Whether punishment for cybercrime should or should not be more

The Pennsylvania State University

IST110: L12 Cybercrime Assignment

April 4, 2024

Topic: Whether punishment for cybercrime should or should not be more severe for repeat offenders; does it depend on what form of cybercrime?

In the type of cybercrime, one of the disputable issues is if the punishment for repeat offenders should be made more severe. Punishment has various levels defined by the specific facet of cybercrime and the extent of damage it brings about. This paper proposes that punishment for cyber criminals who commit repeated offenses should be severe with special emphasis on cases where a crime generates harm to individuals, organizations, or society.

Argument:

Punishment terms for repeat cybercrime offenders cannot be arched too high for all sorts of cybercrime. In its place, it should be more fitting to the exact particulars of the situation. To start with, as far as non-violent cybercrimes like hacking for personal gain or unauthorized access to network systems is concerned, rehabilitation will be the best method if it is a onetime offense of a first-time offender. Further, crime-related activities may be subjected to harsher punishments if there are multiple convictions or intervention attempts made previously to deter future recidivism and safeguard the public (Holt & Bossler, 2017).

While in the instance of cybercrimes that are classified as posing a significant threat to public safety or national security, such as cyberterrorism or large-scale data theft, a more rigorous approach may be called for even for first time offenders. In such situations, the damage done by cybercrime is much more than what someone can afford to rehabilitate, and society has to take this kind of offense very strictly (Reyns et al., 2019).

For this argument, academics point to the indicators on recidivism among cybercriminals, which are substantiated in the body of research. Research evidence shows that traditional law enforcement methods used for cyber offenders might not work for the fear of plentiful victims while others deemphasize the need for criminals to go under specialized treatment and rehabilitation programs focusing on their specific needs for cyber offenders (Jaishankar,

2020). As in instance, there is research which was conducted and published by the Journal of Cybersecurity that showed reduction in the recidivism rates among cybercriminals and those who finished deferring with the specific intervention programmers which were focused on addressing the causes that lead to criminal behavior (Yar, 2013).

Counterargument:

Individuals who will protest this approach may often allege that existence of the same punishment for several cybercrime offenders reveals that cybercrime behavior cannot be tolerated and that is a level of understanding which may be considered as a stronger deterrence. They may consider the leniency towards repeat offenders in relation to cybercrimes as a mistake and a clear indication of how unserious the matter is, and it also provides loopholes which makes it hard to fully protect the victims.

Nevertheless, the opponents often take cybercrime scenarios in a narrow perspective and do not see different underlying reasons for this criminal activity. The toughest sanctions are imposed even if the extent of uniqueness of the case is not accounted for; therefore, this may lead to injustices and hamper the ability to strike the root causes of cyber criminality. Besides that, the single-solution-fits-all approach to punishments will not consider reformation and reintegration into society that could lead to a decrease in the number of re-offenders (Wall, 2018).

Conclusion:

The sentence for repeat cybercrime offenders should be determined on a case-by-case basis, including the type and seriousness of cybercrime, prior criminal record, and opportunities for rehabilitation. Albeit there is no guarantee that a targeted approach will eliminate re-offenders, it is a much more balanced and practical approach which not only is useful for solving cybercrime, but also for promoting society's security as well. Through assessment of individual factors, psychological characteristics, and environmental considerations, which all influence the likelihood of future offending or harm to the individuals or institutions caused by cybercrime respectively, we can customize our interventions more effectively and prevent cybercrime more often.

References:

Holt, T. J., & Bossler, A. M. (2017). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge.

Reyns, B. W., Henson, B., & Fisher, B. S. (2019). Cybercrime Victimization and Offending. Annual Review of Criminology, 2(1), 271-293.

Jaishankar, K. (Ed.). (2020). Global Criminology: Crime and Victimization in a Globalized Era. CRC Press.

Yar, M. (2013). Cybercrime and Society. SAGE Publications.

Wall, D. S. (2018). Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime. New Media & Society, 20(11), 4182-4201.