Clarence V. Kimbrell Jr.
Article 2 Review
201 Cyber Security and Social Science
Professor Armistead

Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks

By Nori Katagiri

The introduction of this article sets the foundation for the rest of the compelling argument about international laws and norms. Hackers and malicious online attackers were given a divine blessing by the increased number of users online. More people participating in online activities means more people they could prey on. The number of hacks, malware, and phishing attacks skyrocketed during the pandemic. The argument states despite the rise of these very predatory means of accessing people's information very little was conducted about or how to prevent it on a global scale. Misinformation campaigns about the virus and vaccination were running rapidly which in turn altered people's mindset about the problem. This further proves the point that it was looked past and may not have even been considered as a factor. Governments around the world have state-sponsored hacking groups or targets, and which they have to abide by the rules and regulations of the state. Then arises the problem of how little effort to regulate non-state-sponsored cyber-attacks within a state is left to anarchy. This topic relates to the principles of social sciences because of equity or the lack of it in this case. Pushing for only state-sponsored cyber-attacks and not within a state can be very problematic for its population. This article aims to study how international politics and policies play a very big role in cyber-attacks conducted globally. The main type of research method used to analyze this information was the use of case studies of a specific event and a specific process. These case studies were able to bring together a strong hypothesis that proves Nori's point on an international level. There are many concepts discussed in the article that we have covered in class such as motives for hackers and cultures that are created in the world of hacking. This article contributes to the organizations within states such as Microsoft to have to protect their programs at very high costs. Instead of the failures that international law and norms have yet to accomplish. Katagiri's article on international law and norms doing very little in preventing non-cyber attacks shines a light on how these are not accomplishing much and need to be reworked and looked at. This can be looked at in many ways Nori suggested that "the need for reconsideration of state commitment to the existing international legal and norms system as a preventive mechanism against non-state OCO[1].

[1] OCO stands for Overseas Contingency Operations. Normally shorted to just OCO for convenience.

Source:

Nori Katagiri, Why international law and norms do little in preventing non-state cyber attacks, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, tyab009, https://doi.org/10.1093/cybsec/tyab009