

## Review Form 1.7

Journal Name:	<b>Current Journal of Applied Science and Technology</b>
Manuscript Number:	<b>Ms_CJAST_116951</b>
Title of the Manuscript:	<b>Bias and Fairness Issues in Artificial Intelligence-driven Cybersecurity</b>
Type of the Article	

### **General guideline for Peer Review process:**

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty**', provided the manuscript is scientifically robust and technically sound. To know the complete guideline for Peer Review process, reviewers are requested to visit this link:

(<https://www.journalcjast.com/index.php/CJAST/editorial-policy> )

**Review Form 1.7**

**PART 1: Review Comments**

	<b>Reviewer's comment</b>	<b>Author's comment</b> (if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)
<p><b>Compulsory</b> REVISION comments</p> <p>1. <b>Is the manuscript important for scientific community?</b> (Please write few sentences on this manuscript)</p> <p>2. <b>Is the title of the article suitable?</b> (If not please suggest an alternative title)</p> <p>3. <b>Is the abstract of the article comprehensive?</b></p> <p>4. <b>Are subsections and structure of the manuscript appropriate?</b></p> <p>5. <b>Do you think the manuscript is scientifically correct?</b></p> <p>6. <b>Are the references sufficient and recent? If you have suggestion of additional references, please mention in the review form.</b></p> <p><b><u>(Apart from above mentioned 6 points, reviewers are free to provide additional suggestions/comments)</u></b></p>	<p>1. The manuscript appears to be important for the scientific community as it addresses the critical issues of bias and fairness in the application of artificial intelligence for cybersecurity. With the increasing use of AI in cybersecurity systems, it is crucial to understand and mitigate potential biases and ensure fairness to maintain the reliability and trustworthiness of these systems.</p> <p>2. The title "Bias and Fairness Issues in Artificial Intelligence-driven Cybersecurity" is appropriate and accurately reflects the main focus of the manuscript.</p> <p>3. The abstract provides a comprehensive overview of the manuscript's aim, significance, discussion, and conclusion. It covers the key points discussed in the paper.</p> <p>4. The subsections and structure of the manuscript are generally appropriate. It follows a logical flow, starting with an introduction, discussing the intersection of cybersecurity and AI, examining the areas of AI deployment in cyberspace, and then delving into the sources and solutions to bias and fairness issues.</p> <p>5. The manuscript appears to be scientifically correct based on the information provided. The authors have cited relevant references to support their claims and have discussed the topic comprehensively.</p> <p>6. The references cited in the manuscript appear to be sufficient and cover both recent and older relevant sources. However, the manuscript could benefit from the inclusion of some additional recent references to strengthen the discussion on bias and fairness in AI-driven cybersecurity.</p>	
<p><b>Minor</b> REVISION comments</p> <p>1. <b>Is language/English quality of the article suitable for scholarly communications?</b></p>	<p>The language and English quality of the article are suitable for scholarly communications. The writing is clear and coherent, with proper use of technical terminology and formatting.</p>	
<p><b>Optional/General</b> comments</p>	<p>The introduction section could benefit from a more concise and focused overview of the key problems and motivations behind examining bias and fairness in AI cybersecurity systems. Currently, it provides a broad background on AI and cybersecurity but does not clearly articulate the specific challenges or importance of addressing bias/fairness until later sections.</p> <p>While the manuscript discusses the main drivers of bias (data, algorithms, teams), the analysis of how each of these sources can introduce bias is relatively brief. More in-depth examples and analysis of real-world cases where bias crept in from these sources in cybersecurity contexts could strengthen this section.</p> <p>The definitions and examples of different fairness concepts (individual, group, counterfactual) are valuable. The manuscript could benefit from more technical depth on mathematical formulations and operationalizations of these fairness definitions.</p> <p>The bias mitigation taxonomy in Figure 3 is useful, but the text discussion of specific mitigation techniques is limited. More details on state-of-the-art algorithmic debiasing methods, data preprocessing, and model auditing approaches would make this a more complete technical treatment.</p> <p>While theoretical concepts are well-covered, the lack of real-world case studies examining bias issues in deployed AI cybersecurity systems is a missed opportunity. Illustrative examples could make the concepts more concrete.</p>	

[Review Form 1.7](#)

**PART 2:**

	<b>Reviewer's comment</b>	<b>Author's comment</b> <i>(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)</i>
<b>Are there ethical issues in this manuscript?</b>	<i>(If yes, Kindly please write down the ethical issues here in details)</i>	

**Reviewer Details:**

Name:	<b>Eduard Manziuk</b>
Department, University & Country	<b>Khmelnytskyi National University, Ukraine</b>