# Development of cybercrimes in the 21st century

The 21 st century has opened a door of new ideas, new technology and inventions. The 21 st century has also allowed for the social media to expansion to grow at an alarming rate. With all good things come some bad. With the 21 st century moving at a rapid speed so did the cybercrimes. Cybercrimes have increased by twelve percent in the last five years. With more technology comes more problems one might say. Cybercrimes are crimes that involves a criminal working on a compute or a shared network device. Even though most cybercrimes involve a cybercriminal doing illegal activities for profitable gain. Some cybercrimes involve viruses to be sent on computers, or phone devices, anything that has malware security, these types crimes is to damage or disable a person's computer or devices by plaguing it with many viruses, to also spread malware, obtain sensitive information, Steal images or other materials. Most cybercriminals tend to target a larger network because infecting a larger network makes it harder for these criminals to be harder to catch. [1] There are Common types of cybercrimes that include bank information theft, identity theft, online predatory crimes and unauthorized computer access. There are also more heinous crimes like cyberterrorism that can be cause of serious concern. [2] Victimization through the Internet is becoming more prevalent as cyber criminals have developed more effective ways to remain anonymous. And as more personal information than ever is stored on networked computers, even the occasional or non-user is at risk . These types of crimes can be broken into three different parts each resulting into different criminal activity. Some crimes target just a specific number of networks or devices a day. These types of crimes include computer-generated persecution, and

credit card scamming or stolen Identify. The FBI tracks and idenifists cybercriminals who commit bank schemes and forgery devices that takes a person’s personal information electronically. The FBI are the main source of security that helps prevent these hackers/scammers from getting away with damaging a person’s life. There are certain laws that state we are all have a right to our own privacy. The privacy act was established in 1974. The act was passed to help maintain an individual’s use of personal information in agencies this law was helped established through the executive branch. With the invention of the internet the meaning behind privacy changed a little bit so new laws had to be reestablished in order to maintain everyone’s right to privacy. The electronic communications act was passed in the mid-eighties the law states that the U. S. federal government has the right to obtain any digital or electronically communication devices ranging from Social media, emails, public records, certain databases as well. The law also states that no warrants or subpoenas need to be had if it is more than one hundred and eighty days old. There is also the fraud and abuse act which states that if any person’s or individual tries to access and share any protected information that is it considered a federal crime. Many of these Acts or laws are made to keep a person safe from any hacking or privacy concerns. These acts have also been made to help protect the government as well. For example Snowden leaked information about the government watching its U. S. citizens through their electronic devices. Snowden then in return broke the Privacy Act by leaking sensitive information about the government. It just goes to show how easily information can get put out there and how easily someone could hack or even take down agencies. A lot of Cybercrimes happen because agencies are not aware of the risk they take

every day by putting their business on the internet. The internet and devices truly make it easier for hackers to do illegal activities. Most cybercrimes happen every 2. 5 seconds that means every one and ten people are being scammed or hacked. The laws that stated are supposed to help others be safe but what about more serious crimes like cyber terrorism? What kinds of laws are there for those crimes or Child pornography? There a lot of heinous crimes that occur online every second of the day. [3]Cyberterrorism is the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society. Cyberterrorism is when terriosts create their own cyber space in which they have full control over communication networks and can implement attacks as well. Cyberterrorism can range from Social, cultural, political, tactical these are the many motivations a cyber-attack can happen. Over the last decade society has become more and more dependent on technology. The individuals that use technology to commit heinous acts pose an a threat on a global scale because the internet and technology changes every day which means so does cyberterriost ways of hacking or even creating mass panic. Most cyber terriost goals are to in create violence using either a social media plaute form or even by hacking one’s device. For example with the group Anynnous is a group that specializies in hacking  they are known for unleashing cyber-attacks, that include ddos against many government agencies. Anynoumous is known to expose corrupt corropuations, Steal bank information. Cyberterrioism can also be when a group or individual tries to expose government agenices in hopes to cause the government to crash. Cybeterriosim is slowly on the rise. With groups like anynoiums and even ISIS who also play a big part of trying to create fear in the citizens of the united

states by making black mail videos, trying to recruit others online through videos and social media.  Cyberterrioism also includes [4] phising which is when a criminal sends someone fraudlent emails in order to gain access to an indiviudals information such as bank information, credit card information and even social security information as well. There is also something called [5]water hole which is when an cybercriminal makes a fake page in order to compromise the original one so that when the user visits the page they will be bombarded with viruses.  [6] Ransom ware is when a cyber terrorist tries to encrypt certain files in order to lock out the user from any files and black mailing the user to pay some sort of ransom. Cyberterrorism fells in the same category as terrorism because you have a criminal trying to create some sort of chaos only different is it's through technology. Even though cybercrime is an act of privacy violation so is the ways law enforcement does to fight these crimes often law enforcement have to look through someone's email, or access phone records in order to stop a cyber hacker. The fourth amendment of the United States protects people from searches and it protects our privacy. Suprisily though it contradicts certain protections that include the cyber web so it can be harder to for law enforcement to use certain techniques to fight cybercrimes. Unlike the real boundaries are not often set in the cyber world. The computer world is made of some many networks and can go and on forever  which is why law enforcement has to be very cautious when trying to trace a hackers or a cyber terrorist,. [7] Most hackers change their coding constantly in order not to be found, this done by setting up secure networks or codes that will change every other hour if a hacker is constantly able to do that then the likely hood of an individual being caught are often slim to none. The more advanced the hacker or cyber

terriost the more likely they are to also spread viruses fastest on different networks. The black market on the internet is supposed to be a way hackers can get a hold of sensitive information as well. It is a site where cyber terriost go to sell and purchase illegal things some of those things are hacking devices, information on government agencies. With sites like the black market on the web it is an endless way for cybercrimes to happen. Indiviuals that tend to go on the black market to purchase hacker tools are trying to find better ways to obtains people information. The Silk Road trials occurred when the government grew concern about the dark web the concerns grew when they found out drugs and sex trafficking had been occurring on the black market. The dark web had grown so much that the FBI had to get involved the number or illegal activities that were occurring had risen tremendously. The dark web is a hacker’s paradise because the dark web is so secured that even the FBI had a hard time trying to find individuals and illegal activities. Cybercrimes affect the United States as a whole because certain viruses and worms are planted on any device that’s electronic. If cyber hacking or cyber terrorism is not stopped certain viruses can possible become weaponized this could then cause certain viruses to spread at an alarming rate and the world of social communication as we know it might not exist. The government has formed certain measurements in order to maintain a close eye on the dark web, any groups, cyber terriost. The government had to set up their own counter activities in order to keep cybercrimes rates to a minimum. The government has set up advanced IT security systems that allow permanent access to the web including [8] (ARPARNET) which was established by the department of defense. (ARPARNET) is the main source of monitoring everyone’s social media,

emails, accounts things that have anything that deals with personal information. (ARPARNET) Allows hackers and cyber terriost to be blocked instantly their coding allows for certain information to be processed through a network of data which then is worked through by defense agents who determine if anything abnormal pops on the radar. The department of defense is also another agency that works with the FBI on dismantling the dark web and also finding out the sources of the cyber criminals. Extensive research goes into trying to target these cyber criminals. The Arpanet is an implementation warranty that is use to prevent cyber-attacks by finding solutions and fixing any errors before an attacker can find them and use for their own personal gain. So the department of defense created red teams, blue teams and simulations are used to do this. There are also different approaches like implementing a backup plan if someone was doing an inside job involving potentially sensitive information by doing screenings of certain individuals. There is also another way to prevent cyber-attacks the main thing authorities try and do is by banning them completely meaning blocking out whole network of bad data this will then stop and cease any Anti viruses on a computer. This is done through laws that will define such an attack since there are many characteristics of various networks there would have to be accurate measurements and technical support. The concept of these measurements are to stop any illegal cyber activity for engaging whether it’s online or not. There have been more recent attacks involving the healthcare systems. A lot cyber-attacks have been formulated and targeted major insurance companies as well as hospital information being leaked. Cyber terrorism can happen anywhere even in a hospital or medical setting. There was an attack involving some Ransom software in which many hospitals

were hit with corrupt files which then allowed Cyber hackers to gain access to people’s personal health records, there insurance information and things of that nature. Those types of attacks dealing with medical tend to cause mass panic because now every other person is worried their information got hacked. There also the yahoo. com hacking when millions of emails were compromised that was also a major deal because people’s personal information and mail were being used without their permission. There was also the Blue cross blue shield medical in which someone had left their phone on the floor and somehow a hacker was able to access the whole systems data base with personal and insurance information. There was also a case involving Fargo Bank who had a data breach and people’s banking information was comprised. Even the president’s email was hacked at one point it goes to show you that cybercrimes that are committed should be one of the top pritioties of the United States government.  [9] Over twenty cyber-attacks happened within the last three years and they all involved cyberterriost gaining control of a company’s sensitive information without anyone every expecting it to happen so the importance of cyber hacking must be brought more into the light.  The fact that anyone of us on this planet can be hacked by a cyber terriost is truly mind bobbling. With technology forever changing the need to be come up with better solutions for cybercrimes is forever expanding. Cybercrimes usually occur on dating websites because those type of websites tend to gather a person’s personal information and their interests and cyber hackers the turn around and make fake profiles in order to gather people’s social media information. Terror groups love to use the internet their advantage because they know individuals are constantly on their cellphones, computers, tablets, Tvs so this

gives cyber criminals all the more reason to trick an individual into the last scam. The most common hacker sites are those who offer free things such as a cellphone, a gift card, or women clothing. These types of sites are called a proganda site which allows a user to want to be manipulated into gaining something free. [10]Another example of Progranda is dealing with Al Qaida who played off people's emotions and the he used the internet to his advantage in order to gain popularity. He would hire offsite cyber web hackers to gain access to the internet in order to upload and sale his gruesome videos to the dark web. Al Qaida also was able to hire cyber criminals to do his dirty work when it came to hacking places that had a profit. He also hired cyber criminals to cover his tracks. Those cyber criminals well equipped with the tools they needed to hack banks, and to delivery his messages online. Beyond the world of proganda the cyber web allows certain groups to spread knowledge that can be positive but those same tools also allow a cybercriminal to gain weaponry, and to come up with tactics to take down government agencies. There are pages on the internet that will show someone how to hack someone else's lifestyle. The most dangerous criminals were often caught transferring money online to offshore accounts. In the last twenty years cyber criminals have gotten so more advanced with their tactics. For example [11] a sixty year old lady who lived in New Albany, Indiana had begun to receive numerous emails from Direct TV in which she already in her home. They were offering her money if she switched her account to a premium account. Well not knowing any better the lady put her information on the computer five minutes later her accounts were withdrawn all of her retirement money was gone. It was a very sad story because cyber hackers do not care if you are young, old they just see

everyone as a target. The main thing a Cyber hacker does to their victims is gaining their trust by gathering up all their information. Unforunalately in today’s world the reality is that any individual and organization that is connected to anything electronic or even the internet is susceptible to a cyber-attack. The threats to the cyber world continue to grow the ACSC has reported there will be more cyber-attacks in the next ten years to follow. Based off the number of attacks and the types of attacks it seems to be more and more attacks dealing with

Scamming and also stealing an individual’s information. It isn’t only large organizations that are under threat. Even individuals or organizations that don’t believe they have much to offer hackers can be targeted. So even if you think you’re a small target, you might still be at risk.  Some of the risks a company or an individual could face from cyber hacking is identify theft which can cause damage to a person’s daily life. Some ones credit could be compromised as well. To make things even worse the process of trying to reverse cyber hacking can be very costly and time consuming to say the least. In some cases the type of damage could also come in the form of confidential information being leaked. The best way to prevent cyber-attacks is for companies or an individual to change their whole attitude towards what cyber-attacks are. If a individual has the right tools to understand what happens online and realizes that everyone is a target and then they can take the steps needed to prevent these attacks. It is also important to change the detection of incidents and how to handle certain scenarios as well. The main reason we know the cyber-attacks that are mentioned above happened cause they were not detected in timely manner. Having a backup plan when

dealing with cyber hacking will be very benefictal to a company. Most companies or individuals do not ever consider incident handling as a main source of stopping cyber hacking. Incident handling is the defense of cyber hacking because it guarantees a company is well protected. The main thing that incident handling does is make sure any information that is compromised is not backed up on any devices. There has been a great deal of effort on treating cyber-attacks more than auditing situation. There are a great deal of companies and individuals that look at cyber security maintance as a defiance task and a way to improve overall security and thus avoid costly and damaging incidents in the future. When it comes to cybercrimes knowing how to hurt these criminals back is very critical to stopping future attacks.[11] A cyber expert named John Han, stated that once a hacker knows they can be stopped they will turn around and find new ways to beat the system, So having a great defense is key to stopping these crimes. It seems as though the internet and our electronic devices play a critical role in society. [12] When it comes to cyber laws and ethics are constantly being made to stop these crimes. It is the responsibility of everyone who owns an electronic device or is on the web to follow these laws. It is also important to have security hardware and software installed on all sources that produce any thing that has data or files on it. Anti-spy ware tools should also be installed on anything electronic to help secure any confidential information and in order to remain safe from any cybercrimes. Having a great internet service will also help with maintaining a high level security measures since more than likely a server could be the main thing being hacked, having a good internet service provider can also keep any malicious programs from taking over someone’s devices. Much like buying a

new home you have new doors and locks. When you purchase a house you want to make sure everything works great from the locks to the windows. When buying a house most people decide to get a security system in order secure their home from any outside threats that is the same with the being on your electronic devices. [13]Investing into a great security system can make a big difference when it comes to staying safe from cyber criminals. Following the basic steps of not opening any browsers, using any anti spy or malware systems to help detect anything suspicious comes in hand as well. It is very important to remember that no systems or networks are completely secure even though the web and internet website might say secure there are always ways for cyber criminals to wiggle their way through.[14] Raising the awareness on cybercrimes could potentially protect a lot of individuals from being hacked and any confidential information being leaked. These cybercrimes can be stopped with the right tools and the right security measures. [15]Cyberterrorism, Cyber fraud, Cyber bullying, Cyber hacking are all crimes that are punishable in the court of law.

## References

1. [1] Stacy Cowley, Banks Adopt Military-Style Tactics to Fight Cybercrime The New York Times (2018), https://www. nytimes. com/2018/05/20/business/banks-cyber-security-military. html
2. [2] How Do Hackers Get Into Computer Systems?, WhatIsMyIPAddress. com, https://whatismyipaddress. com/hacking-basics
3. [3] ndiana University Kokomo, Experimenter : the Stanley Milgram story | Search Results | IUCAT, https://iucat. iu. edu/iuk/9628098

4. [4] Ryan Littlefield, Cyber Terrorism: understanding and preventing acts of terror within our cyber space Ryan Littlefield (2017), https://littlefield. co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb
5. [5] What is ARPANET? – Definition from WhatIs. com, SearchNetworking, https://searchnetworking. techtarget. com/definition/ARPANET
6. [6] What is Cybercrime? – Definition from Techopedia, Techopedia. com, https://www. techopedia. com/definition/2387/cybercrime
7. [7] What is phishing? – Definition from WhatIs. com, SearchSecurity, https://searchsecurity. techtarget. com/definition/phishing
8. [8] What is ransomware? – Definition from WhatIs. com, SearchSecurity, https://searchsecurity. techtarget. com/definition/ransomwar
9. [9] What is watering hole attack? – Definition from WhatIs. com, SearchSecurity, https://searchsecurity. techtarget. com/definition/watering-hole-attack
10. [10]N. D.
11. [11] Cyber Security Speaker | Keynote Speaker | John Sileo, Sileo. com, https://www. sileo. com/
12. [12] N. D.
13. [13] N. D.
14. [14] NortonOnline, What are some of the laws regarding internet and data security? Norton Family Premier, https://us. norton.

com/internetsecurity-privacy-laws-regarding-internet-data-security.html

15. [15] N. D