

Peer Response

Reply to Post 1

I concur that cyber criminals have gone beyond adventure or revenge in encompassing the most heinous crimes. Criminals are using more callous approaches to attain their goals, and the expertise of attacks is likely to advance as they experiment with new cyber-attack tactics (Norwich University Online, 2017). What used to be called petty cyber offenses have progressed into severe crimes because cyber-attacks are convenient, cheap, and less risky than physical crimes. Moreover, cybercriminals need only a few expenses beyond a computer and are unconstrained by distance (Jang-Jaccard and Nepal, 2014, pp. 973). The advancement of the global cybercriminal network is primarily credited to the increased opportunity for financial incentives, creating different types of cyber offenders that pose a substantial threat to corporations and governments.

Indeed, the fight against cybercrimes is constrained by jurisdictional challenges. Computer offenses are often transnational, giving rise to complex jurisdictional problems involving people, acts, and things present or carried out in various countries. Even when the offender and the victim are in the same jurisdiction, the needed evidence may reside in a server under a different jurisdiction (Oraegnunam, 2015, pp. 58). There is also a challenge in implementing the prosecutorial proficiency and institutional structures necessary to deal with the threats posed by cyberterrorism (Stockton and Golabek-Goldman, 2013, pp. 7). Consequently, extending the applicability of domestic laws to encompass foreign attackers can provide the much-needed and real-time basis to arraign cyberterrorists.

References

- Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, [online] 80(5), pp.973–993. doi:10.1016/j.jcss.2014.02.005.
- Norwich University Online. (2017). *Who Are Cyber Criminals?* [online] Available at: <https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals> [Accessed 30 Sep. 2022].
- Oraegnunam, I.K.E. (2015). Jurisdictional Challenges in Fighting Cybercrimes: Any Panacea from International Law. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, [online] 6, p.57. Available at: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/naujilj6&div=9&id=&page=> [Accessed 30 Sep. 2022].
- Stockton, P. and Golabek-Goldman, M. (2013). *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257915 [Accessed 30 Sep. 2022].

Reply to Post 2

I agree that the reasons for committing crimes have also not changed despite the rise in technology. However, very different organized crime groups co-occur with diverse organizational models in the digital society as humans and machines interact in new and close ways in systems of human and non-human participants (Di Nicola, 2022). These criminal groups engage in very different criminalities ranging from traditional to most technological, moving from online to offline (Di Nicola, 2022). Therefore, organized crime should be intellectualized as a binary rather than an ordinal category and as groups displaying diverse levels of strength within a continuum instead of groups with or without components defined by an arbitrary threshold (Calderoni et al.,

2022, pp. 4). Although the reasons for committing crimes have not changed, the crimes are still the same and increasing.

Admittedly, the conviction of criminals has become challenging. The legal response is failing because cybercrime is growing with an evolved threat landscape, a complex attribution in cyber contexts, and an increased number of attacks (Arnell and Faturoti, 2022, pp.1). The range of offenders and threat actors is also constantly growing (Arnell and Faturoti, 2022, pp.1). Besides, cybercrime is less constrained by monetary and physical resources than crimes in the physical world because they cause substantial harm remotely (Hui, Kim, and Wang, 2017, pp. 498). The efforts of transnational and extraterritorial jurisdiction as routine facets of responding to cybercrime are also misplaced. Fighting cybercrimes is overall characterized by inefficiencies, flaws, and injustice.

References

- Arnell, P. and Faturoti, B. (2022). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, pp.1–23. doi:10.1080/13600869.2022.2061888.
- Calderoni, F., Comunale, T., Campedelli, G.M., Marchesi, M., Manzi, D. and Frualdo, N. (2022). Organized crime groups: A systematic review of individual-level risk factors related to recruitment. *Campbell Systematic Reviews*, 18(1). doi:10.1002/cl2.1218.
- Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. doi:10.1007/s12117-022-09457-y.
- Hui, K.-L., Kim, S.H. and Wang, Q.-H. (2017). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly*, [online] 41(2), pp.497–523. Available at: <https://misq.umn.edu/cybercrime->

deterrence-and-international-legislation-evidence-from-distributed-denial-of-service-attacks.html [Accessed 30 Sep. 2022]