NATO Cyber Defense Policy: An Ethical Breakdown

James F. Keith

CYSE425W: Cybersecurity Strategy and Policy

Professor Hamza Demirel

March 23, 2025

NATO Cyber Defense Policy: An Ethical Breakdown

NATO prioritizes cyber defense due to rising threats from hostile nations and actors. While enhancing cybersecurity is vital, NATO's Cyber Defense Policy raises ethical concerns regarding how such information is collected. Therefore, the moral implications of the policy are examined by evaluating its costs, protection of rights, and alignment with individual rights.

NATO's Cyber Defense Policy enhances the security of member states against cyber threats through collective defense, which helps deter adversaries and coordinate responses to incidents. This approach improves information sharing, resource allocation, and strategic planning. Lonsdale (2020) notes that "deterrence includes defensive security measures for denial, norms against aggressive behavior, and commitment to cross-domain retaliatory capabilities" (p. 24).

However, these benefits entail costs. Cyber defense requires significant investments in technology, infrastructure, and personnel training. The rapid evolution of cyber threats demands ongoing updates to defense strategies, leading to recurrent expenditures. Lonsdale (2020) notes that "the economic costs of cybersecurity are considerable" (p. 20). This raises concerns about opportunity costs and whether prioritizing cybersecurity undermines other social-based tasks.

NATO's Cyber Defense Policy protects essential rights like national sovereignty, economic stability, and data protection. Countering cyber threats and safeguarding critical infrastructure reinforces member nations' financial interests and indirectly shields citizens' data from rogue actors. However, it also limits other rights, including privacy, freedom of expression, and autonomy. Fidler, Pregent, and Vandurme (2013) note that "advocates of civil liberties, such as the right to privacy, tend to oppose on constitutional and international human rights grounds proposals to increase governmental authority to conduct electronic surveillance and increase

information sharing between governments and non-governmental entities" (p. 18). Lonsdale (2020) further warns that state-imposed cybersecurity controls "weakens public faith in the state" (p. 29). Lastly, Stroppa (2023) cautions, "The increasing use of AI in cybersecurity, however, presents important downsides that need to be taken further into account" (p. 3).

While NATO's cyber defense policy aims to protect member states and citizens, autonomous cyber capabilities raise ethical challenges due to their unpredictability and insufficient human judgment. Retaining human control in operations is crucial for upholding ethical standards. Stroppa (2023) argues that "in order to promote a responsible use of AI in cyberspace for military purposes, a possible way out of the above-mentioned concerns might be that of exercising a context-based degree of human control on autonomous cyber capabilities" (p. 1).

Moreover, the policy must comply with international legal frameworks governing cyber operations. This compliance ensures that measures do not violate individual or national rights. However, the unique nature of cyber warfare complicates applying traditional legal and ethical frameworks, as noted by Fidler et al. (2013): "Whether NATO members could agree on what offensive cyber operations international law would permit is also not clear, especially in light of difficulties cyber presents to the international law on armed conflict revealed by the Tallinn Manual and other analyses" (p. 24). Thus, tailored guidelines are necessary to address these specificities in cyber operations.

NATO's cyber defense policy is pivotal in safeguarding member states against evolving cyber threats. However, it introduces ethical implications that require careful consideration, particularly concerning the balance between collective security and individual rights. Ensuring that cyber defense measures are transparent, accountable, and compliant with international legal and ethical standards is essential to uphold the rights they aim to protect.

References

Fidler, D. P., Pregent, R., & Vandurme, A. (2013). NATO, Cyber Defense, and International Law. *Journal of International and Comparative Law*, *4*(1), 18, 24. https://scholarship.law.stjohns.edu/jicl/vol4/iss1/1/

Lonsdale, D. J. (2020). The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios. *Journal of Military Ethics*, *19*(1), 20, 24, 29. https://doi.org/10.1080/15027570.2020.1764694

Stroppa, M. (2023). Legal and ethical implications of autonomous cyber capabilities: A call for retaining human control in cyberspace. *Ethics and Information Technology*, *25*(7), 1, 3. https://doi.org/10.1007/s10676-023-09679-w