Vanessa Martin

May 4, 2017

Professor McCabe

Cyber Crime

The Internet has allowed criminal activity to occur without the perpetrators having to physically interact with another party. More than half of the world's population uses the Internet which allows people that participate in illegal activity to have a wide selection of people to target. Cyber crime "a crime that has some kind of computer or cyber aspect to it.(Symantec)" Crime meaning "an illegal act for which someone can be punished by the government (Merriam-Webster)" These crimes include drug trafficking, prostitution, fraud and intellectual property theft. Many of these crimes that appear virtually have existed as physical events and adapted to the digital format. The Internet is also used for terrorist acts and there is the possibility for a cyber war. The Internet has afforded ordinary people to perform criminal acts across borders and on a global scale. Digital crimes are becoming increasingly more complex because the Internet is not bounded by geography or location.Cyber criminals are motivated by a number of reasons such as financial gain, fame amongst their peers or to make a political statement. To combat cyber crime many nations have organizations dedicated to protect their citizens as well as themselves from being targeted by people with malicious intentions.

The Internet altered the structure of the illegal drug trade because it permits drugs to be sold with discretion. Those who indulge in illegal substances are no longer limited to conducting transactions on the street where risk being caught by police, receiving low quality product or being robbed. People are enabled by the Internet to purchase almost any illicit substance that exists from any Internet enabled computer device. Suppliers of illegal substances also benefit from the Internet because they are able to reach a larger pool of potential customers as well as conceal their identity. Several “underground” online drug marketplaces have operated, however Silk Road (now defunct) was the most notorious.

Silk Road was similar to the legal online marketplace Ebay where customers can leave merchants public reviews and feedback regarding the product. The supplier can interact with customers to answer questions regarding shipping time, payment and establish relationships with clientele. Silk Road was located on the Deep Web which allowed the website to operate without interference with law enforcement until it’s dissolution. The Deep Web is home to a portion websites that are not indexed by mainstream search engines like Google and Bing. To gain access into websites located in the Deep Web one has to use a browser called TOR. “The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.(Tor Project)” Tor complicates pinpointing one's IP address which is an identification number for computers with Internet access. One can figure out the physical location of a computer given an IP address.

To purchase substances via Silk Road and other online marketplaces where illegal goods and services are sold customers often use a form of digital currency called Bitcoin. Bitcoin has “real world” value meaning it can do everything conventional currency can do such as buy and sell goods and transfer money to other parties (Antonopoulos). Bitcoin is different than conventional currency in that it only exists virtually as there is no physical object that determines the value of Bitcoin. Bitcoin is useful for Internet transactions in general because it is fast, secure and is “borderless.” There is no central organization that grants Bitcoins, Bitcoins are distributed peer-2-peer. Bitcoin transactions are “pseudo-anonymous” because although each transaction is recorded to prevent counterfeiting and fraud, the transactions are not tied to any addresses that are linked to a person’s identity.

Similar to the illegal drug trade, prostitution is a another crime that now occupies digital space more than physical. The FBI defines prostitution as “the unlawful promotion of or participation in sexual activities for profit. (Holt)” The Internet allows people to perform erotic labor in the virtual space (webcam pornography) and in the physical space (prostitution). The Internet has reshaped the business practices and experiences of sex workers because they have more autonomy in how they advertise, the type of clients they see as well as schedule and wages. Pimps, brothels, strip clubs and other physical interactions are not needed to solicit customers. Because the Internet affords sex workers better labor conditions more people want to become a part of the sex trade there is increased interest amongst across social and economic classes (Jones). People that would be considered upstanding citizens are more likely in participating in erotic labor for profit because the barriers to entry are low (Holt). The wages of prostitutes that solicit online are higher than the wages of street prostitutes by 20% which suggests that the services of online prostitutes are in demand (Holt). Sex workers are also able to select clients with higher incomes.

Similar to online drug marketplaces the websites that fuel the online sex industry employ Web 2.0 technologies such as message boards and forums where sex workers and their potential clients can interact directly without meeting physically. Web 2.0 technologies refer to "Internet based communications that feature a high degree of user interactivity and the generation of mediated content by those same users. (Yar)" Clients are able to build a reputation by writing reviews. These reviews can either help or damage the escort's business. Sex workers who solicit online also utilize technologies like online payment systems such as PayPal. It is common for sex workers to thoroughly screen and do background checks on clients. Social media pages such as Facebook or LinkedIn can be used to choose is a client's identity if authentic. Other online resources are available for screening clients such as blacklists compiled by the global sex work community warning against people that have put a sex worker in danger.

Although the Internet can allow sex workers to operate discreetly by using pseudonyms and obscuring images however there is no way to ensure total privacy when using the Internet. To track the identity of a sex worker police often use reverse image searches as well as basic Google searches to see if the prostitute is active on any other websites (McAfee).Although, sex workers that use the Internet to operate their business are less likely to harassed by police enforcement and physically harmed by clients compared to street based counterparts conversely they face greater chances of being abused verbally and psychologically. Digital photos contain metadata which may contain GPS location which can be used to figure out personal addresses of sex workers. Sex workers are also vulnerable to having their personal information disclosed by unauthorized parties which is called "doxing". Clients can also film and photograph sex workers without their consent and sell the media without negotiating compensation.

In January of 2017 Backpage, a classified website, had it's adult category seized. The closure of the adult section was though as a win for eliminating child sex trafficking. Backpage administrators claimed that the shutdown of the adult classified page was an attack “on their first amendment rights (Williams)”. Censorship of any type of media is a polarizing topic because freedom of speech is considered a fundamental right in democratic societies, but when abused media has the ability to cause harm. Many people believe that Internet Service Providers such as Verizon and Comcast should not determine what information people are able to access on the Internet. Net Neutrality refers to the concept that “promotes the total openness of the Internet, seeking to keep it free from any form of traffic discrimination, blocking, degradation, and deliberate derailment that might infringe on the experience of Internet users.(Fundukian)” The FCC (Federal Communications Commission) is responsible for mandating the guidelines for Internet Service Providers and other telecommunications companies that prevent them from overstepping their boundaries regarding censorship.

Internet Service Providers have been acknowledged for prioritizing traffic to certain websites and deliberately slowing down traffic to certain sites. For example, in 2008 the FCC found that Comcast was exercising discriminatory in the management of its network (Fundukian). Comcast blocked it’s subscribers from accessing peer-2-peer file sharing applications such as BitTorrent by monitoring user's Internet activity and selectively block websites that advertise peer-2-peer file sharing capabilities. What Comcast was doing was illegal because people were using these file sharing applications to access legal content such as mp3 music files. Comcast probably wanted to limit access to file sharing sites because they did not want to be complicit in what they assumed to be intellectual property theft. The content shared to torrent sites are often stolen copyrighted material. However according to United States copyright law purchasers of copyrighted material are permitted to share the works if they intend to not profit off of it.

Since the 20th century the world has been engaging in what is called the Knowledge economy. Knowledge manifests as *content* which has monetary value. Information is valuable because it gives companies an advantage from a business standpoint. Hackers are people with profound technical knowledge that use their skills to steal information such as ideas, inventions, and creative expressions by exploiting vulnerabilities in computer software. “As technology evolves so do the threats, often at a pace that is faster than companies can keep track of” (Mondaq). Financial, engineering, and scientific companies are at risk at being attacked by cyber criminals because they hold immense amounts of valuable data and information. According to research conducted by IMB in 2015, 100 million medical records were were compromised (Mondaq). Medical records are valuable because pharmaceutical and health insurance companies generate substantial profits worldwide. By knowing what ailments people suffer from companies can efficiently target people to make health related purchases. Business intelligence is a valuable commodity because a company’s unique set of business processes makes them profitable in a competitive marketplace.

Computer Fraud and Abuse Act is a law created by U.S government to prosecute those that violate people’s privacy via computer. CFAA prosecutes those that “intentionally access a computer without authorization or exceed authorized access to obtain information contained in a financial record, information from any department or agency of the U.S, or and information from any protected computer. (Cornell Law)”

The easiest way to steal information is through social engineering. Social engineering is the use of deception to manipulate individuals into willingly giving up confidential or personal information. Social engineers are essentially *con-men*. “Playing on victims emotions, social engineers employ a diversity of tactics to impact the emotional state of the victim, thus influencing their willingness to divulge confidential information. (Holt)” Social engineers appeal to people’s primal emotions such as greed, fear and joy. Everyone is predisposed to cognitive bias which causes people to believe information provided to them which may influence bad decisions.

Social engineering is a common tactic in Phishing scams. Phishing acts deceive people into submitting their personal information like credit card and social security numbers. Phishing attacks look like emails and websites that look like they come from legitimate sources such as banks and utilities companies but the operators are not affiliated with any legitimate organization.Spearfishing targets known patrons of businesses. “Cybercriminals know that if you get an email that looks like it's from your medical provider and it's talking about a surgery you had last year, you are more likely to believe it. (O’Mara)”

Companies are increasingly seeing ransomware attacks. Ransomware is malicious code written by hackers that turns computers into “zombies.” These computers are controlled by the hacker until the company grants the hacker a sum of money. Ransomware is a form of extortion. It is common for ambitious cyber criminals target government organizations, hospitals, universities and corporations. Although attackers are usually motivated by money however some attackers are *weaponized*. “Instead he/she is using ransomware for its destructive power, the ability to sabotage critical data or sensitive systems, in order to disrupt a law enforcement agency, destroy evidence, or force it to capitulate. (Glassberg) ” Hackers often target the government for cyber attacks to unleash government secrets to the public that they did not want citizens to know about and some hackers simply want to create chaos.

Many people wonder is a cyber war possible and I believe a cyber war is already occurring. The concept of hand to hand combat is already waning and warfare is already mitigated by drones and missiles that are controlled by computers.China is actively building their army of hackers to use their skills to fight in cyber war attacks. (Greengard). Nations are being targeted for attacks using computer networks and the consequences are being felt. Stuxnet is a computer worm that is able to infect computers that have vulnerable Windows operating systems that control the operations of oil pipelines, electrical power grids, and nuclear energy plants. Iran’s was once hit by the Stuxnet worm which resulted 30,000 machines in the Bushehr nuclear power plant to run incorrectly for several months (Greengard). Cyber warfare has the potential to to cause strategic damage to the government and civilians.

Crime occurs covertly on the Internet. Criminal acts that happen online range from selling illicit drugs to sabotaging the government. The nature of cybercrime is becoming increasingly complex. The Internet makes it more tedious to figure out a person's true identity although there is no true secrecy or privacy online.

Works Cited

Antonopoulos, Andreas M. *Mastering Bitcoin Unlocking digital crypto-currencies*. Sebastopol: O'Reilly & Associates, 2014. Print.

Glassberg, J. (2016). THE RANSOMWARE THREAT. *Law & Order, 64*(9), 48-51.

Greengard, Samuel. "The New Face of War." *Communications of the ACM* 53.12 (2010): 20-22. Web.

Holt, Thomas J. *Crime online: correlates, causes, and context*. Durham, NC: Carolina Academic Press, 2016. Print.

Jones, A (2015), Sex Work in a Digital Era. Sociology Compass, 9, 558–570.

Moore, Robert. *Cybercrime: investigating high-technology computer crime*. London: Routledge Taylor & Francis Group, 2015. Print.

O'Mara, Anthony. "How cyber criminals use social engineering." *Computer Reseller News* [UK] 3 Oct. 2016: S9. *General OneFile*. Web.

Yar, Majid. "E-Crime 2.0: The Criminological Landscape of New Social Media." *Information & Communications Technology Law*, vol. 21, no. 3, Oct. 2012, pp. 207-219. EBSCO*host*, doi:10.1080/13600834.2012.744224.

Williams, Timothy. "Backpage's Sex Ads Are Gone. Child Trafficking? Hardly." *The New York Times*. The New York Times, 11 Mar. 2017. Web

Project, Inc. The Tor. "Tor." *Tor Browser*. Tor, n.d. Web.

"Crime." *Merriam-Webster*. Merriam-Webster, n.d. Web.

"Net Neutrality." *Gale Encyclopedia of E-Commerce*. Ed. Laurie J. Fundukian. 2nd ed. Vol. 2. Detroit: Gale, 2012. 543-545. *Gale Virtual Reference Library*.

"What is Cybercrime?" *Cybercrime - The Definition of Cybercrime | Norton*. Symantec, n.d. Web.

"Why Combatting Cyber-Crime Is Critical For Life Science Companies." *Mondaq Business Briefing* 3 May 2017. *General OneFile*. Web

"How to Investigate Prostitutes on Backpage." *Insights to Advancing Your Professional Career*. McAfee, 12 Oct. 2016. Web.

"18 U.S. Code § 1030 - Fraud and related activity in connection with computers." *LII / Legal Information Institute*. Cornell Law, n.d. Web.