International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

CYBERCRIME -A RISK TO HUMANITY

Dr. Gagan B Khanna

BBD Govt. College, Chimanpura, Shahpura, Jaipur, Rajasthan, India

ABSTRACT: Cybercrime is a type of crime involving a computer or a computer network.[1][2] The computer may have been used in committing the crime, or it may be the target.[3] Cybercrime may harm someone's security or finances.[4][5]

Internationally, both state and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyberwarfare. Warren Buffett describes cybercrime as the "number one problem with mankind"[6] and said that it "poses real risks to humanity".[7]

A 2014 report sponsored by McAfee estimated that cybercrime had resulted in $445 billion USD in annual damage to the global economy.[8] Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.[9] In 2013, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concluded that nearly 1 percent of global gross domestic product (GDP), close to $600 billion, is lost to cybercrime each year.[10] The World Economic Forum 2011 Global Risk Report confirmed that organized cybercrime groups are joining forces to commit criminal activities online, while estimating the likelihood of their detection and prosecution to be less than 1 percent in the US.[11] There are also many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, legally or otherwise.

KEYWORDS: cybercrime, security, warfare, fraud, credit, debit, criminal, economic, legally, confidential

I.INTRODUCTION

Computer crime encompasses a broad range of activities, including computer fraud, financial crimes, scams, cybersex trafficking, and ad fraud.[12][13]

Computer fraud

Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system.[14] If computer fraud involves the use of the internet, it can be considered Internet fraud. The legal definition of computer fraud varies by jurisdiction, but typically involves accessing a computer without permission or authorization.

Forms of computer fraud include hacking into computers to alter information, distributing malicious code such as computer worms or viruses, installing malware or spyware to steal data, phishing, and advance-fee scams.[15]

Other forms of fraud may be committed using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crimes often result in the loss of personal or financial information.

Cyberterrorism

Cyberterrorism are acts of terrorism committed through the use of cyberspace or computer resources.[16] Acts of disruption of computer networks and personal computers through viruses, worms, phishing, malicious software, hardware, or programming scripts can all be forms of cyberterrorism.[17]

Government officials and information technology (IT) security specialists have documented a significant increase in network problems and server scams since early 2001. Within the United States, there is an increasing concern from agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA). Such incidents are part of an organized effort by cyberterrorist foreign intelligence services or other groups to map potential security flaws in critical systems.[18]

Cyberextortion

Cyberextortion occurs when a website, e-mail server, or computer system is subjected to or threatened with attacks by malicious hackers, such as denial-of-service attacks. Cyberextortionists demand money in return for promising to stop the attacks and to offer "protection". According to the FBI, cyberextortionists are increasingly attacking corporate websites and networks, crippling their ability to operate, and demanding payments to restore their service. More than 20 cases are reported each month to the FBI, and many go unreported in order to keep the victim's name out of the

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

public domain. Perpetrators use a distributed denial-of-service attack.[19] However, other cyberextortion techniques exist, such as doxing, extortion, and bug poaching. An example of cyberextortion was the Sony Hack of 2014.[20]

Ransomware

Ransomware is a type of malware used in cyberextortion to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid. The threat of ransomware is a global issue, with more than 300 million attacks worldwide in 2010. According to the 2009 Unit 42 Ransomware Threat Report, the average ransom demand in cases handled by Norton climbed 144 percent to $2.2 million. This report included an 85 percent increase in the number of victims who had their personal information shown on dark web information dumps.[21] A loss of nearly $400 million in 2010 and 2009 is just one of the statistics showing the impact of ransomware attacks on everyday people.[22]

Cybersex trafficking

Cybersex trafficking is the transportation of victims and then the live streaming of coerced sexual acts or rape on webcam.[23][24][25][26] Victims are abducted, threatened, or deceived and transferred to "cybersex dens".[27][28][29] The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with an internet connection.[25] Perpetrators use social media networks, video conferences, dating pages, online chat rooms, apps, dark web sites,[30] and other platforms.[31] They use online payment systems[30][32][33] and cryptocurrencies to hide their identities.[34] Millions of reports of its occurrence are sent to authorities annually.[35] New legislation and police procedures are needed to combat this type of cybercrime.[36]

There are an estimated 6.3 million victims of cybersex trafficking, according to a recent report by the International Labour Organization and IOM.[37][38] This number includes about 1.7 million child victims. An example of cybersex trafficking is the 2013–2011 Nth room case in South Korea.[39]

Cyberwarfare

The U.S. Department of Defense notes that cyberspace has emerged as a national-level concern through several recent events of geostrategic importance, including the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become normalized in future warfare among nation-states, the military commanders intend to adapt the concept of cyberspace operations impact in the future.[40]

Computer as a tool

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the like existed before the development of computers and the internet. The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.[41]

Crimes that use computer networks or devices to advance other ends include:

- Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime)
- Information warfare
- Phishing scams
- Spam
- Propagation of illegal obscene or offensive content, including harassment and threats

The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.

Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware.[42] Or they may contain links to fake online banking or other websites used to steal private account information.

Obscene or offensive content

The content of websites and other electronic communications may be distasteful, obscene, or offensive for a variety of reasons. In some instances, these communications may be illegal.

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

Ad-fraud

Ad-frauds are particularly popular among cybercriminals, as such frauds are lucrative and less likely to be prosecuted.[43] Jean-Loup Richet, a professor at the Sorbonne Business School, classified the large variety of ad-fraud committed by cybercriminals into three categories: identity fraud, attribution fraud, and ad-fraud services.[13]

Identity fraud aims to impersonate real users and inflate audience numbers. Several ad-fraud techniques relate to this category and include traffic from bots (coming from a hosting company or a data center, or from compromised devices); cookie stuffing; falsifying user characteristics, such as location and browser type; fake social traffic (misleading users on social networks into visiting the advertised website); and the creation of fake social media accounts to make the bot appear legitimate.

Attribution fraud impersonates the activities of real users, such as clicks and conversations. Multiple ad-fraud techniques belong to this category: hijacked devices and the use of infected users (through malware) as part of a botnet to participate in ad fraud campaigns; click farms (companies where low-wage employees are paid to click or engage in conversations and affiliates' offers); incentivized browsing; video placement abuse (delivered in display banner slots); hidden ads (which will never be viewed by real users); domain spoofing (ads served on a website other than the advertised real-time bidding website); and clickjacking, in which the user is forced to click on an ad.

Ad fraud services are related to all online infrastructure and hosting services that might be needed to undertake identity or attribution fraud. Services can involve the creation of spam websites (fake networks of websites created to provide artificial backlinks); link building services; hosting services; creation of fake and scam pages impersonating a famous brand and used as part of an ad fraud campaign.

II.DISCUSSION

Online harassment

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing, for example, on gender, race, religion, nationality, or sexual orientation.

There are instances when committing a crime using a computer can lead to an enhanced sentence. For example, in the case of United States v. Neil Scott Kramer, the defendant was given an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3) for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct." Kramer appealed the sentence on the grounds that there was insufficient evidence to convict him under this statute because his charge included persuading through a computer device and his cellular phone technically is not a computer. Although Kramer tried to argue this point, the U.S. Sentencing Guidelines Manual states that the term "computer" means "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

In the United States, over 41 states have passed laws and regulations that regard extreme online harassment as a criminal act. These acts can be punished on a federal scale, such as US Code 18 Section 2261A, which states that using computers to threaten or harass can lead to a sentence of up to 20 years, depending on the action taken.[44]

Several countries outside of the United States have also created laws to combat online harassment. In China, a country that supports over 20 percent of the world's internet users, the Legislative Affairs Office of the State Council passed a strict law against the bullying of young people through a bill in response to the Human Flesh Search Engine.[45][46] The United Kingdom passed the Malicious Communications Act, among other acts from 1997 to 2013, which stated that sending messages or letters electronically that the government deemed "indecent or grossly offensive" and/or language intended to cause "distress and anxiety" can lead to a prison sentence of six months and a potentially large fine.[47][48] Australia, while not directly addressing the issue of harassment, has grouped the majority of online harassment under the Criminal Code Act of 1995. Using telecommunication to send threats or harass and cause offense was a direct violation of this act.[49]

Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech. In fact, spoken or written "true threat" speech or text is

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

criminalized because of "intent to harm or intimidate". That also applies to online or network-related threats in written text or speech.

Cyberbullying has increased drastically with the growing popularity of online social networking. As of January 2011, 44 percent of adult internet users in the United States have "personally experienced online harassment".[50] Children who experience online harassment deal with negative and sometimes life-threatening side effects. In 2010, reports displayed 41 percent of children developing social anxiety, 37 percent of children developing depression, and 26 percent of children having suicidal thoughts.[51]

The United Arab Emirates was named in a spying scandal where the Gulf nation along with other repressive governments purchased NSO Group's mobile spyware Pegasus for mass surveillance. Prominent activists and journalists were targeted as part of the campaign, including Ahmed Mansoor, Princess Latifa, Princess Haya, and more. Ghada Oueiss was one of the many high-profile female journalists and activists who became the target of online harassment. Oueiss filed a lawsuit against UAE ruler Mohamed bin Zayed Al Nahyan along with other defendants, accusing them of sharing her photos online. The defendants, including the UAE ruler, filed motions to dismiss the case of the hack-and-leak attack.[52]

Drug trafficking

Darknet markets are used to buy and sell recreational drugs online. Some drug traffickers use encrypted messaging tools to communicate with drug mules or potential customers. The dark web site Silk Road was the first major online marketplace for drugs, starting operation in 2011. It was permanently shut down in 2014 by the FBI and Europol. After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged. However, it was just an older marketplace named Diabolus Market, that used the name for more exposure from the brand's previous success.[53]

Darknet markets have had a rise in traffic in recent years for many reasons, one of the biggest contributors being the anonymity offered in purchases, and often a seller-review system.[54] There are many ways in which darknet markets can financially drain individuals. Vendors and customers alike go to great lengths to keep their identities a secret while online. Commonly used tools are virtual private networks (VPN), Tails, and the Tor Browser to help hide their online presence. Darknet markets entice customers by making them feel comfortable. People can easily gain access to a Tor browser with DuckDuckGo browser that allows a user to explore much deeper than other browsers such as Google Chrome. However, actually gaining access to an illicit market is not as simple as typing it in on a search engine like one would with Google. Darknet markets have special links that change frequently, ending in .onion as opposed to the typical .com, .net, and .org domain extensions. To add to privacy, the most prevalent currency on these markets is Bitcoin. Bitcoin allows transactions to be anonymous, with the only information available to the public being the record that a transaction occurred between two parties.[55]

An issue marketplace users face is when vendors or the market itself are exit scamming.[56] This is when a vendor with a high rating will act as if they are selling on the market and have users pay for products they will not receive.[57] The vendor will then close off their account after receiving money from multiple buyers and never send what was purchased. The vendors all being involved in illegal activities have a low chance of not exit scamming when they no longer want to be a vendor. In 2012, an entire market known as Wall Street Market had allegedly exit scammed, stealing $30 million dollars from the vendors' and buyers' wallets in bitcoin.[58]

FBI has cracked down on these markets. In July 2014, FBI seized one of the biggest markets, commonly called Alphabay, which later re-opened in August 2010 under the control of DeSnake, one of the original administrators.[59][60] Investigators will pose as a buyer and order products from darknet vendors in the hopes that vendors leave a trail the investigators can follow. One investigation had an investigator pose as a firearms seller and for six months people purchased from them and provided home addresses.[61] The FBI was able to make over a dozen arrests during this six-month investigation.[61] Another one of law enforcement's crackdowns was on vendors selling fentanyl and opiates. With thousands of people dying each year due to drug overdose, investigators have made it a priority.[62] Many vendors do not realize the extra criminal charges that go along with selling drugs online. Commonly they get charged with money laundering and charges for when the drugs are shipped in the mail on top of being a drug distributor.[63] In 2012, a vendor was sentenced to 10 years in prison after selling cocaine and methamphetamine under the name JetSetLife.[64] Although investigators spend large amounts of time tracking down people, in 2013, only 65 suspects who bought and sold illegal goods on some of the biggest markets were identified.[65] This is compared to the thousands of transactions taking place daily on these markets.

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

Notable incidents

- One of the highest-profile banking computer crimes occurred over a course of three years beginning in 1970. The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over $1.5 million from hundreds of accounts.[66]
- A hacking group called MOD (Masters of Deception) allegedly stole passwords and technical data from Pacific Bell, Nynex, and other telephone companies as well as several big credit agencies and two major universities. The damage caused was extensive; one company, Southwestern Bell, suffered losses of $370,000 alone.[66]
- In 1983, a 19-year-old UCLA student used his PC to break into a Defense Department International Communications system.[66]
- Between 1995 and 1998, the Newscorp satellite pay-to-view encrypted SKY-TV service was hacked several times during an ongoing technological arms race between a pan-European hacking group and Newscorp. The original motivation of the hackers was to watch Star Trek reruns in Germany, which was something which Newscorp did not have the copyright to allow.[67]
- On 26 March 1999, the Melissa worm infected a document on a victim's computer, then automatically sent that document and a copy of the virus spread via e-mail to other people.
- In February 2000, an individual going by the alias of MafiaBoy began a series denial-of-service attacks against high-profile websites, including Yahoo!, Dell, Inc., E*TRADE, eBay, and CNN. About 50 computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in DDoS attacks. On 3 August 2000, Canadian federal prosecutors charged MafiaBoy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks.
- The Stuxnet worm corrupted SCADA microprocessors, particularly of the types used in Siemens centrifuge controllers.
- The Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legitimate. But apparently, the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. The RBN has been described by VeriSign as "the baddest of the bad".[68] It offers web hosting services and internet access to all kinds of criminal and objectionable activities, with individual activities earning up to $150 million in one year. It specialized in, and in some cases monopolized, personal identity theft for resale. It is the originator of MPack and an alleged operator of the now defunct Storm botnet.
- On 2 March 2010, Spanish investigators arrested three men suspected of infecting over 13 million computers around the world. The "botnet" of infected computers included PCs inside more than half of the Fortune 1000 companies and more than 40 major banks, according to investigators.[69]
- In August 2010, the international investigation Operation Delego, operating under the aegis of the Department of Homeland Security, shut down the international pedophile ring Dreamboard. The website had approximately 600 members and may have distributed up to 123 terabytes of child pornography (roughly equivalent to 16,000 DVDs). To date this is the single largest U.S. prosecution of an international child pornography ring; 52 arrests were made worldwide.[70]
- In January 2012, Zappos.com experienced a security breach compromising the credit card numbers, personal information, and billing and shipping addresses of as many as 24 million customers.[71]
- In June 2012, LinkedIn and eHarmony were attacked, compromising 65 million password hashes. 30,000 passwords were cracked and 1.5 million EHarmony passwords were posted online.[72]
- In December 2012, the Wells Fargo website experienced a denial-of-service attack, potentially compromising 70 million customers and 8.5 million active viewers. Other banks thought to be compromised include Bank of America, J. P. Morgan U.S. Bank, and PNC Financial Services.[73]
- On 23 April 2013, the Twitter account of the Associated Press was hacked. The hacker posted a hoax tweet about fictitious attacks in the White House that they claimed left then-President Obama injured.[74] This hoax tweet resulted in a brief plunge of 130 points from the Dow Jones Industrial Average, the removal of $136 billion from the S&P 500 index,[75] and the temporary suspension of AP's Twitter account. The Dow Jones later restored its session gains.
- In May 2014, 74 countries logged a ransomware cybercrime, called "WannaCry".[76]
- Illicit access to camera sensors, microphone sensors, phonebook contacts, all internet-enabled apps, and metadata of mobile telephones running Android and iOS were reportedly made accessible by Israeli spyware, found to be in operation in at least 46 nation-states around the world. Journalists, royalty, and government officials

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

were among the targets.[77][78][79] Previous accusations of cases of Israeli weapons companies meddling in international telephony[80] and smartphones[81] have been eclipsed in the 2013 reported case.

- In December 2012, United States intelligence officials and an investigation by The New York Times revealed that ToTok, a messaging application widely used in the United Arab Emirates, is a spying tool for the UAE. The research revealed that the Emirati government attempted to track every conversation, movement, relationship, appointment, sound, and image of those who installed the app on their phones.[82]

Combating computer crime

It is difficult to find and combat cybercrime perpetrators due to their use of the internet in support of cross-border attacks. Not only does the internet allow people to be targeted from various locations, but the scale of the harm done can be magnified. Cybercriminals can target more than one person at a time. The availability of virtual spaces[83] to public and private sectors has allowed cybercrime to become an everyday occurrence.[84] In 2013, The Internet Crime Complaint Center received 351,937 complaints of cybercrime, which lead to $2.7 billion lost.[85]

Investigation

In a criminal investigation, a computer can be a source of evidence (see digital forensics). Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countries,[86] Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example, the EU-wide Data Retention Directive (previously applicable to all EU member states) stated that all e-mail traffic should be retained for a minimum of 12 months.

There are many ways for cybercrime to take place, and investigations tend to start with an IP Address trace; however, that is not necessarily a factual basis upon which detectives can solve a case. Different types of high-tech crime may also include elements of low-tech crime, and vice versa, making cybercrime investigators an indispensable part of modern law enforcement. Methods of cybercrime detective work are dynamic and constantly improving, whether in closed police units or in international cooperation framework.[87]

In the United States, the FBI[88] and the Department of Homeland Security (DHS)[89] are government agencies that combat cybercrime. The FBI has trained agents and analysts in cybercrime placed in their field offices and headquarters.[88] Under the DHS, the Secret Service has a Cyber Intelligence Section that works to target financial cybercrimes. They use their intelligence to protect against international cybercrime. Their efforts work to protect institutions, such as banks, from intrusions and information breaches. Based in Alabama, the Secret Service and the Alabama Office of Prosecution Services work together to train professionals in law enforcement through the creation of The National Computer Forensic Institute.[89][90][91] This institute works to provide "state and local members of the law enforcement community with training in cyber incident response, investigation, and forensic examination in cyber incident response, investigation, and forensic examination."[91]

Due to the common use of encryption and other techniques to hide their identity and location by cybercriminals, it can be difficult to trace a perpetrator after the crime is committed, so prevention measures are crucial.[84][92]

III.RESULTS

Prevention

The Department of Homeland Security also instituted the Continuous Diagnostics and Mitigation (CDM) Program.[93] The CDM Program monitors and secures government networks by tracking and prioritizing network risks, and informing system personnel so that they can take action. In an attempt to catch intrusions before the damage is done, the DHS created the Enhanced Cybersecurity Services (ECS) to protect public and private sectors in the United States.[94] The Cyber Security and Infrastructure Security Agency approves private partners that provide intrusion detection and prevention services through the ECS. An example of one of these services offered is DNS sinkholing.[95][96]

Many cybersecurity products and technologies are used by organizations, but cybersecurity professionals have been skeptical of prevention-focused strategies.[97] The mode of use of cybersecurity products has also been called into question. Google click fraud czar Shuman Ghosemajumder has argued that companies using a combination of individual products for security is not a scalable approach and advocated for the use of cybersecurity technology primarily in the form of services.[98]

Legislation

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries such as the Philippines, laws against cybercrime are weak or sometimes

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.[99]

Then-President Barack Obama released an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze the assets of convicted cybercriminals and block their economic activity within the United States. This is some of the first solid legislation that combats cybercrime in this way.[100]

The European Union adopted directive 2013/40/EU. All offences of the directive, and other definitions and procedural institutions are also in the Council of Europe's Convention on Cybercrime.[101]

It is not only the US and the European Union that are introducing new measures against cybercrime. On 31 May 2014, China announced that its new cybersecurity law takes effect on this date.[102]

In Australia, common legislation in Commonwealth jurisdiction which is applied to combat cybercrime by means of criminal offence provisions and information gathering and enforcement powers includes the Criminal Code Act 1995 (Cth), the Telecommunications Act 1997 (Cth), and the Enhancing Online Safety Act 2015 (Cth).

In Roads and Traffic Authority of New South Wales v Care Park Pty Limited [2012] NSWCA 35, it was found that the use of a discovery order made upon a third party for the purposes of determining the identity or whereabouts of a person may be exercised merely on the prerequisite that such information requested will aid the litigation process.[103]

In Dallas Buyers Club LLC v iiNet Limited [2015] FCA 317, guidance is provided on the interpretation of rule 7.22 of the Federal Court Rules 2011 (Cth) with respect to the issue of to what extent a discovery order must identify a person for it to be a valid request for information to determine the identity or whereabouts of a person in the circumstance of an end-user of an internet service being a different person to the account holder. Justice Perram stated: "... it is difficult to identify any good reason why a rule designed to aid a party in identifying wrongdoers should be so narrow as only to permit the identification of the actual wrongdoer rather than the witnesses of that wrongdoing."[104]

Penalties

Penalties for computer-related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.[105]

However, some hackers have been hired as information security experts by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create perverse incentives. A possible counter to this is for courts to ban convicted hackers from using the internet or computers, even after they have been released from prison – though as computers and the Internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian. However, nuanced approaches have been developed that manage cyber offenders' behavior without resorting to total computer or internet bans.[106] These approaches involve restricting individuals to specific devices which are subject to computer monitoring or computer searches by probation or parole officers.[107]

Awareness

As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals increasingly attempt to steal that information. Cybercrime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information continues to grow in importance. According to the FBI's Internet Crime Complaint Center in 2014, there were 269,422 complaints filed. With all the claims combined there was a reported total loss of $800,492,073.[108] But cybercrime does not yet seem to be on the average person's radar. There are 1.5 million cyber-attacks annually, which means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing that only 16 percent of victims had asked the people who were carrying out the attacks to stop.[109] Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online.

Intelligence

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

As cybercrime has proliferated, a professional ecosystem has evolved to support individuals and groups seeking to profit from cybercriminal activities. The ecosystem has become quite specialized, including malware developers, botnet operators, professional cybercrime groups, groups specializing in the sale of stolen content, and so forth. A few of the leading cybersecurity companies have the skills, resources and visibility to follow the activities of these individuals and groups.[110] A wide variety of information is available from these sources which can be used for defensive purposes, including technical indicators such as hashes of infected files[111] or malicious IPs/URLs,[111] as well as strategic information profiling the goals, techniques and campaigns of the profiled groups. Some of it is freely published, but consistent, ongoing access typically requires subscribing to an adversary intelligence subscription service. At the level of an individual threat actor, threat intelligence is often referred to as that actor's "TTP" or "tactics, techniques, and procedures", as the infrastructure, tools, and other technical indicators are often trivial for attackers to change. Corporate sectors are considering crucial role of artificial intelligence cybersecurity.[112][113]

INTERPOL Cyber Fusion Center has begun a collaboration with cybersecurity key players to distribute information on the latest online scams, cyber threats and risks to internet users. Reports cutting across social engineered frauds, ransomware, phishing, and other has since 2014 been distributed to security agencies in over 150 countries.[114]

Diffusion of cybercrime

The broad diffusion of cybercriminal activities is an issue in computer crime detection and prosecution.

Hacking has become less complex as hacking communities have greatly diffused their knowledge through the internet.[115] Blogs and communities have contributed substantially to information sharing as beginners can benefit from older hackers' knowledge and advice.

Furthermore, hacking is cheaper than ever: before the cloud computing era, in order to spam or scam, one needed a variety of resources, such as a dedicated server, skills in server management, network configuration, and maintenance, and knowledge of internet service provider standards. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam.[116] Cloud computing could be helpful for a cybercriminal as a way to leverage his or her attack, in terms of brute-forcing a password, improving the reach of a botnet, or facilitating a spamming campaign.[117]

IV.CONCLUSIONS

The National Cyber Crime Unit (NCCU) is a command of the United Kingdom's National Crime Agency.[1] With the creation of the National Crime Agency in 2013, the unit was formed following the merge of the Serious Organised Crime Agency's cyber division with the Police Central E-Crime Unit (PCeU) of the Metropolitan Police Service, and is one of four current commands which look at the growing use of cyber crime and ways to identify it.[2]The current head of the NCCU is Dr Jamie Saunders, formally of the UK Foreign and Commonwealth Office (FCO), where from January 2012, he was director of international cyber policy.[3] The National Security Agency (NSA) is a national-level intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence (DNI). The NSA is responsible for global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT). The NSA is also tasked with the protection of U.S. communications networks and information systems.[8][9] The NSA relies on a variety of measures to accomplish its mission, the majority of which are clandestine.[10] The existence of the NSA was not revealed until 1975. The NSA has roughly 32,000 employees.[11]

REFERENCES

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
2. ^ "cybercrime | Definition". Encyclopedia Britannica. Retrieved 25 May 2010.
3. ^ Kruse, Warren G.; Heiser, Jay G. (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.
4. ^ Bossler, Adam M.; Berenblum, Tamar (20 October 2012). "Introduction: new directions in cybercrime research". Journal of Crime and Justice. 42 (5): 495–499. doi:10.1080/0735648X.2012.1692426. ISSN 0735-648X.
5. ^ "cybercrime | Definition, Statistics, & Examples | Britannica". www.britannica.com. Retrieved 14 December 2010.
6. ^ "BUFFETT: This is 'the number one problem with mankind'". Business Insider. Retrieved 17 May 2010.
7. ^ "Warren Buffett: 'Cyber poses real risks to humanity'". finance.yahoo.com. Retrieved 17 May 2010.
8. ^ "Cyber crime costs global economy $445 billion a year: report". Reuters. 9 June 2014. Retrieved 17 June 2014.

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

9. ^ "#Cybercrime— what are the costs to victims - North Denver News". North Denver News. 17 January 2015. Retrieved 16 May 2015.
10. ^ Lewis, James (February 2013). "Economic Impact of Cybercrime - No Slowing Down" (PDF).
11. ^ "The Global Risk Report 2011" (PDF). World Economic Forum. 15th Edition: 102. 15 January 2011.
12. ^ Gordon, Sarah (25 July 2006). "On the definition and classification of cybercrime". Journal in Computer Virology. 2: 13–20. doi:10.1007/s11416-006-0015-z. S2CID 3334277.
13. ^ Richet, Jean-Loup (1 January 2009). "How cybercriminal communities grow and change: An investigation of ad-fraud communities". Technological Forecasting and Social Change. 174 (121282): 121282. doi:10.1016/j.techfore.2010.121282. ISSN 0040-1625. S2CID 239962449.
14. ^ Lehman, Jeffrey; Phelps, Shirelle (2005). West's Encyclopedia of American Law, Vol. 3 (2 ed.). Detroit: Thomson/Gale. p. 137. ISBN 9780787663742.
15. ^ "Computer and Internet Fraud". LII / Legal Information Institute. Retrieved 1 November 2011.
16. ^ Parker D (1983) Fighting Computer Crime, U.S.: Charles Scribner's Sons.
17. ^ "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress". www.everycrsreport.com. Retrieved 5 September 2010.
18. ^ Combs, Cindy C.; Slann, Martin W. (2002). Cyberterrorism. Facts on File. pp. 52–53. ISBN 9781438110196.
19. ^ Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (PDF). Archived from the original (PDF) on 6 July 2011.
20. ^ Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Archived from the original on 25 September 2015. Retrieved 20 September 2015.
21. ^ "The Growing Ransomware Threat: 4 Trends and Insights". Palo Alto Networks. 25 March 2009. Retrieved 11 May 2008.
22. ^ "100+ ransomware statistics for 2008 and beyond - Norton". us.norton.com. Retrieved 11 May 2008.
23. ^ Carback, Joshua T. (2013). "Cybersex Trafficking: Toward a More Effective Prosecutorial Response". Criminal Law Bulletin. 54 (1): 64–183. p. 64.
24. ^ "IJM Seeks to End Cybersex Trafficking of Children and #RestartFreedom this Cyber Monday and Giving Tuesday". PR Newswire. 28 November 2015.
25. ^ "Cybersex Trafficking". IJM. 2011.
26. ^ "Cyber-sex trafficking: A 21st century scourge". CNN. 18 July 2013.
27. ^ "Senator warns of possible surge in child cybersex traffic". The Philippine Star. 13 April 2011.
28. ^ "Duterte's drug war and child cybersex trafficking". The ASEAN Post. 18 October 2012.
29. ^ "Norwegian national, partner nabbed; 4 rescued from cybersex den". Manila Bulletin. 1 May 2011.
30. ^ "Cheap tech and widespread internet access fuel rise in cybersex trafficking". NBC News. 30 June 2013.
31. ^ "Senate to probe rise in child cybersex trafficking". The Philippine Star. 11 November 2012.
32. ^ "Global taskforce tackles cybersex child trafficking in the Philippines". Reuters. 15 April 2012.
33. ^ "Webcam slavery: tech turns Filipino families into cybersex child traffickers". Reuters. 17 June 2013.
34. ^ "How the internet fuels sexual exploitation and forced labour in Asia". South China Morning Post. 2 May 2012.
35. ^ "1st Session, 42nd Parliament, Volume 150, Issue 194". Senate of Canada. 18 April 2013.
36. ^ "Cybersex trafficking spreads across Southeast Asia, fuelled by internet boom. And the law lags behind". South China Morning Post. 11 September 2012.
37. ^ "Global Estimates of Modern Slavery Forced Labour and Forced Marriage" (PDF). International Labour Organization. Retrieved 22 December 2009.
38. ^ "Cybersex Trafficking | International Justice Mission Canada". IJM Canada. Retrieved 22 December 2009.
39. ^ "What is 'Nth Room' case and why it matters". Korea Herald. 24 April 2011.
40. ^ Murphy, Dennis (February 2010). "War is War? The utility of cyberspace operations in the contemporary operational environment" (PDF). Center for Strategic Leadership. Archived from the original (PDF) on 20 March 2012.
41. ^ Joseph, Aghatise E. (28 June 2006). "Cybercrime definition". www.crime-research.org.
42. ^ "Save browsing". google.
43. ^ Wilbur, Kenneth C.; Zhu, Yi (24 October 2008). "Click Fraud". Marketing Science. 28 (2): 293–308. doi:10.1287/mksc.1080.0397. ISSN 0732-2399.
44. ^ "Federal CyberStalking Bill Info". www.haltabuse.org. Retrieved 4 December 2012.

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

45. ^ "China has more internet users than any other country, according to Mary Meeker's Internet Trends Report". World Economic Forum. Retrieved 4 December 2012.
46. ^ "Chinese Authorities Address Online Bullying – Cybersmile". Retrieved 2 November 2012.
47. ^ "Legal Perspective – Cybersmile". Retrieved 2 November 2012.
48. ^ "Malicious Communications Act 1988". www.legislation.gov.uk. Retrieved 2 November 2012.
49. ^ "Criminal Code Act 1995". www.legislation.gov.au. Retrieved 2 November 2012.
50. ^ "U.S. internet users who have experienced online harassment 2011". Statista. Retrieved 5 April 2010.
51. ^ "All the Latest Cyber Bullying Statistics and What They Mean In 2010". BroadbandSearch.net. Retrieved 5 April 2010.
52. ^ "'I will not be silenced': Women targeted in hack-and-leak attacks speak out about spyware". NBC News. Retrieved 1 August 2010.
53. ^ "We talked to the opportunist imitator behind Silk Road 3.0". The Daily Dot. 7 November 2014. Retrieved 4 October 2015.
54. ^ Arora, Beenu. "Council Post: Five Key Reasons Dark Web Markets Are Booming". Forbes. Retrieved 23 June 2011.
55. ^ "Guide: What is Bitcoin and how does Bitcoin work? - CBBC Newsround". Retrieved 23 June 2011.
56. ^ Christian, Jon (4 February 2015). "The 'Exit Scam' Is the Darknet's Perfect Crime". Vice. Retrieved 23 June 2011.
57. ^ "The 'Exit Scam' Is the Darknet's Perfect Crime". www.vice.com. Retrieved 14 July 2011.
58. ^ Winder, Davey. "Did A Bitcoin Exit Scam Cause Dark Web Wall Street Market Crash?". Forbes. Retrieved 25 September 2010.
59. ^ Brandom, Russell (17 February 2012). "The golden age of dark web drug markets is over". The Verge. Retrieved 23 June 2011.
60. ^ Greenberg, Andy (23 September 2010). "He Escaped the Dark Web's Biggest Bust. Now He's Back". Wired. Condé Nast Publications. Archived from the original on 23 September 2010.
61. ^ "7 Ways the Cops Will Bust You on the Dark Web". www.vice.com. Retrieved 14 July 2011.
62. ^ "America's Drug Overdose Epidemic: Data to Action". Centers for Disease Control and Prevention. 24 March 2011. Retrieved 14 July 2011.
63. ^ "The Consequences of Mailing Drugs and Other Banned Substances". www.cottenfirm.com. Retrieved 23 June 2011.
64. ^ "Darknet drug vendor sentenced to 10 years prison". www.dea.gov. Retrieved 23 June 2011.
65. ^ "Feds Crack Down on Darknet Vendors of Illicit Goods". www.bankinfosecurity.com. Retrieved 14 July 2011.
66. ^ Weitzer, Ronald (2003). Current Controversies in Criminology. Upper Saddle River, New Jersey: Pearson Education Press. p. 150.
67. ^ Mann, David; Sutton, Mike (6 November 2011). ">>Netcrime". British Journal of Criminology. 38 (2): 201–229. CiteSeerX 10.1.1.133.3861. doi:10.1093/oxfordjournals.bjc.a014232.
68. ^ "A walk on the dark side". The Economist. 30 September 2007. Archived from the original on 10 November 2007. Retrieved 11 May 2011.
69. ^ "Spanish police crack massive 'zombie computer' network". France 24. 3 March 2010.
70. ^ "DHS: Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children". Dhs.gov. 3 August 2011. Retrieved 10 November 2011.
71. ^ Li, David K. (17 January 2012). "Zappos cyber attack". New York Post.
72. ^ Rodriguez, Salvador (6 June 2012). "Like LinkedIn, eHarmony is hacked; 1.5 million passwords stolen". Los Angeles Times.
73. ^ Rothacker, Rick (12 October 2012). "Cyber attacks against Wells Fargo "significant," handled well: CFO". Reuters.
74. ^ "AP Twitter Hack Falsely Claims Explosions at White House". Samantha Murphy. 23 April 2013. Retrieved 23 April 2013.
75. ^ "Fake Tweet Erasing $136 Billion Shows Markets Need Humans". Bloomberg. 23 April 2013. Retrieved 23 April 2013.
76. ^ "Unprecedented cyber attacks wreak global havoc". Straits Times. 13 May 2014.
77. ^ "Israeli spyware found on phones in 45 countries, U.S. included". The Washington Times.

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

78. ^ "Researchers find hints of Israeli spyware around globe - SFGate". Archived from the original on 24 September 2013. Retrieved 24 September 2013.
79. ^ "Your Smartphone could be running Israeli Spyware!". September 2013.
80. ^ "Phone hackers for hire: A peek into the discreet, lucrative business tapped by the FBI". 29 April 2015.
81. ^ Beaumont, Peter (26 August 2015). "Israeli firm accused of creating iPhone spyware". The Guardian.
82. ^ "Chat App ToTok Is Spy Tool For UAE – Report". Silicon UK Tech News. 27 December 2012. Retrieved 27 December 2012.
83. ^ Barnard-Wills, David; Ashenden, Debi (21 March 2012). "Securing Virtual Space: Cyber War, Cyber Terror, and Risk". Space and Culture. doi:10.1177/1206331211430016. S2CID 146501914.
84. ^ Brenner, Susan W. (2010). Cybercrime : criminal threats from cyberspace. Santa Barbara, Calif.: Praeger. ISBN 9780313365461. OCLC 464583250.
85. ^ "Facts + Statistics: Identity theft and cybercrime". Retrieved 2 December 2012.
86. ^ Zehra Ali (21 January 2013). "Mandatory Data Retention Worldwide". Retrieved 17 December 2013.
87. ^ "Archived copy" (PDF). Archived from the original (PDF) on 19 March 2015. Retrieved 23 July 2014.
88. ^ "Cyber Crime". Federal Bureau of Investigation. Retrieved 4 December 2012.
89. ^ "Combating Cyber Crime". Department of Homeland Security. 19 June 2012. Retrieved 1 November 2012.
90. ^ "NCFI - About". www.ncfi.usss.gov. Archived from the original on 31 December 2012. Retrieved 4 December 2012.
91. ^ "Investigation". www.secretservice.gov. Retrieved 3 December 2012.
92. ^ "The Importance of Understanding Encryption in Cybersecurity". Florida Tech Online. 18 August 2015. Retrieved 4 December 2012.
93. ^ "Continuous Diagnostics and Mitigation Program | CISA". www.cisa.gov.
94. ^ "Enhanced Cybersecurity Services (ECS) | CISA".
95. ^ "Enhanced Cybersecurity Services (ECS) | CISA". www.cisa.gov.
96. ^ "Detection and Prevention | CISA". www.cisa.gov. Retrieved 1 November 2012.
97. ^ "Report: 74% of security leaders say that prevention-first strategies will fail". VentureBeat. 26 April 2009. Retrieved 3 May 2009.
98. ^ Ghosemajumder, Shuman (4 December 2014). "You Can't Secure 100% of Your Data 100% of the Time". Harvard Business Review. ISSN 0017-8012. Retrieved 3 May 2009.
99. ^ Kshetri, Nir. "Diffusion and Effects of Cyber Crime in Developing Countries". Archived from the original on 18 October 2015. Retrieved 29 April 2015.
100. ^ Northam, Jackie (April 2015). "U.S. Creates First Sanctions Program Against Cybercriminals". NPR.
101. ^ Moise, Adrian Cristian (2015). "Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level" (PDF). Journal of Law and Administrative Sciences. Archived from the original (PDF) on 8 December 2015.
102. ^ "China's new cybersecurity law takes effect today". CNBC. June 2014.
103. ^ "Roads and Traffic Authority of New South Wales v Care Park Pty Limited - NSW Caselaw". NSW Caselaw. Retrieved 22 August 2010.
104. ^ "Dallas Buyers Club LLC v iiNet Limited [2015] FCA 317". Federal Court of Australia. Retrieved 22 August 2010.
105. ^ "Criminal Justice System for Adults in NYS". Retrieved 17 December 2013.
106. ^ "Managing the Risks Posed by Offender Computer Use - Perspectives" (PDF). December 2011. Archived from the original (PDF) on 5 November 2013. Retrieved 25 January 2015.
107. ^ Bowker, Art (2012). The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century. Springfield: Thomas. ISBN 9780398087289. Archived from the original on 2 April 2015. Retrieved 25 January 2015.
108. ^ "2014 Internet Crime Report" (PDF). Internet Crime Complaint Center (IC3). 2015. Retrieved 31 October 2014.
109. ^ Feinberg, T (2008). "Whether it happens at school or off-campus, cyberbullying disrupts and affects". Cyberbullying: 10.
110. ^ "Dridex: Tidal waves of spam pushing dangerous financial Trojan" (PDF). symantec.com.[failed verification]
111. ^ "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware « Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware". FireEye. Retrieved 3 January 2013.

ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 4.921| Bimonthly, Peer Reviewed & Referred Journal|

| Volume 3, Issue 4, July 2016 |

112. ^ Janofsky, Adam (19 September 2013). "How AI Can Help Stop Cyberattacks". The Wall Street Journal. ISSN 0099-9660. Retrieved 20 September 2013.
113. ^ Noyes, Katherine. "This company uses A.I. to stop cyberattacks before they start". Computerworld. Retrieved 20 September 2013.
114. ^ "Cybercrime threat response". www.interpol.int. Retrieved 17 May 2010.
115. ^ Richet, Jean-Loup (July 2013). "From Young Hackers to Crackers". International Journal of Technology and Human Interaction. 9 (3): 53–62. doi:10.4018/jthi.2013070104 – via Research Gate.
116. ^ Richet, Jean-Loup (2011). "Adoption of deviant behavior and cybercrime 'Know how' diffusion". York Deviancy Conference.
117. ^ Richet, Jean-Loup (2012). "How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime". 17th AIM Symposium.
118. ^ "ASEAN Declaration to Prevent and Combat Cybercrime". ASEAN. 14 November 2014. Archived from the original on 3 July 2010. Retrieved 5 June 2009.