The rise of computer crimes

Technology, Computer

Abstract: There are more cyberthreats now than what society could have ever foreseen. Cybercriminals are getting smarter and becoming more advanced by the second leaving behind those who are protecting the United States citizens at a local, state and federal level behind. Most citizens have their information stored on some device, which leaves them vulnerable to any cyberattack that occur. This research paper reviews literature and discusses topics such as the dark web, technology, financial, admissibility in court, and investigations. All subtopics are discussed to explain the rise of computer crimes in our criminal and legal systems in the United States.
Keywords: Dark Web, Technology, Financial, Admissibility in Court, Investigations, and Criminal Justice INTRODUCTION The computer was a massive advancement for mankind and the start of technological advances humans could not even dream of. In the 1990s personal computers had entered homes, offices, and increased communication and process of globalization.

The invention of “ www.” Created the average user to have access to the internet anywhere, anytime. In 1998, 72 websites were vandalized by 47 attackers and a year later in 1999, 1, 079 websites vandalized by 430 attackers (Li, 2003). “ The General Accounting Office reported 250, 000 attacks against the U. S. Department of Defense computers in 1995. These numbers represented different aspects of the situation of risks and threats on the Internet” (Li, 2017). All statics above occurred in the 90s, the same year common citizens gained access to computers but with clear limited knowledge on how computers worked. In the same decade, hundreds of thousands of computers were hacked and websites vandalized by hackers

who were trying to make their mark in cyberspace. With the utilization of peer-reviewed journal articles, the scholarly articles will offer insight and cases that will agree or disagree with the development of digital evidence (digital forensics) to be an admissible piece of evidence in the courtroom. The reasoning behind using such trusted articles is they do not seek their own agenda and have no opinion included in their research. This helps make the information and research found unbiased which helps weighs the pros, cos and allows the researcher to draw their own conclusions. The criminal and legal justice systems have taken steps to combat electronic warfare, whether it be on a small scale or a bigger scale. Computer forensics was developed in effort to help law enforcement to obtain the digital evidence and analyze and testify to its admissibility in the case and courtroom. Due to our] developing society it is difficult to keep up the training of digital forensics which can make presenting it in a courtroom difficult. The purpose of this study is to analyze the importance of digital evidence and continuing the training and educational aspect of technology. In part of education the law enforcement side of such advancements it is important to also analyze our laws.

Statement of the Problem

The purpose of this study is to examine and analyze the increase of computer crimes in our society, criminal and legal systems. The criminal justice and legal system made preserving the integrity of physical evidence collected at crimes scenes intricate and complex but makes it easier to testify the chain of evidence for each item in a courtroom. Technology is so advanced and will continue to grow exponentially in our lifetimes but

unfortunately this is not the same as our legal and justice systems in the United States. Our justice systems have been the same since laws and regulations were founded hundreds of years ago yet we apply these same laws to digital evidence when there was no such thing back when the law was established. Serious cybercrimes have increased and escalated over the years, but at a faster rate than one would have thought. Like the war on drugs, when there was an increase in drugs there was also an increase in arrests and people jailed, but we do not see the same correspondence when looking at the rise of computer and cybercrimes. There is a disconnection between criminal justice and legal professionals understanding the parameters of such digital evidence has been the reason investigations go unsolved and unprosecuted. Cybercrime and rapid advancement have distinctive inconsistencies between the Unites States' systems of law and law enforcement officers including first responders through the defense and prosecution. In this research paper it will review literature encompassing the dark web, technology and its advancement, financial gain, admissibility of digital evidence in court, and the investigation. Exploring these subtopics will raid awareness or start conversation of impending, ongoing, and future investigations.

LITERATURE REVIEW THE DARK WEB

What is the dark web? How does one access the dark web? Is it easily acceptable? How does the dark web contribute to criminal activity? Is out law enforcement and legal system strong enough to defend and protect against criminals who use the dark web? These are only but a few questions about

the dark web, but the main question is what is the dark web? In its simplest terms, the dark web is an area of the internet where the purchase of illegal goods can be sold on the black market (Bruemmer, 2017). One may think using or getting to the black takes a specialized skillset but because of the development of technology and almost every citizen having access to a computer, the sale of illegal items and usage of the dark web has become mainstream. In the article sited above, Data breach digest: Dark web 101: What it is and how to keep your data safe, it discusses how companies can learn about the dark web and use it to further protect themselves. In regard to this research paper the article can still apply to the rise of computer crimes in the justice system. Bruemmer lists 3 main steps for a company to ensure they are educated and protected against criminals in the dark web. Step one, " set-up your first line of defense," describes strong defense protocol that will help keep your secured data out of the hands of the criminals. At a local, state, or federal level there are civilian or law enforcement officers who are trained to prevent data breaches because of the sensitive information they store. Step two implies said business to sign up for business credit but because that does not apply to the purposes of this research paper it will be skipped. The last and final step discussed is considering remediation steps, this step applies to a breach that may have just occurred. Two specific points in this final step are important and can be applied to the criminal justice need to be addressed, identity protection and dark web and internet record scans. Identity protection is highly important in law enforcement especially on a federal level where special agents' identities can get leaked and that is not only bad for the agency, but the individual

involved. The second, dark web and internet record scans, although may not seem as important as identification protection it should be considered just as important. If there are officers across all three levels of law enforcement who understand the dark web, knows how to search and contact criminals selling or participating in criminal activity it is possible it will not get to the point of identities of agents and officers leaked on the internet (dark or regular internet).

TECHNOLOGY

Technology is expanding at an exponentially faster rate than the development of society and its effort to keep up with technological advances. In a journal article titled, Cyber-crimes and their impacts: A review, they define a cybercrime that " can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction" (Saini, 2012). In simpler terms, the act of using technology to breach or " illegally trespass" another's computer system with intent to use the information found on the device(s). This article also lists some types of cyber-criminals and the type of cybercrimes. Cybercriminals include crackers, hackers, pranksters, career criminals, cyber terrorists, cyber bulls and salami attackers. A few of the cybercriminals look familiar and can be heard in day-to-day descriptions of common cybercriminals at a local and state level. A cracker are individuals whose sole purpose is to cause loss of their victim of some type. The intent is to make the victim pay, for example, this could include the cracker implanting a virus on one's computer and requesting monetary gains to release information

back to the victim. This is to not be confused with a hacker, which intent does not include blackmail or monetary gains. Hackers use their skills for educational and curiosity purposes. When a hacker hacks, the intent is to gain notoriety among the community that can help build their reputation. A hacker’s goal is a bigger target, someone or something with power or money. Career criminals is a person where this is an income-based job for them, full or part-time. This type of cybercriminal tends to conspire with others and work with organized crime gangs. Cyber terrorists are the biggest threat and not because one may think it is one big job and has a clear objective, but because there are so many forms of a cyber terrorist attack. “ Cyber bulls” is very common among younger persons from elementary through college students. Per its name, cyber bulls use the internet as a place to harass individuals using unappropriated posts, chat rooms and fake profiles to attack an individual. The list includes seven kinds of cyber-criminals, the final two are two terms that are not so common and are defined below per the article: Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or longlasting harm. Salami attackers: Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e. g. a bank employee inserts a program into bank‘ s servers, which deducts a small amount from the account of every customer (Saini, 2012). FINANCIAL What is the main difference between a regular crime and one that include the cyber world, cybercrimes? There are several differences, two being access and anonymity. If an individual decides to rob someone or something they would

physically assault or enter the place in question, but a cybercriminal can hide behind screens and firewalls. In the journal article The Simple Economics of Cybercrimes, it lists three ways cybercrimes are structurally unique, “ they’re technically and skill-intensive, they have a higher degree of globalization that conventical crimes and they’re relatively new” (Kshetri, 2006). Like any other crime, cybercrimes, computer crimes are a cycle of basic want and needs and the third point, “ relatively new,” is that exactly. Since the development and release of internet and computers to the public cyber-terrorism, crime, and bullying, as stated before, have grown exponentially and left behind those who are supposed to protect and serve. A $32 billion dollar financial loss struck citizens in 2010 when Norton Cybercrime disclosed there was a data breach and over 74 million victims were attacked. Upon more analysis of cybercrimes, research has found that just about seventy percent of adults admit they fall victim to some cyber scam, which results in “ 1 million cybercrime victims a day” (Saini, 2012). Due to the dependency of technology this society has the risk has increased. The problem is access and it goes both ways, victim and cybercriminal. As a victim there is too much access to networks and computers and with no basic knowledge of how networks and computers work, hacking someone is that much easier. ADMISSIBILITY IN COURT Forensic reporting and expert testimony of such digital evidence is still fairly new to society and new to the criminal and legal systems of the United States. The first case of scientific evidence admission was Daubert v. Merrell Dow Pharmaceutical Inc., 509 U. S. 579, 595 (1993). This is a landmark case, legally, because it set a standard in which judges could determine the admissibility of scientific

findings in federal court. This prompted a five-prong standard, commonly known as the Daubert standard, that assists in the uncovering of scientific evidence in the courtroom, which includes:

1. Testing: Has the scientific procedure been independently tested? (2) Peer Review:
2. Has the scientific procedure been published and subjected to peer review?
3. Error rate: Is there a known error rate, or potential to know the error rate, associated with the use of the scientific procedure?
4. Standards: Are there standards and protocols for the execution of the methodology of the scientific procedure?
5. Acceptance: Is the scientific procedure generally accepted by the relevant scientific community? (Garrie, 2014).

The Daubert standard was groundbreaking in for both the legal and criminal justice systems because it introduced a new way for law enforcement to produce supplementary pieces of evidence than that of just physical evidence. This standard only allowed judges to have an objective scope for accepting this type of evidence, until six years later in the court case of Kumho Tire v. Carmichael, 526 U. S. 137 (1999) expanded up the standard to include expert witness and testimony of such scientific evidence. The Federal Rule of Evidence 702 or FRE 702, provides specific guidelines that qualifies one to be an “ expert” or “ expert witness” of “ scientific, technical, or other specialized knowledge” (Garrie, 2012). Due to forensic science and digital forensics still developing, the Kumho Tire standard postulates an expert being one who has technical or specialized knowledge in that field and not a

regular person called to testify. Investigation Cybercrimes have gained notoriety and have become much more complexed that requires expert testimony, outside and with local, state or federal agencies. Common violent and non-violent crimes can be tied to some type of MO or modus operandi that cannot be tied to cybercrimes. This makes tracking the crime and criminal down if you are not an expertise in computers. Advanced blended attacks leverage vulnerabilities in fixed and wireless networks to steal credentials and conduct reconnaissance (FireEye Labs, 2015). The increase of digital evidence in police investigations and courtrooms should call for practices of handling, analyzing and interpreting forensic digital evidence. Cyber-investigations range from invasive and interpersonal searches by law enforcement or intelligence agencies of a person’s life. Regular protocol and steps of an investigation will be followed the same of any other case, but should there be more protocol and action taken by the court to prevent tampering of evidence? Short answer, yes, but if not all law enforcement officers understand the basics of computers let alone seizing them correctly can we guarantee the chain of custody? Search and seizure of digital evidence still includes the discovery of evidence, identification of suspects, detaining and arresting offenders, and interviewing witnesses. Trans-jurisdictional practices vary based on geographical location, therefore it is extremely important for officers to review and know how they must handle seized digital evidence. Before one commits a search, they should ensure follow strict protocol or all evidence relating to the digitally seized evidence can be ruled inadmissible in the courtroom (Brown, 2015). Plain view doctrine may still be applicable to digital evidence but will vary, again, based

on jurisdiction. However, if there are cases in the risk of losing the digital evidence is far higher if you seize it because of “ data sanitizing and other anti-forensics tools are active,” search and seizers will be limited per state laws because of the vulnerability of the data (Dee, 2012).

DISCUSSION

The dark web, technology, financials, admissibility in the court, and investigations of computer/cybercrimes has evolved far more than what our society has done so today. As all parts mentioned in this research paper, technology and society, continue to move ahead, criminals become smarter and law enforcement and justice system remain in the dark. As a whole our societal norms and morals have become obsessed with being dependent on technology. Need a GPS? Use your phone. Need to find a nearby gas station? Use your phone. Left your wallet at home? You can use your phone now, as long as your credit card is linked to the app on your phone that stores that information. The development of more technology increases the usage amongst the people but that also means it increases the risk and number of hackers, crackers, pranksters, and cyberbullies. The understanding of the cybercrimes could impact the way our society functions and how our local, state and federal law enforcement officers respond to an attack and seizing of evidence. The lack of basic understanding of how technology works allows financial loss, victimization and inadmissible digital evidence to get thrown out of court cases. The understanding of how cybercriminals work and the destigmatization od what one looks like will help protect the victims, businesses and national security.