Katie Barnes

MET CJ 610 01

Professor Lee

May 24, 2021

As technology evolves society has become more reliant on digital devices for everyday use. Sadly, the more we rely on technology as a part of our daily lives the more at risk we are to the world of hackers. Hackers come in different colors not all are bad. The white hats are the good hackers trying to help solve cybercrime, black hats are considered the bad guys (the criminals of cyberspace) and the grey hats are somewhere in-between (Internet Hackers, 2017). We trust the internet for many simple things like online shopping, to pay our bills, for work, or school etc. However, as we are incorporating technology into our daily routines, we are risking potentially losing our identity, to cybercrimes like credit card fraud or our personal data being used for ransom.

Ransomware is a virus introduced through E-Mail, once infected the virus grabs every personal file on your computer making everything inaccessible and put up for ransom by the hacker (Internet Hackers, 2017). This means that you must pay the ransom to the hacker, or you will lose everything for good. This is just an example of cybercrime at a Micro- level which essentially refers to small scales of crime. The Micro-level phenomena are contrasted with the Macro- level phenomena, which describes a broader societal trend at the neighborhood or national level (Graham & Smith, 2021). For An example, governments or other countries using technology for mass destruction like targeting factories, water supplies, or power grids (Dart,

2013). Explaining why a hacker may commit a cybercrime with the Routine Activities Theory as a mid-level theory which is basically a practical application of situational crime-prevention' measures by changing conditions and circumstances (Lee, 2020). There are many reasons that individuals or groups of individuals decide to choose computer hacking. While some choose to do no harm, others use these skills to commit acts of theft, violence, or cause destruction. Companies such as Facebook, Google, or Apple, use our data to buy and sell personal information for promotional use (Internet Hackers, 2017). These companies make money of our personal information such as our habits and daily activities on our devices, this helps advertisers make money off their customers. Some hackers want to steal money from credit cards or banks, while others try to steal information from large corporations or secret information such as government secrets.

Many Hackers can eavesdrop on companies and government agencies by retrieving data that can be used against a person, company, or a country. While some cybercrimes are easy to track others are merely impossible like a needle in a haystack as the cybercriminal could be in another country committing cybercrimes. With newer technology and being able to know when someone is eavesdropping is an interesting way to pinpoint where the crime is originating from. Perhaps the creation of the quantum processor could help with crime solving. Quantum mechanics can work both as good and bad. It could help to trace crime by breaking through encryptions while being able to discover who is listening in. However, this could also mean the cryptographer could share secrets. Ironically, encryption is what keeps secrets safe over the internet if quantum mechanics can break those secrets, it could be used maliciously by those who could buy and sell those secrets (Dart, 2017). For future hackers the criminal justice policies should be evaluated. "As Beccaria thought punishment should be proportionate to the crime

committed, and criminal behavior would be deterred by certainty, swiftness, and severity of punishment (Lee, 2021)". The Cyberworld is really a war between the white hats, the black hats and those who are undecided who there are.

Moreover, as deterrent strategies reflect on my theoretical perspectives, I think that continuing to train and hire more white hat hackers is key. If we stay one step ahead of fighting cybercrimes, we can potentially defeat some crimes before they even occur. I think that we do have an invasion of privacy, but it may be critical for future hacking that we have acquired all these technical abilities to essentially watch the world around us. The world has become so unsafe that our children can't even play outside or go to school without a fear of them being kidnapped, harmed, or abducted shipped off into sex- trafficking. Many may view this as paranoia while others want to prevent such things from happening to innocent people. A handful or citizens may view cybersecurity as an invasion of privacy while others view it as a necessary security measure. Whether we like it, or not bad hackers are finding ways to invade and make everyone vulnerable to their invasions, so we need to come up with strategies to be ahead of their crimes. In Songdo South Korea, their city was created from scratch from the ground up as a smart city. Everyone is on surveillance daily there is no privacy for anyone. This means that there is less crime because it is harder to commit crime having surveillance daily (Internet Hackers, 2017). I believe as a society that has become completely reliant on technology that it would be safest to come up with surveillance strategies like Songdo in South Korea. We can either get in the loop or become controlled by other countries where we no longer have a choice but to rely on them. I do believe in privacy, but I think privacy should be available when you are inside your own home. Once you come outside among the rest of society you should understand that we have families from small children to the elderly that rely on us to keep them safe. We can't do that if

we do not upgrade and excel. I do not believe we shouldn't have our fundamental rights, but I do believe that if you are a law-abiding citizen, you should not have an issue with surveillance outside your home. We should always have privacy in settings where we change our clothing, sleep, or use the bathroom. That type of privacy should never be unchanged. We have the right as citizens to protect our bodies and our children from sexual predators.

Utilizing the Routine Activities Theory, I think it is important as a crime preventing strategy to increase police patrol in "hot spot areas; using locked doors, windows, and alarm systems; and creating community crime-watch programs (Lee, 2021). In the cyberworld, this could mean more surveillance, more cybersecurity, red flags on known hackers, spreading cybercrime awareness through education and training. As we recruit Army and Marine soldiers, we shall recruit cybersecurity agents and intelligence with the same intent 'to protect and serve our country'. I like the idea of hacker conferences and conventions it is a great idea to create new ideas and strategies while learning about new crimes and trends. As far as deterring crime, the more society is aware that we 'the white hats and law enforcement' are watching and tracking cyber crimes the less likely the crimes will occur. If we implement new laws and punishments that are harsher individuals or group of individuals who care about their freedom my deter away from crime.

References

Dart Kate, & British Broadcasting Corporation (Producers), & Dart, K. (Director). (2013). Rise of the Hackers. [Video/DVD] Public Broadcasting Service. https://video.alexanderstreet.com/watch/rise-of-the-hackers

Graham R, Smith S, (2020). *Cybercrime and Digital Deviance.* Routledge, New York, NY.

Internet Hackers in 2017. Bernanke, J. Mayor, B. (Producers), & Peter Schnall (Director). (2017). Digits: Guardians of the Web. [YouTube]. Retrieved from https://www.youtube.com/watch?v=rXFolJiuMl8&t=9s

Lee, H. (2021) Module 3: *Causations of Cybercrime: Criminology Explanations*. Boston University Metropolitan College