NATO Cyber Defense Policy: A Social Breakdown

James F. Keith

CYSE425W: Cybersecurity Strategy and Policy

Professor Hamza Demirel

April 6, 2025

NATO Cyber Defense Policy: A Social Breakdown

The North Atlantic Treaty Organization (NATO) Cyber Defense Policy is a strategic response to the growing cyber threats in our increasingly interconnected world. This policy goes beyond technical aspects; it carries significant social implications, influencing societal values, behaviors, and inequalities. By examining the social factors that contributed to its creation, its societal impacts, and the cultural and subcultural dynamics that have shaped it, the complex relationship between NATO's cyber strategies and the broader social context is uncovered.

Societal shifts toward digital reliance and escalating cyber risks propelled the development of NATO's Cyber Defense Policy as societies increasingly relied on critical infrastructures. Whether it be communication networks or power systems, significant disruptions could destabilize the worldwide social order. Komalasari and Mustafa (2023) note that "In today's interconnected world, where digital technologies permeate every aspect of society, international cyber conflicts have emerged as a pressing global concern" (p. 2). As a result, robust policies like NATO's are needed to safeguard the systems these technologies rely upon. Furthermore, this change reflects a broader societal demand for security in an era where cyber threats, ranging from state-sponsored attacks to data breaches, pose a significant threat to everyday life.

NATO's Cyber Defense Policy yields both unifying and divisive social outcomes. Fostering coordinated cyber defenses enhances societal trust in institutions that protect digital infrastructure. However, this technical focus can exacerbate social inequities. Cavelty et al. (2023) notes that "Although cyber resilience is theoretically compelling, and despite the announcement by many organizations that becoming cyber resilient is one of their goals, it remains a vague and elusive concept that is hard to implement" (p. 2). Cyber policies, like

NATO's, often ignore the varied coping abilities of individuals and communities. Wealthier nations can utilize advanced defenses, while less-resourced groups and marginalized communities become increasingly vulnerable, thereby widening digital divides. This disparity shows that the policy may inadvertently reinforce systemic inequalities based on access to technology and resources.

Cultural and subcultural elements have profoundly shaped NATO's Cyber Defense Policy, embedding it with values and priorities from its member states. The policy reflects a Euro-Atlantic cultural emphasis on democracy and technological progress, influencing its proactive stance. Creese et al. (2021) notes that "The capacity of a nation to build online security might well depend on the attitudes, values, and practices of Internet users, such as their awareness of security risks, their online habits and practices, and the prioritisation they place on their security" (p. 1). This underscores how cultural norms of trust and governance inform NATO's strategies. Furthermore, the policy is subculturally shaped by NATO's military and technical communities, which prioritize operational efficiency and collective defense principles. However, this technocratic emphasis may conflict with civilian cultures that prioritize inclusivity and diversity.

NATO's Cyber Defense Policy is a socially influenced framework driven by the dependence on digital systems and the requirement for resilience against unpredictable threats. While it strengthens security and trust, it also has the potential to exacerbate social inequalities, highlighting the dual aspects of collective cyber defense. As cyber threats continue to evolve, it will be crucial to incorporate social considerations to ensure that the policy equitably serves all societal segments.

References

Cavelty, M. D., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. Journal of Risk Research, 26(7), 2. https://doi.org/10.1080/13669877.2023.2208146

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. Personal and Ubiquitous Computing, 25(5), 1. https://doi.org/10.1007/s00779-021-01569-6

Komalasari, R., & Mustafa, C. (2023). Combating International Cyber Conflict: A Healthy Just War and International Law Analysis of NATO and Indonesian Policies. Jurnal Pertahanan, 9(3), 2. https://dx.doi.org/10.33172/jp.v9i3.16867