# Article information:

taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate | Journal of Cybersecurity | Oxford Academic
<https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288>

# Article summary:

1. This article surveys the literature to understand the nature of cyber-harm and to create a taxonomy of cyber-harms encountered by organizations.

2. The taxonomy comprises five broad themes: physical or digital harm; economic harm; psychological harm; reputational harm; and social and societal harm.

3. The article also analyses four real-world case studies to provide initial indications about how different types of harm are connected and how cyber-harm in general may propagate.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article is generally reliable, as it provides an extensive literature survey on the concept of cyber-harm, as well as a detailed analysis of four real-world case studies. The authors have provided evidence for their claims, such as citing relevant sources from criminology, economics, news articles, databases, etc., which adds credibility to their argument. Furthermore, the authors have presented both sides of the argument equally by providing insight into potential risks associated with cyber-attacks and discussing security controls needed for treatment of harm.

However, there are some areas where the article could be improved upon. For example, while the authors have discussed various types of harms that can result from cyber-attacks, they do not provide any evidence or data to support their claims about how these harms propagate or interact with each other. Additionally, while they discuss potential risks associated with cyber-attacks, they do not provide any concrete solutions or recommendations for mitigating these risks. Finally, while they discuss security controls needed for treatment of harm, they do not provide any specific details on what these controls should be or how they should be implemented in practice.

# Topics for further research:

* Cyber-attack risk mitigation strategies
* Cyber-attack prevention techniques
* Cyber-harm propagation models
* Cyber-harm economic impact
* Cyber-attack security control implementation
* Cyber-attack legal implications

# Report location:

<https://www.fullpicture.app/item/97b9daf47250ab7d60b80ed282a584be>