Cybercrime

Cybercrime is a crime that involves a computer and a network.[1][2] The computer may have been used in the commission of a crime, or it may be the target.[3] Cybercrime may harm someone's security and financial health.[4][5]

There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental 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 "poses real risks to humanity."[7]

A report (sponsored by McAfee) published in 2014 estimated that the annual damage to the global economy was $445 billion.[8] Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.[9] In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that nearly one percent of global GDP, close to $600 billion, is lost to cybercrime each year.[10] The World Economic Forum 2020 Global Risk report confirmed that organized Cybercrimes bodies are joining forces to perpetrate criminal activities online while estimating the likelihood of their detection and prosecution to be less than 1 percent in the US.[11]

Classifications

With traditional crime reducing, global communities continue to witness a sporadic growth in cybercrime.[12] Computer crime encompasses a broad range of activities, from financial crimes to scams, through cybersex trafficking and ad frauds [13][14]

Financial fraud crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering in an unauthorized way. This requires little technical expertise and is a common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
- Altering or deleting stored data;[15]

Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crime often result in the loss of private information or monetary information.

Cyberterrorism

Government officials and information technology security specialists have documented a significant increase in Internet problems and server scams since early 2001. There is a growing concern among government agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) that such intrusions are part of an organized effort by cyberterrorist foreign intelligence services, or other groups to map potential security holes in critical systems.[16] A cyberterrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Cyberterrorism, in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda piece on the Internet that there will be bomb attacks during the holidays can be considered cyberterrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing, etc.[17]

Cyberextortion

Cyberextortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybercrime extortionists 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 public domain. Perpetrators typically use a distributed denial-of-service attack.[18] However, other cyberextortion techniques exist such as doxing extortion and bug poaching.

An example of cyberextortion was the attack on Sony Pictures of 2014.[19]

Ransomware is a kind of cyberextortion in which a malware is used to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid. Kapersky Lab 2016 Security Bulletin report estimates that a business falls victim of Ransomware every 40 minutes.[20] and predicted to attack a business every 11 minutes in 2021. With Ransomware remaining one of the fastest growing cybercrimes in the world, global Ransomware damage is predicted to cost up to $20 billion in 2021.[21]

Cybersex trafficking

Cybersex trafficking is the transportation of victims and then the live streaming of coerced sexual acts and or rape on webcam.[22][23][24][25] Victims are abducted, threatened, or deceived and transferred to 'cybersex dens.'[26][27][28] The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with internet connection.[24] Perpetrators use social media networks, videoconferences, dating pages, online chat rooms, apps, dark web sites,[29] and other platforms.[30] They use online payment systems[29][31][32] and cryptocurrencies to hide their identities.[33] Millions of reports of its occurrence are sent to authorities annually.[34] New legislation and police procedures are needed to combat this type of cybercrime.[35]

An example of cybersex trafficking is the 2018–2020 Nth room case in South Korea.[36]

Cyberwarfare

The U.S. Department of Defense notes that the cyberspace has emerged as a national-level concern through several recent events of geostrategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.[37]

Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world, in general, is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. It is seldom committed by loners, instead it involves large syndicate group.

Crimes that primarily target computer networks include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

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 likes have existed even before the development in high-tech equipment. 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.[38]

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.[39] 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.

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. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".[40]

Ad-fraud

Ad-frauds are particularly popular among cybercriminals, as such frauds are less likely to be prosecuted and are particularly lucrative cybercrimes.[41] Jean-Loup Richet, Professor at the

Sorbonne Business School, classified the large variety of ad-fraud observed in cybercriminal communities into three categories: (1) identity fraud; (2) attribution fraud; and (3) ad-fraud services.[14]

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 signals to make a bot look more legitimate, for instance by opening a Twitter or Facebook account.

Attribution fraud aims to impersonate real users' behaviors (clicks, activities, conversations, etc.). Multiple ad-fraud techniques belong to this category: hijacked devices and the use of infected users (through a 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 (that will never be viewed by real users); domain spoofing (ads served on a website other than the advertised real-time bidding website); and clickjacking (user is forced to click on the 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.

A successful ad-fraud campaign involves a sophisticated combination of these three types of ad-fraud—sending fake traffic through bots using fake social accounts and falsified cookies; bots will click on the ads available on a scam page that is faking a famous brand.

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, sexual orientation.

There are instances where 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 alone, Missouri and over 40 other 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.[42]

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.[43][44] 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.[45][46] 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.[47]

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

Cyberbullying has increased drastically with the growing popularity of online social networking. As of January 2020, 44% of adult internet users in the United States have "personally experienced online harassment."[48] Children who experience online harassment deal with negative and sometimes life-threatening side effects. In 2021, reports displayed 41% of children developing social anxiety, 37% of children developing depression, and 26% of children having suicidal thoughts.[49]

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 the 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.[50]

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. The dark web site Silk Road was a major online marketplace for drugs before it was shut down by law enforcement (then reopened under new management, and then shut down by law enforcement again). 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.[51]

Darknet markets have had an up-rise in traffic in recent years for many reasons. One of the biggest contributors being the anonymity and safety that goes along when using the markets.[52] There are numerous ways you can lose all your money invested and be caught when using Darknet markets. Vendors and customers alike go to great lengths to keep their identities a secret while online. Commonly used tools are virtual private networks, Tails, and Tor to help hide their trail left behind for investigators. Darknet markets make the user feel safe as they can get what they want from the comfort of their home. 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 isn't as simple as typing it in on the search engine like you would with google. Darknet markets have special links that are changing everyday ending in .onion opposed to the typical .com, .net. and .org domain extensions. To add to privacy the biggest currency on these markets is Bitcoin. Bitcoin allows transactions to be committed between people by exchanging wallet addresses and never having to know anything about the person you're sending money to.[53]

One of the biggest issues the users face who use marketplaces are the vendors or market itself exit scamming.[54] This is when usually a vendor with a high rating will act as if they're still selling on the market and have users send them money.[55] The vendor will then close off his account after receiving money from multiple buyers and never send what they purchased. The vendors all being involved in illegal activities have a low chance at not exit scamming when they no longer want to be a vendor. In 2019, an entire market called Wall Street Market had allegedly exit scammed, stealing 30 million dollars from the vendors and buyers wallets in bitcoin.[56]

Federal agents have had a huge crackdown on these markets. In July 2017, federal agents seized one of the biggest markets commonly called Alphabay which ironically later re-opened in August 2021 under the control of one of the original administrators DeSnake.[57][58] Commonly investigators will pose as a buyer and order packages from darknet vendors in the hopes they left a trail they can follow. One investigation had an investigator pose as a firearms seller and for six months people purchased from them and provided home addresses.[59] They were able to make over a dozen arrests during this six-month investigation.[59] Another one of law enforcement's biggest crackdowns are on vendors selling fentanyl and opiates. With thousands of people dying each year due to drug over dose it was long overdue for law enforcement to crack down on these markets.[60] Many vendors don't realize the extra 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.[61] Each state has its laws and regulations on drugs therefore vendors have the face multiple charges from different states. In 2019, a vendor was sentenced to 10 years in prison after selling cocaine and methamphetamine under the name JetSetLife.[62] Although many investigators spend a lot of time tracking down people in the course of a year only 65 suspects were identified who bought and sold illegal goods on some of the biggest markets.[63] This is compared to the thousands of transactions taking place daily on these markets.

- One of the highest profiled banking computer crime occurred during 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.[64]
- 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.[64]
- In 1983, a 19-year-old UCLA student used his PC to break into a Defense Department International Communications system.[64]

- 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.[65]
- 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 Flame (malware) that mainly targeted Iranian officials in an attempt to obtain sensitive information.[66]
- 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".[67] 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 3 men who were suspected of infecting of 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.[68]
- 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.[69]

- In January 2012 Zappos.com experienced a security breach after as many as 24 million customers' credit card numbers, personal information, billing and shipping addresses had been compromised.[70]
- 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.[71]
- December 2012 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: Bank of America, J. P. Morgan U.S. Bank, and PNC Financial Services.[72]
- 23 April 2013 saw the Associated Press' Twitter account's hacked - the hacker posted a hoax tweet about fictitious attacks in the White House that they claimed left President Obama injured.[73] This hoax tweet resulted in a brief plunge of 130 points from the Dow Jones Industrial Average, removal of $136 billion from S&P 500 index,[74] and the temporary suspension of AP's Twitter account. The Dow Jones later restored its session gains.
- In May 2017, 74 countries logged a ransomware cybercrime, called "WannaCry"[75]
- 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 being in operation in at least 46 nation-states around the world. Journalists, Royalty and government officials were amongst the targets.[76][77][78] Previous accusations of cases of Israeli-weapons companies meddling in international telephony[79] and smartphones[80] have been eclipsed in the 2018 reported case.
- In December 2019, the United States intelligence and an investigation by The New York Times revealed that messaging application of the United Arab Emirates, ToTok is a spying tool. The research revealed that the Emirati government attempted to track every conversation, movement, relationship, appointment, sound and image of those who install the app on their phones.[81]

Combating computer crime

It is difficult to find and combat cyber crime's 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. Cyber criminals can target more than one person at a time. The availability of virtual spaces[82] to public and private sectors has allowed cybercrime to become an everyday occurrence.[83] In 2018, The Internet Crime Complaint Center received 351,937 complaints of cybercrime, which lead to $2.7 billion lost.[84]

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[85] Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide Data Retention Directive (applicable to all EU member states) states 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.[86]

Senator Tommy Tuberville touring the National Computer Forensic Institute in Hoover, Alabama in 2021.

In the United States, the Federal Bureau of Investigation (FBI)[87] and the Department of Homeland Security (DHS)[88] are government agencies that combat cybercrime. The FBI has trained agents and analysts in cybercrime placed in their field offices and headquarters.[87]

Under the DHS, the Secret Service has a Cyber Intelligence Section that works to target financial cyber crimes. 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.[88][89][90] 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."[90]

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.[83][91]

Prevention

The Department of Homeland Security also instituted the Continuous Diagnostics and Mitigation (CDM) Program.[92] 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.[93] 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.[94][95]

Many cybersecurity products and technologies are used by organizations, but cybersecurity professionals have been skeptical of prevention-focused strategies.[96] 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.[97]

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 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.[98]

Then-President Barack Obama released in an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze 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.[99]

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.[100]

It is not only the US and the European Union who are introducing new measures against cybercrime. On 31 May 2017 China announced that its new cybersecurity law takes effect on this date.[101]

In Australia, common legislation in Commonwealth jurisdiction which is applied to combat against cybercrime by means of criminal offence provisions and information gathering and enforcement powers include the *Criminal Code Act 1995* (Cth), *Telecommunications Act 1997* (Cth) and *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.[102]

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.*'[103]

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.[104]

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.[105] These approaches involve restricting individuals to specific devices which are subject to computer monitoring or computer searches by probation or parole officers.[106]

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.[107] But cybercrime does yet seem to be on the average person's radar. There are 1.5 million cyber-attacks annually, that means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing us that only 16% of victims had asked the people who were carrying out the attacks to stop.[108]

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

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 group.[109] 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[110] or malicious IPs/URLs,[110] as well as strategic information profiling the goals, techniques and campaigns of the profiled groups. Some of it is freely published, but consistent, on-going access typically requires subscribing to an adversary intelligence subscription service. At the level of an individual threat actor, threat intelligence is often referred to 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.[111][112]

INTERPOL Cyber Fusion Center have begun a collaboration with cybersecurity key players to distribute information on latest online scams, cyber threats and risks to internet users. Reports cutting across social engineered frauds, ransomware, phishing, and other has since 2017 been distributed to security agencies in over 150 countries.[113]

Diffusion of cybercrime

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

Hacking has become less complex as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could 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 dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc. 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.[114] 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.[115]

Agencies

- ASEAN[116]
- Australian High Tech Crime Centre
- Cyber Crime Investigation Cell, a wing of Mumbai Police, India
- Cyber Crime Unit (Hellenic Police), formed in Greece in 1995
- EUROPOL
- INTERPOL
- National Cyber Crime Unit, in the United Kingdom
- National Security Agency, in the United States
- National White Collar Crime Center, in the United States
- Cyber Police Department - Japan National Police Agency

See also

- Computer Fraud and Abuse Act
- Computer security
- Computer trespass
- Cloud computing security
- Convention on Cybercrime
- Cybercrime countermeasures
- Cyber defamation law

- Cyber-
- Cyberheist
- Darknet
- Dark web
- Deep web
- Domain hijacking
- Electronic evidence
- (Illegal) drop catching
- Economic and industrial espionage
- FBI
- Immigration and Customs Enforcement (ICE)
- Internet homicide
- Internet suicide pact
- Legal aspects of computing
- List of computer criminals
- Metasploit Project
- National Crime Agency (NCA)
- Penetration test
- Police National E-Crime Unit
- Protected computer
- Techno-thriller
- Trespass to chattels
- United States Secret Service
- Virtual crime
- White-collar crime
- Web shell

References

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
2. "cybercrime | Definition, Statistics, & Examples" (https://www.britannica.com/topic/cybercrime) . Encyclopedia Britannica. Retrieved 25 May 2021.
3. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials (https://archive.org/details/computerforensic0000krus) . Addison-Wesley. p. 392 (https://archive.org/details/computerforensic0000krus/page/392) . ISBN 978-0-201-70719-9.
4. Bossler, Adam M.; Berenblum, Tamar (20 October 2019). "Introduction: new directions in cybercrime research" (https://doi.org/10.1080%2F0735648X.2019.1692426) . Journal of Crime and Justice. **42** (5): 495–499. doi:10.1080/0735648X.2019.1692426 (https://doi.org/10.1080%2F0735648X.2019.1692426) . ISSN 0735-648X (https://www.worldcat.org/issn/0735-648X) .
5. "cybercrime | Definition, Statistics, & Examples | Britannica" (https://www.britannica.com/topic/cybercrime) . www.britannica.com. Retrieved 14 December 2021.
6. "BUFFETT: This is 'the number one problem with mankind' " (https://www.businessinsider.in/buffett-this-is-the-number-one-problem-with-mankind/articleshow/58555300.cms) . Business Insider. Retrieved 17 May 2021.
7. "Warren Buffett: 'Cyber poses real risks to humanity' " (https://finance.yahoo.com/news/warren-buffett-cyber-attacks-131445079.html) . finance.yahoo.com. Retrieved 17 May 2021.
8. "Cyber crime costs global economy $445 billion a year: report" (https://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609) . Reuters. 9 June 2014. Retrieved 17 June 2014.
9. "#Cybercrime— what are the costs to victims - North Denver News" (http://northdenvernews.com/cybercrime-costs-victims/) . North Denver News. 17 January 2015. Retrieved 16 May 2015.
10. Lewis, James (February 2018). "Economic Impact of Cybercrime - No Slowing Down" (https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf) (PDF).
11. "The Global Risk Report 2020" (http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf) (PDF). World Economic Forum. 15th Edition: 102. 15 January 2020.
12. Netherlands, Statistics. "Less traditional crime, more cybercrime" (https://www.cbs.nl/en-gb/news/2020/10/less-traditional-crime-more-cybercrime) . Statistics Netherlands. Retrieved 17 May 2021.
13. 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 (https://doi.org/10.1007%2Fs11416-006-0015-z) . S2CID 3334277 (https://api.semanticscholar.org/CorpusID:3334277) .

14. Richet, Jean-Loup (1 January 2022). "How cybercriminal communities grow and change: An investigation of ad-fraud communities" (https://www.sciencedirect.com/science/article/pii/S0040162521007162) . Technological Forecasting and Social Change. **174** (121282): 121282. doi:10.1016/j.techfore.2021.121282 (https://doi.org/10.1016%2Fj.techfore.2021.121282) . ISSN 0040-1625 (https://www.worldcat.org/issn/0040-1625) . S2CID 239962449 (https://api.semanticscholar.org/CorpusID:239962449) .

15. "Computer and Internet Fraud" (https://www.law.cornell.edu/wex/computer_and_internet_fraud) . LII / Legal Information Institute. Retrieved 1 November 2020.

16. Laqueur, Walter; C., Smith; Spector, Michael (2002). Cyberterrorism (https://books.google.com/books?id=H7fT0BQxwDsC&pg=PA49) . Facts on File. pp. 52–53. ISBN 9781438110196.

17. "Cybercriminals Need Shopping Money in 2017, too! - SentinelOne" (https://sentinelone.com/blogs/cybercriminals-need-shopping-money-holidays/) . sentinelone.com. 28 December 2016. Retrieved 24 March 2017.

18. Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (https://web.archive.org/web/20110706175959/http://www.ere-security.ca/PDF/Cyberextortion%20by%20DoS%2C%20Risk%20Magazine%20June%202006.pdf) (PDF). Archived from the original (http://www.ere-security.ca/PDF/Cyberextortion%20by%20DoS,%20Risk%20Magazine%20June%202006.pdf) (PDF) on 6 July 2011.

19. Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion" (https://web.archive.org/web/20150925133121/http://www.cyphort.com/latest-sony-pictures-breach-deadly-cyber-extortion/) . Archived from the original (http://www.cyphort.com/latest-sony-pictures-breach-deadly-cyber-extortion/) on 25 September 2015. Retrieved 20 September 2015.

20. "Kaspersky Security Bulletin 2016. The ransomware revolution" (https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/) . securelist.com. Retrieved 17 May 2021.

21. "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021" (https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/) . Cybercrime Magazine. 19 October 2018. Retrieved 17 May 2021.

22. Carback, Joshua T. (2018). "Cybersex Trafficking: Toward a More Effective Prosecutorial Response". Criminal Law Bulletin. **54** (1): 64–183. p. 64.

23. "IJM Seeks to End Cybersex Trafficking of Children and #RestartFreedom this Cyber Monday and Giving Tuesday" (https://www.prnewswire.com/news-releases/ijm-seeks-to-end-cybersex-trafficking-of-children-and-restartfreedom-this-cyber-monday-and-giving-tuesday-300368744.html) . PR Newswire. 28 November 2016.

24. "Cybersex Trafficking" (https://www.ijmuk.org/our-work/cybersex-trafficking) . IJM. 2020.

25. "Cyber-sex trafficking: A 21st century scourge" (https://www.cnn.com/2013/07/17/world/asia/philippines-cybersex-trafficking/index.html) . CNN. 18 July 2013.

26. "Senator warns of possible surge in child cybersex traffic" (https://www.philstar.com/headlines/2020/04/13/2006955/senator-warns-possible-surge-child-cybersex-traffic) . The Philippine Star. 13 April 2020.

27. "Duterte's drug war and child cybersex trafficking" (https://theaseanpost.com/article/dutertes-drug-war-and-child-cybersex-trafficking) . The ASEAN Post. 18 October 2019.

28. "Norwegian national, partner nabbed; 4 rescued from cybersex den" (https://news.mb.com.ph/2020/05/01/norwegian-national-partner-nabbed-4-rescued-from-cybersex-den/) . Manila Bulletin. 1 May 2020.

29. "Cheap tech and widespread internet access fuel rise in cybersex trafficking" (https://www.nbcnews.com/tech/tech-news/cheap-tech-widespread-internet-access-fuel-rise-cybersex-trafficking-n886886) . NBC News. 30 June 2018.

30. "Senate to probe rise in child cybersex trafficking" (https://www.philstar.com/headlines/2019/11/11/1967750/senate-probe-rise-child-cybersex-trafficking) . The Philippine Star. 11 November 2019.

31. "Global taskforce tackles cybersex child trafficking in the Philippines" (https://www.reuters.com/article/us-philippines-trafficking-children/global-taskforce-tackles-cybersex-child-trafficking-in-the-philippines-idUSKCN1RR1D1) . Reuters. 15 April 2019.

32. "Webcam slavery: tech turns Filipino families into cybersex child traffickers" (https://www.reuters.com/article/us-philippines-trafficking-technology/webcam-slavery-tech-turns-filipino-families-into-cybersex-child-traffickers-idUSKBN1JE00X) . Reuters. 17 June 2018.

33. "How the internet fuels sexual exploitation and forced labour in Asia" (https://www.scmp.com/comment/insight-opinion/article/3008403/how-internet-fuels-sexual-exploitation-and-forced-labour) . South China Morning Post. 2 May 2019.

34. "1st Session, 42nd Parliament, Volume 150, Issue 194" (https://sencanada.ca/en/content/sen/chamber/421/debates/194db_2018-04-18-e) . Senate of Canada. 18 April 2018.

35. "Cybersex trafficking spreads across Southeast Asia, fuelled by internet boom. And the law lags behind" (https://www.scmp.com/news/asia/southeast-asia/article/3026664/how-cambodias-outdated-laws-make-it-harder-tackle-cybersex) . South China Morning Post. 11 September 2019.

36. "What is 'Nth Room' case and why it matters" (http://www.koreaherald.com/view.php?ud=20200424000512) . Korea Herald. 24 April 2020.

37. Dennis Murphy (February 2010). "War is War? The utility of cyberspace operations in the contemporary operational environment" (https://web.archive.org/web/20120320012856/http://www.carlisle.army.mil/DIME/documents/War%20is%20War%20Issue%20Paper%20Final2.pdf) (PDF). Center for Strategic Leadership. Archived from the original (http://www.carlisle.army.mil/DIME/documents/War%20is%20War%20Issue%20Paper%20Final2.pdf) (PDF) on 20 March 2012.

38. Joseph, Aghatise E. (28 June 2006). "Cybercrime definition" (http://www.crime-research.org/articles/joseph06/) . www.crime-research.org.

39. "Save browsing" (http://googleonlinesecurity.blogspot.jp/2012/06/safe-browsing-protecting-web-users-for.html) . google.

40. * Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. (https://www.igi-global.com/book/cyber-crime-victimization-women/50518) Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

41. Wilbur, Kenneth C.; Zhu, Yi (24 October 2008). "Click Fraud" (https://pubsonline.informs.org/doi/abs/10.1287/mksc.1080.0397) . Marketing Science. **28** (2): 293–308. doi:10.1287/mksc.1080.0397 (https://doi.org/10.1287%2Fmksc.1080.0397) . ISSN 0732-2399 (https://www.worldcat.org/issn/0732-2399) .

42. "Federal CyberStalking Bill Info" (http://www.haltabuse.org/resources/laws/federal.shtml) . www.haltabuse.org. Retrieved 4 December 2019.

43. "China has more internet users than any other country, according to Mary Meeker's Internet Trends Report" (https://www.weforum.org/agenda/2019/06/most-people-on-the-internet-live-in-this-country/) . World Economic Forum. Retrieved 4 December 2019.

44. Solutions, Madison Web. "Chinese Authorities Address Online Bullying – Cybersmile" (https://www.cybersmile.org/news/chinese-authorities-address-online-bullying) . Retrieved 2 November 2019.

45. Solutions, Madison Web. "Legal Perspective – Cybersmile" (https://www.cybersmile.org/advice-help/category/cyberbullying-and-the-law) . Retrieved 2 November 2019.

46. Participation, Expert. "Malicious Communications Act 1988" (http://www.legislation.gov.uk/ukpga/1988/27/section/1/data.htm) . www.legislation.gov.uk. Retrieved 2 November 2019.

47. AG. "Criminal Code Act 1995" (http://www.legislation.gov.au/Details/C2019C00043/Html/Volume_1) . www.legislation.gov.au. Retrieved 2 November 2019.

48. "U.S. internet users who have experienced online harassment 2020" (https://www.statista.com/statistics/333942/us-internet-online-harassment-severity/) . Statista. Retrieved 5 April 2021.

49. "All the Latest Cyber Bullying Statistics and What They Mean In 2021" (https://www.broadbandsearch.net/blog/cyber-bullying-statistics) . BroadbandSearch.net. Retrieved 5 April 2021.

50. " 'I will not be silenced': Women targeted in hack-and-leak attacks speak out about spyware" (https://www.nbcnews.com/tech/social-media/i-will-not-be-silenced-women-targeted-hack-leak-attacks-n1275540) . NBC News. Retrieved 1 August 2021.

51. "We talked to the opportunist imitator behind Silk Road 3.0" (http://www.dailydot.com/layer8/silk-road-3-blake-benthall/) . The Daily Dot. 7 November 2014. Retrieved 4 October 2016.

52. Arora, Beenu. "Council Post: Five Key Reasons Dark Web Markets Are Booming" (https://www.forbes.com/sites/forbestechcouncil/2020/04/23/five-key-reasons-dark-web-markets-are-booming/) . Forbes. Retrieved 23 June 2020.

53. "Guide: What is Bitcoin and how does Bitcoin work? - CBBC Newsround" (https://www.bbc.co.uk/newsround/25622442) . Retrieved 23 June 2020.

54. Christian, Jon (4 February 2015). "The 'Exit Scam' Is the Darknet's Perfect Crime" (https://www.vice.com/en_us/article/xyw7xn/darknet-slang-watch-exit-scam) . Vice. Retrieved 23 June 2020.

55. "The 'Exit Scam' Is the Darknet's Perfect Crime" (https://www.vice.com/en_us/article/xyw7xn/darknet-slang-watch-exit-scam) . www.vice.com. Retrieved 14 July 2020.

56. Winder, Davey. "Did A Bitcoin Exit Scam Cause Dark Web Wall Street Market Crash?" (https://www.forbes.com/sites/daveywinder/2019/05/03/did-a-bitcoin-exit-scam-cause-dark-web-wall-street-market-crash/) . Forbes. Retrieved 25 September 2021.

57. Brandom, Russell (17 February 2019). "The golden age of dark web drug markets is over" (https://www.theverge.com/2019/2/17/18226718/alphabay-takedown-drug-marketplace-federal-arrest) . The Verge. Retrieved 23 June 2020.

58. Greenberg, Andy (23 September 2021). "He Escaped the Dark Web's Biggest Bust. Now He's Back" (https://www.wired.com/story/alphabay-desnake-dark-web-interview/) . Wired. Condé Nast Publications. Archived (https://web.archive.org/web/20210923132523/https://www.wired.com/story/alphabay-desnake-dark-web-interview/) from the original on 23 September 2021.

59. "7 Ways the Cops Will Bust You on the Dark Web" (https://www.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web) . www.vice.com. Retrieved 14 July 2020.

60. CDC (24 March 2020). "America's Drug Overdose Epidemic: Data to Action" (https://www.cdc.gov/injury/features/prescription-drug-overdose/index.html) . Centers for Disease Control and Prevention. Retrieved 14 July 2020.

61. "The Consequences of Mailing Drugs and Other Banned Substances" (https://www.cottenfirm.com/blog/2019/september/the-consequences-of-mailing-drugs-and-other-bann/) . www.cottenfirm.com. Retrieved 23 June 2020.

62. "Darknet drug vendor sentenced to 10 years prison" (https://www.dea.gov/press-releases/2019/04/12/darknet-drug-vendor-sentenced-10-years-prison) . www.dea.gov. Retrieved 23 June 2020.

63. "Feds Crack Down on Darknet Vendors of Illicit Goods" (https://www.bankinfosecurity.com/feds-crack-down-on-darknet-vendors-illicit-goods-a-11145) . www.bankinfosecurity.com. Retrieved 14 July 2020.

64. Weitzer, Ronald (2003). Current Controversies in Criminology. Upper Saddle River, New Jersey: Pearson Education Press. p. 150.

65. David Mann And Mike Sutton (6 November 2011). ">>Netcrime". British Journal of Criminology. **38** (2): 201–229. CiteSeerX 10.1.1.133.3861 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.133.3861) . doi:10.1093/oxfordjournals.bjc.a014232 (https://doi.org/10.1093%2Foxfordjournals.bjc.a014232) .

66. Aaron Gershwin (26 June 2019). "Flame: The Most Sophisticated Cyber Espionage Tool Ever Made" (https://hackernoon.com/flame-the-most-sophisticated-cyber-espionage-tool-ever-made-45f24e41cc16) . hackernoon.com. Retrieved 1 July 2019.

67. "A walk on the dark side" (https://web.archive.org/web/20071110134626/http://economist.com/displaystory.cfm?story_id=9723768) . The Economist. 30 September 2007. Archived from the original (http://economist.com/displaystory.cfm?story_id=9723768) on 10 November 2007. Retrieved 11 May 2011.

68. "Spanish police crack massive 'zombie computer' network" (https://www.france24.com/en/20100303-spanish-police-crack-massive-zombie-computer-network) . France 24. 3 March 2010.

69. "DHS: Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children" (https://www.dhs.gov/ynews/releases/20110803-napolitano-holder-announce-largest-prosecution-criminal-network.shtm) . Dhs.gov. 3 August 2011. Retrieved 10 November 2011.

70. DAVID K. LI (17 January 2012). "Zappos cyber attack" (http://www.nypost.com/p/news/national/zappos_cyber_attack_pWsrU60crm8SGHJWYGuP7K) . New York Post.

71. Salvador Rodriguez (6 June 2012). "Like LinkedIn, eHarmony is hacked; 1.5 million passwords stolen" (https://articles.latimes.com/2012/jun/06/business/la-fi-tn-eharmony-hacked-linkedin-20120606) . Los Angeles Times.

72. Rick Rothacker (12 October 2012). "Cyber attacks against Wells Fargo "significant," handled well: CFO" (https://www.reuters.com/article/net-us-wellsfargo-cyberattacks-idUSBRE89B1C620121012) . Reuters.

73. "AP Twitter Hack Falsely Claims Explosions at White House" (http://mashable.com/2013/04/23/ap-hacked-white-house/) . Samantha Murphy. 23 April 2013. Retrieved 23 April 2013.

74. "Fake Tweet Erasing $136 Billion Shows Markets Need Humans" (https://www.bloomberg.com/news/2013-04-23/fake-report-erasing-136-billion-shows-market-s-fragility.html) . Bloomberg. 23 April 2013. Retrieved 23 April 2013.

75. "Unprecedented cyber attacks wreak global havoc" (http://www.straitstimes.com/world/europe/unprecedented-cyberattacks-wreak-global-havoc) . Straits Times. 13 May 2017.

76. "Israeli spyware found on phones in 45 countries, U.S. included" (https://www.washingtontimes.com/news/2018/sep/18/israeli-spyware-found-phones-45-countries-us-inclu/) . The Washington Times.

77. "Archived copy" (https://web.archive.org/web/20180924105848/https://www.sfgate.com/business/technology/article/Researchers-find-hints-of-Israeli-spyware-around-13237819.php) . Archived from the original (https://www.sfgate.com/business/technology/article/Researchers-find-hints-of-Israeli-spyware-around-13237819.php) on 24 September 2018. Retrieved 24 September 2018.

78. "Your Smartphone could be running Israeli Spyware!" (https://www.siasat.com/news/smartphone-or-israeli-spywarehow-safe-your-smartphone-1400791/) . September 2018.

79. "Phone hackers for hire: A peek into the discreet, lucrative business tapped by the FBI" (https://www.pcworld.com/article/3062396/security/phone-hackers-for-hire-a-peek-into-the-discreet-lucrative-business-tapped-by-the-fbi.html) . 29 April 2016.

80. Beaumont, Peter (26 August 2016). "Israeli firm accused of creating iPhone spyware" (https://www.theguardian.com/world/2016/aug/26/israeli-firm-accused-of-creating-iphone-spyware) . The Guardian.

81. "Chat App ToTok Is Spy Tool For UAE – Report" (https://www.silicon.co.uk/mobility/mobile-apps/totok-spy-tool-for-uae-325873) . Silicon UK Tech News. 27 December 2019. Retrieved 27 December 2019.

82. Barnard-Wills, David; Ashenden, Debi (21 March 2012). "Securing Virtual Space: Cyber War, Cyber Terror, and Risk". Space and Culture. doi:10.1177/1206331211430016 (https://doi.org/10.1177%2F1206331211430016) . S2CID 146501914 (https://api.semanticscholar.org/CorpusID:146501914) .

83. Brenner, Susan W., 1947- (2010). Cybercrime : criminal threats from cyberspace. Santa Barbara, Calif.: Praeger. ISBN 9780313365461. OCLC 464583250 (https://www.worldcat.org/oclc/464583250) .

84. "Facts + Statistics: Identity theft and cybercrime" (https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime) . Retrieved 2 December 2019.

85. Zehra Ali (21 January 2018). "Mandatory Data Retention Worldwide" (https://www.privacyend.com/mandatory-data-retention/) . Retrieved 17 December 2018.

86. "Archived copy" (https://web.archive.org/web/20150319194419/http://www.unafei.or.jp/english/pdf/RS_No79/No79_15RC_Group2.pdf) (PDF). Archived from the original (http://www.unafei.or.jp/english/pdf/RS_No79/No79_15RC_Group2.pdf) (PDF) on 19 March 2015. Retrieved 23 July 2017.

87. "Cyber Crime" (https://www.fbi.gov/investigate/cyber) . Federal Bureau of Investigation. Retrieved 4 December 2019.

88. "Combating Cyber Crime" (https://www.dhs.gov/cisa/combating-cyber-crime) . Department of Homeland Security. 19 June 2012. Retrieved 1 November 2019.

89. "NCFI - About" (https://web.archive.org/web/20191231015231/https://www.ncfi.usss.gov/ncfi/pages/about.xhtml?dswid=-4902) . www.ncfi.usss.gov. Archived from the original (https://www.ncfi.usss.gov/ncfi/pages/about.xhtml?dswid=-4902) on 31 December 2019. Retrieved 4 December 2019.

90. "Investigation" (https://www.secretservice.gov/investigation/) . www.secretservice.gov. Retrieved 3 December 2019.

91. "The Importance of Understanding Encryption in Cybersecurity" (https://www.floridatechonline.com/blog/information-technology/the-importance-of-understanding-encryption-in-cybersecurity/) . Florida Tech Online. 18 August 2016. Retrieved 4 December 2019.

92. "Continuous Diagnostics and Mitigation Program | CISA" (https://www.cisa.gov/cdm) . www.cisa.gov.

93. "Enhanced Cybersecurity Services (ECS) | CISA" (https://www.cisa.gov/enhanced-cybersecurity-services-ecs) .

94. "Enhanced Cybersecurity Services (ECS) | CISA" (https://www.cisa.gov/enhanced-cybersecurity-services-ecs#) . www.cisa.gov.

95. "Detection and Prevention | CISA" (https://www.cisa.gov/detection-and-prevention) . www.cisa.gov. Retrieved 1 November 2019.

96. "Report: 74% of security leaders say that prevention-first strategies will fail" (https://venturebeat.com/2022/04/26/report-74-of-security-leaders-say-that-prevention-first-strategies-will-fail/) . VentureBeat. 26 April 2022. Retrieved 3 May 2022.

97. Ghosemajumder, Shuman (4 December 2017). "You Can't Secure 100% of Your Data 100% of the Time" (https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time) . Harvard Business Review. ISSN 0017-8012 (https://www.worldcat.org/issn/0017-8012) . Retrieved 3 May 2022.

98. Kshetri, Nir. "Diffusion and Effects of Cyber Crime in Developing Countries" (https://web.archive.org/web/20151018103250/http://web.a.ebscohost.com/ehost/detail/detail?vid=3&sid=21efdb54-ad43-447f-ab46-ce7fa854a98f%40sessionmgr4003&hid=4109&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=buh&AN=55328703/) . Archived from the original (http://web.a.ebscohost.com/ehost/detail/detail?vid=3&sid=21efdb54-ad43-447f-ab46-ce7fa854a98f%40sessionmgr4003&hid=4109&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=buh&AN=55328703/) on 18 October 2015. Retrieved 29 April 2015.

99. Northam, Jackie (April 2015). "U.S. Creates First Sanctions Program Against Cybercriminals" (https://www.npr.org/blogs/thetwo-way/2015/04/01/396811276/u-s-creates-first-sanctions-program-against-cybercriminals/) . NPR.

100. Adrian Cristian MOISE (2015). "Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level" (https://web.archive.org/web/20151208231600/http://jolas.ro/wp-content/uploads/2015/07/jolas_sia38.pdf) (PDF). Journal of Law and Administrative Sciences. Archived from the original (http://jolas.ro/wp-content/uploads/2015/07/jolas_sia38.pdf) (PDF) on 8 December 2015.

101. "China's new cybersecurity law takes effect today" (https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html) . CNBC. June 2017.

102. "Roads and Traffic Authority of New South Wales v Care Park Pty Limited - NSW Caselaw" (https://www.caselaw.nsw.gov.au/decision/54a636e23004de94513d959b) . NSW Caselaw. Retrieved 22 August 2021.

103. "Dallas Buyers Club LLC v iiNet Limited [2015] FCA 317" (https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2015/2015fca0317) . Federal Court of Australia. Retrieved 22 August 2021.

104. OMH. "Criminal Justice System for Adults in NYS" (https://www.omh.ny.gov/omhweb/forensic/manual/html/chapter1.htm) . Retrieved 17 December 2018.

105. "Managing the Risks Posed by Offender Computer Use - Perspectives" (https://web.archive.org/web/20131105202421/http://appaweb.csg.org/Perspectives/Perspectives_V35_N4_P40.pdf) (PDF). December 2011. Archived from the original (http://appaweb.csg.org/Perspectives/Perspectives_V35_N4_P40.pdf) (PDF) on 5 November 2013. Retrieved 25 January 2015.

106. Bowker, Art (2012). The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century (https://web.archive.org/web/20150402094342/http://www.ccthomas.com/details.cfm?P_ISBN13=9780398087289) . Springfield: Thomas. ISBN 9780398087289. Archived from the original (http://www.ccthomas.com/details.cfm?P_ISBN13=9780398087289) on 2 April 2015. Retrieved 25 January 2015.

107. "2014 Internet Crime Report" (https://pdf.ic3.gov/2014_IC3Report.pdf) (PDF). Internet Crime Complaint Center (IC3). 2015. Retrieved 31 October 2017.

108. Feinberg, T (2008). "Whether it happens at school or off-campus, cyberbullying disrupts and affects". Cyberbullying: 10.

109. "Dridex: Tidal waves of spam pushing dangerous financial Trojan" (https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/dridex-financial-trojan-16-en.pdf) (PDF). symantec.com.

110. "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" (https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html) . FireEye. Retrieved 3 January 2018.

111. Janofsky, Adam (19 September 2018). "How AI Can Help Stop Cyberattacks" (https://www.wsj.com/articles/how-ai-can-help-stop-cyberattacks-1537322940) . The Wall Street Journal. ISSN 0099-9660 (https://www.worldcat.org/issn/0099-9660) . Retrieved 20 September 2018.

112. Noyes, Katherine. "This company uses A.I. to stop cyber attacks before they start" (https://www.computerworld.com/article/3081326/security/this-company-uses-ai-to-stop-cyberattacks-before-they-start.html) . Computerworld. Retrieved 20 September 2018.

113. "Cybercrime threat response" (https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-threat-response) . www.interpol.int. Retrieved 17 May 2021.

114. Richet, Jean-Loup (2011). "Adoption of deviant behavior and cybercrime 'Know how' diffusion". York Deviancy Conference.

115. Richet, Jean-Loup (2012). "How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime". 17th AIM Symposium.

116. *"ASEAN Declaration to Prevent and Combat Cybercrime" (https://web.archive.org/web/20210703044553/https://asean.org/asean-declaration-prevent-combat-cybercrime/) . ASEAN. 14 November 2017. Archived from the original (https://asean.org/asean-declaration-prevent-combat-cybercrime/) on 3 July 2021. Retrieved 5 June 2022.*

Further reading

- Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (2006) (eds) *Cybercrime: Digital Cops in a Networked Environment*, New York University Press, New York.
- Bowker, Art (2012) "The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century" Charles C. Thomas Publishers, Ltd. Springfield.
- Brenner, S. (2007) *Law in an Era of Smart Technology,* Oxford: Oxford University Press
- Broadhurst, R., and Chang, Lennon Y.C. (2013) "Cybercrime in Asia: trends and challenges (https://link.springer.com/chapter/10.1007%2F978-1-4614-5218-8_4#page-1) ", in B. Hebenton, SY Shou, & J. Liu (eds), Asian Handbook of Criminology (pp. 49–64). New York: Springer (ISBN 978-1-4614-5217-1)
- Chang, L.Y. C. (2012) *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait (http://www.e-elgar.com/shop/cybercrime-in-the-greater-china-region?___website=uk_warehouse)* . Cheltenham: Edward Elgar. (ISBN 978-0-85793-667-7)
- Chang, Lennon Y.C., & Grabosky, P. (2014) "Cybercrime and establishing a secure cyber world (https://link.springer.com/chapter/10.1007%2F978-1-349-67284-4_15#page-1) ", in M. Gill (ed) Handbook of Security (pp. 321–339). NY: Palgrave.
- Csonka P. (2000) Internet Crime; the Draft council of Europe convention on cyber-crime: A response to the challenge of crime in the age of the internet? *Computer Law & Security Report* Vol.16 no.5.
- Easttom, C. (2010) *Computer Crime Investigation and the Law*
- Fafinski, S. (2009) *Computer Misuse: Response, regulation and the law* Cullompton: Willan
- Glenny, M. *DarkMarket : cyberthieves, cybercops, and you* (https://archive.org/details/darkmarketcybert0000glen) , New York, NY : Alfred A. Knopf, 2011. ISBN 978-0-307-59293-4
- Grabosky, P. (2006) *Electronic Crime,* New Jersey: Prentice Hall
- Halder, D., & Jaishankar, K. (2016). Cyber Crimes against Women in India (https://us.sagepub.com/en-us/nam/cyber-crimes-against-women-in-india/book253900) . New Delhi: SAGE

Publishing. ISBN 978-9385985775.

- Halder, D., & Jaishankar, K. (2011) Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. (http://www.igi-global.com/book/cyber-crime-victimization-women/51518) Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
- Jaishankar, K. (Ed.) (2011). Cyber Criminology: Exploring Internet Crimes and Criminal behavior. (https://books.google.com/books?id=cWOQWx4QPFYC) Boca Raton, FL, USA: CRC Press, Taylor, and Francis Group.
- McQuade, S. (2006) *Understanding and Managing Cybercrime,* Boston: Allyn & Bacon.
- McQuade, S. (ed) (2009) *The Encyclopedia of Cybercrime,* Westport, CT: Greenwood Press.
- Parker D (1983) *Fighting Computer Crime,* U.S.: Charles Scribner's Sons.
- Pattavina, A. (ed) *Information Technology and the Criminal Justice System,* Thousand Oaks, CA: Sage.
- Paul Taylor (1999). *Hackers: Crime in the Digital Sublime* (3 November 1999 ed.). Routledge; 1 edition. p. 200. ISBN 978-0-415-18072-6.
- Richet, J.L. (2013) From Young Hackers to Crackers, *International Journal of Technology and Human Interaction (IJTHI)*, 9(3), 53–62.
- Richet, J.L. (2022). "How cybercriminal communities grow and change: An investigation of ad-fraud communities" (https://www.sciencedirect.com/science/article/pii/S0040162521007162) . *Technological Forecasting and Social Change*. **174** (121282): 121282. doi:10.1016/j.techfore.2021.121282 (https://doi.org/10.1016%2Fj.techfore.2021.121282) . ISSN 0040-1625 (https://www.worldcat.org/issn/0040-1625) . S2CID 239962449 (https://api.semanticscholar.org/CorpusID:239962449) .
- Robertson, J. (2 March 2010). Authorities bust 3 in infection of 13m computers. Retrieved 26 March 2010, from Boston News: Boston.com (https://www.boston.com/business/technology/articles/2010/03/02/authorities_bust_3_in_infection_of_13m_computers/)
- Rolón, D. N. Control, vigilancia y respuesta penal en el ciberespacio (http://de.scribd.com/doc/215756732/Dario-N-Rolon-Vigilancia-informatica-y-responsabilidad-penal-de-proveedores-de-internet) , Latin American's New Security Thinking, Clacso, 2014, pp. 167/182
- Walden, I. (2007) *Computer Crimes and Digital Investigations,* Oxford: Oxford University Press.
- Wall, D.S. (2007) *Cybercrimes: The transformation of crime in the information age,* Cambridge: Polity.

- Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online*, Routledge, London.
- Yar, M. (2006) *Cybercrime and Society*, London: Sage.

External links

Wikimedia Commons has media related to ***Cybercrime***.

The Wikibook *The Computer Revolution* has a page on the topic of: ***Computer Crime***

- International Journal of Cyber Criminology (http://www.cybercrimejournal.com)
- Common types of cyber attacks (https://www.ibm.com/services/business-continuity/cyber-attack)
- Countering ransomware attacks (https://www.ibm.com/services/business-continuity/ransomware-attack)

Government resources

- Cybercrime.gov (http://www.cybercrime.gov/) from the United States Department of Justice
- National Institute of Justice Electronic Crime Program (https://web.archive.org/web/20100528122405/http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/welcome.htm) from the United States Department of Justice
- FBI Cyber Investigators home page (https://web.archive.org/web/20161217213634/https://www2.fbi.gov/cyberinvest/cyberhome.htm)
- US Secret Service Computer Fraud (https://web.archive.org/web/20080608160657/http://www.ustreas.gov/usss/financial_crimes.shtml#Computer)
- Australian High Tech Crime Centre (https://web.archive.org/web/20041118085257/http://www.ahtcc.gov.au/)
- UK National Cyber Crime Unit (https://web.archive.org/web/20131014171419/http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit) from the National Crime Agency

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cybercrime&oldid=1102696408"

Last edited 8 days ago by Migfab008