Shize Lin

Marc Friedenberg

IST 110: Section 003: Info People Tech

April 25, 2025

Punishment Over Rehabilitation

As internet technology advances, cybercrime has become more frequent and poses a serious threat to the security of public information and personal property. In response, the justice system must take a clear stance on whether to focus on rehabilitation or retribution. Cybercrimes vary in form, including identity theft, online fraud, and impersonation. Many of these crimes involve simple methods that are easy to copy. Some argue that cybercriminals should be rehabilitated, hoping to uncover technical potential. However, this view overlooks the fact that most cybercrimes do not require real skill. Only a small number of offenders possess advanced abilities. Most operate with limited knowledge, and if they are not punished strictly, their behavior may escalate. This paper argues that punishment should be the priority, especially for offenses that lack technical complexity. Excessive leniency only encourages further wrongdoing.

Most cybercrimes do not require high-level skills. In many cases, basic learning or imitation is enough. For example, phishing emails and identity impersonation are common. Phishing involves fake messages pretending to be

from banks or government offices, tricking people into clicking links that steal account data. Impersonation often occurs on social media, where offenders use fake profiles to commit fraud. These actions are standardized, and many people can use ready-made tools without programming skills. Putting such offenders into rehabilitation is unlikely to change behavior and uses resources better spent on serious cases. More importantly, light punishment creates the impression that these crimes are low risk and high reward. The 2016 Mirai botnet attack is a clear case. According to the U.S. Attorney's Office (2018), the malware disrupted internet access for millions in the U.S., Germany, and beyond. Though the developers pleaded guilty, they received probation, community service, and a fine due to cooperation with the FBI. This result suggested that cooperating after the fact can reduce punishment.

Some believe cybercriminals should be rehabilitated because they may have useful skills. But this belief is overly idealistic. Few offenders can build advanced systems. Most copy scripts, buy tools, or run others' programs. These individuals lack the depth needed for system design. The idea of hidden potential is often unfounded. Talented people can succeed legally and don't need to break the law. Overemphasizing rehabilitation inflates the value of illegal behavior and discourages law-abiding professionals. Therefore, punishment—not misplaced leniency—should be the main approach to cybercrime.

In conclusion, as cybercrime becomes more widespread, the justice system should treat punishment as its core response. Most cybercrimes lack technical

depth and are easy to imitate. Without consequences, these actions may seem acceptable. The idea of technical potential often excuses wrongdoing. Those with real ability do not need crime to succeed. Focusing on punishment is the best way to protect online order and public safety.

Reference

1. U.S. Attorney's Office, District of Alaska. (2018, September 18). *Hackers' cooperation with FBI leads to substantial assistance in other complex cybercrime investigations* [Press release]. U.S. Department of Justice. https://www.justice.gov/usao-ak/pr/hackers-cooperation-fbi-leads-substantial-assistance-other-complex-cybercrime