Punishment for Cybercrime Should Focus on Rehabilitation

Cybercrimes are common today in our information society. They can be as small as minor offenses such as unauthorized access, or as big as coordinated attacks endangering national security.

There is, therefore, active discussion about how cybercrime should be treated. While some may argue that retribution is more important, I think punishment for cybercrime should focus more on rehabilitation.

THE UNDERLYING ISSUES

Understanding the motivations behind cybercrime is a must as legislators and law enforcement seek to develop effective prevention strategies that go beyond mere punishment.

There could be multiple factors driving cybercriminals. Many engage in cybercrime primarily for monetary benefits. Individuals from economically disadvantaged backgrounds may turn to cybercrime as an alternative means of income. Like in the case of the Nigerian prince scam, the rise of which can be traced to a series of economic crashes in the 1980s, and the resulting joblessness among young people in Nigeria. (Ozeh & Ohajionu, 2019) (Moga, GALLE, & Rukayyat, 2021)

Some individuals, known as hacktivists, commit cybercrimes to promote political or social ideologies or to advance specific causes. The desire for status or recognition or sometimes just the thrill of outsmarting systems can also drive individuals to commit cybercrimes.

SKILL REDIRECTION

Cybercriminals often possess advanced technical skills in computer systems to launch an attack. Rehabilitation programs can redirect these skills toward positive ends, such as cybersecurity consulting. Their experience with hacking provides perspectives of the attackers on breaches, therefore it would be valuable if they could advise organizations on strengthening their protocols or developing new technologies that safeguard cybersecurity.

For example, the famous 1998 testimony of L0pht Heavy Industries, a Boston-based hacker collective, before the U.S. Senate shows the contributions that individuals with hacking expertise can make. (Tropeano, 2019) During their testimony, they warned that they could "take down the internet in 30 minutes," which was widely reported, calling for attention to cybersecurity. They also provided perspectives on many cybersecurity issues, some of them remain relevant to this day. (Grand, 2011)

DETERRENCE BY RETRIBUTION IS INEFFECTIVE

It is a common argument that retribution creates deterrence against cybercrimes, since it can make attackers deem that it is not worth the risk. However, this deterrence has shown limited effectiveness.

The anonymity provided by cyberspace makes it difficult to identify and apprehend attackers, which reduces the perceived threat of punishment. Many cybercriminals, especially minors and skilled hackers, discount their likelihood of being caught, and the psychological impact of retribution is not as effective.

Cybercriminals are often strategic actors who adapt to enforcement efforts rather than being wholly deterred. The global nature of cybercrime further complicates deterrence. While international frameworks like the Convention on Cybercrime have led to reductions in attacks within enforcing countries, they have often displaced attacks to non-enforcing countries instead. (Hui, Kim, & Wang, 2017)

Historical evidence also shows that penalties can stimulate retaliatory behavior. For example, following the arrest of WikiLeaks founder Julian Assange in 2010, Anonymous launched Operation Avenge Assange, targeting entities that had severed ties with WikiLeaks under governmental pressure. (U.S. Attorney's Office, Northern District of California, 2014)

CONCLUSION

We should acknowledge the required skills and motivations of cybercriminals and the limitations of retribution. Redirecting the technical expertise of cybercriminals into constructive roles not only provides a productive path for offenders but also strengthens overall cybersecurity. Addressing the

psychological, social, and economic drivers of cybercrime is also very important. Given the anonymity and global nature of cybercrime, retribution alone is insufficient to deter such offenses effectively.

In conclusion, punishment for cybercrime should prioritize rehabilitation over retribution. A rehabilitative approach is better for the long-term goals of preventing cybercrimes, protecting societal safety, and integrating talented individuals into beneficial roles.

BIBLIOGRAPHY

Grand, J. (2011, March 14). *Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries)*. Retrieved December 1, 2024, from YouTube: https://www.youtube.com/watch?v=VVJldn_MmMY

Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017, June). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly, 41*, 497-524. Retrieved December 1, 2024, from https://www.jstor.org/stable/26629724

Moga, E., GALLE, S. A., & Rukayyat, A. (2021, August 25). A Historical Assessment of Cybercrime in Nigeria. *Journal of Research in Humanities and Social Science, 9*(9), 84-94. Retrieved December 1, 2024, from https://www.questjournals.org/jrhss/papers/vol9-issue9/Ser-1/N09098494.pdf

Ozeh, C. C., & Ohajionu, C. C. (2019). Unemployment, Migration and Cyber Criminality in Nigeria. In O. O. Oshita, I. M. Alumona, & F. C. Onuoha, *Internal Security Management in Nigeria: Perspectives, Challenges and Lessons* (pp. 165-180). Springer Nature Singapore. doi:https://doi.org/10.1007/978-981-13-8215-4_9

Tropeano, R. (2019, January 9). *Cybersecurity: When Hackers Went to the Hill — Revisiting the L0pht Hearings of 1998*. Retrieved December 1, 2024, from National Security Archive: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-01-09/cybersecurity-when-hackers-went-hill-revisiting-l0pht-hearings-1998

U.S. Attorney's Office, Northern District of California. (2014, November 18). *Thirteen Defendants Plead Guilty For December 2010 Cyber-Attack Against PayPal*. Retrieved December 1, 2024, from United States Department of Justice: https://www.justice.gov/usao-ndca/pr/thirteen-defendants-plead-guilty-december-2010-cyber-attack-against-paypal