ANALYSIS OF ETHICAL IMPLICATIONS OF NATO’s CYBER DEFENSE POLICY

Today we will be looking at the ethical implications that arise from 2024 NATO Cyber defense policy. Specifically, we will be going over the ethical issue of using advanced integrated AI systems and large machine learning models designed to monitor complex networks that this cyber defense policy seeks to use to enhance NATOs cyber defense. To start we will be doing an analysis of these particular issues and concerns to address whether these problems are valid or not. To start we will be going over in more depth the ethical issues as well as a cost and benefit analysis to see whether or not the actions that this policy is seeking to make is worth the possible ethical infringements, then we will take a look at the rights that are protected or limited by the policy on a large scale as well as on an individual basis and then lastly the conclusion. Now let us begin with the first section “the ethical implication and the cost and benefits of them”

Now you already know of the main ethical issues I will be addressing today being the use of advanced integrated AI systems as well as the possible sharing of civilian data to foreign nation states, but why are people concerned with the ethics of this? Well to start let us first address NATOs cyber defense policy use of advanced AI systems and why people have problems with it. Now within NATOs new cyber defense policy it seeks to use AI to help create a transformative cybersecurity shield(Cybersecurity, 2024). The policy also seeks to use AI to constantly analyze and network behaviors while using anomaly detection tools to find potential cyber threats (Cybersecurity, 2024). The ethical problems with using such a system comes in when you are confronted with the possibility of having biased datasets or the AI simply not having access to complete information which would lead to false positives of threats which then could led to innocent people becoming the target for law enforcement when there was no foul play to being with. Now even with this large problem could it be that this approach is still beneficial overall? Well I wouldn't say so. The use of advanced AI and large machine learning models that would be needed for this to work would cost upwards of 100,000 dollars(*How Much Does AI Cost in 2025*, n.d.) and even then with systems this complex it is hard to use it on a large scale that would be needed by NATO(Edozie et al., 2025) Not to mention the amount of money need for research and development for such a system. Now let us continue to the rights that this policy protects or limits due to the use of these AI and machine learning systems.

Now with this policy seeking to secure the NATO member states and its civilians digital infrastructure it is actively seeking to protect its citizens rights to digital privacy and safety even if it means giving up some of that same privacy to NATO due to the policies use of AI and machine learning, which may be much better than it ending up in the hands of a foreign adversary or criminal cybercrime group. Now even though this does protect the rights of the people on a larger scale it doesn't necessarily protect the rights of people on the individual level, because of the AI and machine learning models using individual digital information to gather and analyze information to find threats.

In conclusion, NATO’s new 2024 cyber defense policy has ethical concerns regarding its use of AI and machine learning technologies to enhance its cyber defense. The concerns come from the AI and machine learning models needing to intact large amounts of data from complex networks in order to properly and accurately identify possible cyber threats to NATO, which may lead to individual data being taken by these programs leading to NATO and by association other nation states within the alliance also having access to such data which could infringe on a person right to privacy. The cost of using such a system was also covered and it could cost upwards of 100,000 dollars to implement with also the drawback of such systems not being easily scalable for large operations, and lastly we covered the rights that this policy may protect or limit due to its use of AI. Ultimately this cyber defense policy does protect the rights of the people on a large scale from hostile actors but at the sametime limits those same rights on an individual basis.

SOURCES:

Cybersecurity, D. (2024, December 3). *NATO Cyber Defense: 2024 Strategic Update*. https://www.linkedin.com/pulse/nato-cyber-defense-2024-strategic-update-decentcybersecurity-fo2jc/

Edozie, E., Shuaibu, A. N., Sadiq, B. O., & John, U. K. (2025). Artificial intelligence advances in anomaly detection for telecom networks. *Artificial Intelligence Review*, *58*(4). https://doi.org/10.1007/s10462-025-11108-x

How Much Does AI Cost in 2025. (n.d.). DDI Development. https://ddi-dev.com/blog/programming/how-much-does-ai-cost/