

Article review

Open and easy to access journals that students might select articles from the International Journal of Cybercriminology, International Journal of Cybersecurity Intelligence & Cybercrime, and Journal of Cybersecurity. The reviews should focus on (1) how the topic relates to the principles of the social sciences, (2) the study's research questions or hypotheses, (3) the types of research methods used, (4) the types of data and analysis done, (5) how concepts discussed in class relate to the article, (5) how the topic relates to the challenges, concerns, and contributions of marginalized groups, and the overall contributions of the studies to society.

“Global Surge in Cyber Crimes - Indian Response and Empirical Evidence on Need for a Robust Crime Prevention System.” By Mohammed Shamiulla Arab

1. How the topic relates to the principles of the social sciences

This article touches on some of the principles of science. Let's take a look at Relativism. Throughout the article, the author keeps stressing the point of how the growth of the internet has a direct correlation to the amount of cybercrime that happens throughout the internet. He also explains some social theories related to reasoning behind cybercrime. For example, the author touches on the point of low self-control and cybercrime. This was a topic that we discussed in class so this caught my attention. The author quoted a research study that showed that people with low self-control are more likely to pirate things on the internet. These points he explains in the article are both very good examples of relativism. Now let's look at Objectivity. A majority of the article discussed the topic of India's Cybercrime Laws. One thing I enjoyed about the journal article is that he gave a great explanation of India's cybercrime laws without interjecting with opinion-based ideas. He did suggest that India needs to “develop robust IT crime prevention systems' ” but I interpreted this as a suggestion/conclusion rather than an actual opinion. The author did a good job in keeping his article objective. The last Major principle I want to discuss pertaining to the article is parsimony. With me just beginning my journey into mastering the skills and knowledge of cybersecurity and social science, I still tend to be ignorant to some of the terms and meanings relating to these topics. The author was able to convey his message and research without me being confused. The article was simple enough that I was able to follow it without having to cross research his findings while reading. The author's ability to do this showed that he followed the principle of parsimony.

2. the study's research questions or hypotheses

The abstract was where I was able to extract or assume his research questions and or hypothesis. Though the author never exactly stated his research questions, he made it clear what his intentions for the research article were. His main research question, I assume after reading the article, was the topic of cybercrime. This was obvious but he broke down this topic into different subcategories. I also assume that his sub-category research questions were based around the underlining topics of global cybercrime, how certain countries deal with cybercrime, the history of cybercrime, the transformation of cybercrime, and also the analytics of global cybercrime. This last sub-question in the list(just stated) helped me get to the assumption of the author's thesis. This and that the author practically stated his, what I assume to be, hypothesis in the abstract stating "... [the article] analyzes the various measures used in addressing the crime and the challenges faced. Based on the analysis, the future of cybercrime can be easily analyzed to determine based on the effectiveness of the existing measures and policies governing cyber criminology and justice systems globally." This statement is what I presumed to be his hypothesis,

3. the types of research methods used

Most of the research in the article came from archival research. Other types of research wouldn't have been as beneficial due to his topic being based around the global aspect of cybercrime. Using an experiment, field study, and or surveys didn't seem as adequate leaving archival research as one of the only logical methods to use in the author's situation.

4. the types of data and analysis done

The author pulls a lot of data and statistics dealing with cybercrime and even specific attacks such as Ransome ware attacks. He shows this data by stating statistics in statements and even lacing the article with occasional graphs. He gave a graph about the number of cybercrimes reported in India and even gave a graph about countries with the highest ransom infections rates. These gave a great visual representation of some of the stats dealing with cybercrime. Although he shows this data he also analyzes it and explains a reason why the numbers are the way they are. For example, after he shared the graph showing the stats of ransomware infections between countries, the author also gave a possible explanation of why some of the countries with higher numbers are the way they are. Thailand was one of the countries with the highest number of ransomware infections in the year 2017-2018. The author goes on to explain this number being

so high, stating that due to the exponential growth of internet technology more people are online thus making a higher possibility of attacks. He also goes on to explain that, like India, most of the countries on the graph's cyber criminology defense infrastructure aren't advanced enough to stop such attacks. Other than giving an explanation for the statistics I found that the author also backs his claims by using statistics and data. For example Shamiulla discussed the topic of the gender gap between those who commit cyber crimes. The author went on to explain that gender was a "significant predictor" when it came to hacking and cyber crimes stating "[illegal downloading]... males were 1.46 times more likely perpetrators; however, when it comes to hacking, the difference was much more pronounced; up to 2.85 times more likely than females." The author did a good job in analyzing and explaining some statistics and also backing his own ideas with statistics.

5. how concepts discussed in class relate to the article,

This article sparked a lot of thoughts about things we talked about in class. The author has a section named "Theories Used in Guiding Global Legal Response to Cybercrime" and this section related a lot to what we discussed in class. In class, we discussed some of the theories behind people committing cyber crimes and also some commonly found patterns found amongst hackers and cybercriminals. The author touches on topics about the gender ratio of hackers, schools' impact on hackers, parents' impact on hackers, and also some other theories like self-control and neighborhood integrations. These go hand in hand about some of the social cyber criminology-based topics we discuss in class. This helped me understand this section more, actually, because I could think back to what we learned in class. I also remember in class that we briefly talked about human error when it comes to cyber or technological complications. Our discussion relates to another section in the article. The article touches on the topic of educating the public on the topic of cyber attacks and the threats of cybercrime. These two topics relate because a lot of cyber-attacks are when the hacker socially engineers the victim to give up information. With the human error part being falling for the attack and the need for educating the public about these attacks to avoid it, these two topics go hand in hand.

6. how the topic relates to the challenges, concerns, and contributions of marginalized groups and the overall contributions of the studies to society.

This topic discussed in the article has a lot about different groups (marginalized ones included) and offers a lot of information that could be beneficial to the further studies of cyber criminology in society. The author of this article talks a lot about the cybercrime situation that

takes place in India. With India and other emerging technological countries dealing with a boom of internet technology we are tending to see a significant growth in cybercrime simultaneously. The author shed a lot of light on this topic and offers some interesting points when it comes to ways to further prevent the growth of cyber crime. With the internet still being relatively “new” in some countries, talking about cybercrime in such countries is crucial; especially with there being an inevitable growth of internet tech. What the author does a good job in this article is that he talks about both sides of cybercrime. While stating the positive reasons of the ways countries prevent and deal with cyber crime, he also adds some of the negative impacts they may have on the country as a whole. This allows the creators of such rules and regulations(if they were to take consideration of this article) room to grow and morph such policies to make it as efficient as possible. If we were to only research the ways cybercrime prevention is good and neglect the negative effects it wouldn't be the most efficient for everyone. For example, The author quoted another article explaining how some countries are nervous about the negative effects of cyber crime prevention such as civilian personal privacy, security, and also the effects it could have with the economy. Offering points like these only promotes further research on how to shape policies and regulations to avoid some of these negative effects.