ANALYSIS OF SOCIETAL INFLUENCES ON NATO'S CYBER DEFENSE POLICY

Today, I will be doing an analysis of the social implications of NATO's 2024 cyber defense policy. The reason for this analysis is that even though NATO's cyber defense strategy is for protecting its member states and their civilians there may be unforeseen societal effects as a result of it whether it be negative or positive, it is also possible that the reverse could be true and that societal factors lead a role in the development of NATO's cyber defense plan. So in an effort to learn and understand the possible pros and cons of this cyber policy's effects on our society or our societies effects on NATO's cyber plan we will be going over a few things. The starting sub-subject we will be going over is the possible social factors that may have caused the need for this policy, the social consequences this policy may arise, Cultural/subcultural influences on the policy, and lastly the conclusion of the findings we found today. Now let us begin with our first sub-subject "social factors".

With the rapid growth of technology, especially digital technology, it has become more and more important that we gain access to better, more sophisticated defenses against digital threats, especially those that can pose an existential crisis to the public. With cyber threats like this looming over our heads it shouldn't be surprising when the people start to call for greater cyber defense capabilities to ensure their countries safety from cyber attacks especially when those attacks could possibly bring down an entire county by targeting critical infrastructure. Cyber warfare is also causing a mass concern for people's privacy online and offline(*NATO PA*, 2025), which all factors into the public pushing for more attention being paid to gain a better deal to security against cyberattacks whether it be spyware, ransomware, or your typical malware attack. Now that you understand one of the leading societal factors in NATOs attempt to bolster

its defense against cyber warfare, let us go on to the possible social consequences that this policy might bring about.

Now with there being pressure from social groups to build a better security against cyber threats there will also come certain consequences that will follow. One being that with this new development of better cyber security the public may be faced with possible government overreach under the guise of digital protection. This is especially a concern with NATOs cyber defense policy also stating that they wished to use advanced AI and machine learning to scan for cyber threats which may further reduce civilian digital privacy online or maybe even offline to some extent(Murray et al., 2023). Now that you know of the potential societal consequences this digital defense strategy may bring, let us now continue on to how cultural and subcultural influences have shaped NATO'S defense policy.

Now to begin, let's first start off with the cultural influences that have shaped this cyber defense policy. The main cultural influences within NATO that had a hand in shaping what this cyber defense policy would be is simply NATOs main ethos to mutually support member states with defense, which not only applies to physical threats to member states but also digital threats as well. Now for the subculture that helped shape this policy would be NATOs underlying need to improve its security standards in an effort to keep up deterrence from hostile nation states and the only way to do this is to advance their own digital security technology and techniques(Piper, 2024).

In conclusion, the societal factors that lead to the creation of NATO’s 2024 cyber defense policy is the going concern over cyber attacks within our ever growing technological society and the need for more advanced technologies and techniques to deal with these fast evolving cyber threats. The consequences that occurred as a result of this policy's creation is the possible

overreach by the government, which could lead to a loss of privacy for the public not only online but possibly also offline as well. The cultural and subcultural influence that played a role in this policy is NATO's responsibility to provide a mutual shield amongst its member states to protect the entire alliance from attack, which also includes cyber attacks. This meant in order for NATO to properly maintain deterrence against adversary nations it needed to develop a way to better defend itself against cyber attacks which led to the making of NATO cyber defense policy to guide the alliance in the right direction to develop and deploy more secure and effective cyber security tools.

SOURCES

Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A. (2023). The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe. *Journal of Human Rights Practice*, *16*(1), 397–412. https://doi.org/10.1093/jhuman/huad020

***NATO PA*. (2025, April 3). NATO Strategic Concept Must Tackle Cyber Challenges, Climate-related Security Issues | NATO PA. https://www.nato-pa.int/news/nato-strategic-concept-must-tackle-cyber-challenges-climate-related-security-issues**

Piper, E. (2024, November 25). Russia will not intimidate us with cyberthreats, UK minister tells NATO. *Reuters*. https://www.reuters.com/technology/cybersecurity/britain-nato-must-stay-ahead-new-ai-arms-race-says-uk-minister-2024-11-25/