Article Name: Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime

Author: Fawn Ngo and K. Jaishankar

Volume 11 Issue 1 January - June 2017

1. Relation to Social Sciences Principles

The study of cybercrime delves into behavior within the world through the lens of social sciences. It investigates the influence of frameworks, cultural standards, and technological progress on crime trends and victimization. This area of study integrates insights, from criminology, sociology, psychology and law to grasp the reasons driving actions.

2. Research Questions or Hypotheses

- What are the best ways to define and classify cybercrime, in regions and legal systems?
- How common is cybercrime? What patterns can we see in its characteristics and effects?
- What are the effective strategies for fighting against and stopping activities?
- How are privacy and surveillance aspects connected to the investigation of cybercrimes?

3. Research Methods Used

Conducting surveys and interviews to collect information from individuals about their experiences with cybercrime incidents.

Examining the data from reported crimes in private sectors through methods.

Exploring real life examples to investigate strategies and top approaches in

4. Data types may include:

- Police crime reports
- Information provided by individuals through surveys aimed at those affected by cybercrime
- Insights gathered from discussions with police officers, professionals in the field, and individuals affected by the crime.
- Summarizing prevalence and trends using statistics is essential for gaining insights into data patterns and changes over time.
- Analyzing data thematically to uncover recurring themes in the experiences of both victims and practitioners.
- Exploring approaches to preventing cyber crime through an analysis.

5. Concepts Discussed in Class

- **Routine Activities Theory**
- **Social Learning Theory**.
- **Victimology**

6. Relation to Marginalized Groups

- **Vulnerability**: Certain communities that are marginalized might face increased suspicion of forms of cybercrime like identity theft and online harassment.
- **Access to Resources**: Discrepancies in access and knowledge among groups can impede their capability to defend against cybercrime effectively.

- **Discrimination and Targeting**: Certain groups could be singled out by hackers often than others which brings up issues of fairness and call for customized security measures to address this imbalance.

7. Overall Contributions to Society

- Exploring the intricacies of crime in the era to shape policies and improve law enforcement strategies.
- Raising knowledge and providing education on cybersecurity risks can empower both individuals and communities.
- Enhancing responses to cybercrime by identifying strategies and promoting teamwork among stakeholders.
- Emphasizing the importance of safeguarding privacy. Upholding standards in the context of digital monitoring to support the rights of every person.