p 434

(38) Cybercrimes: An Analytical Study of International and National Legal Regimes, p 64