Is NATO's Cyber Defense Policy Effective?

James F. Keith

CYSE425W: Cybersecurity Strategy and Policy

Professor Hamza Demirel

April 20, 2025

Is NATO's Cyber Defense Policy Effective?

The evolution of NATO's Cyber Defense Policy reflects a strategic response to the increasing complexity of cyber threats in an interconnected world. The question, however, is whether the policy has effectively defended members' digital infrastructure as a collective. Answering this question requires in-depth research and examining how effective the alliance's response to emerging cyber threats is through scholarly and individual assessments.

In determining the effectiveness of the NATO Cyber Defense Policy, one must first examine research conducted by experts to see their perspective. Mad'ar (2019) gives a positive assessment, describing NATO as "a self-aware and confident organization that takes measured steps to enhance the cyber security of the Alliance as a whole" (p. 1). He notes that "given that the Alliance retains a consensus-based decision-making, its progress in the cybersecurity agenda has been substantial in the past five years" (p. 17-18), highlighting how the alliance overcomes constraints to make significant advancements.

Efthymiopoulos (2019) gives a more neutral assessment, highlighting the pros and cons of the NATO Cyber Defense Policy. He states that "a cyber-security strategy for NATO will enhance its innovation and creativity core of operations and methodologies against any kind of virtual threats" (p. 5). However, Efthymiopoulos does critique the lack of a unified legal framework, noting that "cyber-security is yet to be globally, legally, operationally, and strategically defined" (p. 3).

Hasanov, Iskandarov, and Sadiyev present a predominantly negative view of the NATO Cyber Defense Policy, noting that "there are three main reasons of why NATO is still not sufficient on collective cyber security" (p. 9). They highlight differing capabilities among members, frequent threat changes, and difficulties communicating with the private sector as

reasons why the policy fails to hold up. This is noteworthy, as though the policy has advanced, limitations abound when implementing policies.

After reviewing expert assessments of the policy, I'd base my evaluation on three main factors: resilience, deterrence, and interoperability. Resilience assesses the policy's ability to support member states during cyber incidents with tools and resources, while deterrence identifies offensive capabilities available to alliance members to deter possible attacks. While both are important, interoperability is crucial since NATO's 32 member nations must be able to collaborate and share information freely to prevent potential cyberattacks.

Considering all factors, I believe the NATO Cyber Defense Policy is moderately successful. Institutional advancements like the Cyberspace Operations Center enhance resilience and deterrence but raise ethical questions since the public perceives NATO activities with a defensive mindset. Politically, the policy is a great success as it showcases strong international collaboration with little risk, which enemy states like China and Russia abhor. Socially, the policy is gaining momentum as it embraces transparent communication. Though public trust is subpar, engagement with civil and industrial societies throughout the alliance will slowly increase its approval.

Through scholarly and individual evaluations, the effectiveness of the NATO Cyber Defense Policy demonstrates above-average progress. From its reactive beginnings at the turn of the 21st century to operational maturity in the late 2010s, NATO has established a policy framework capable of addressing modern threats. Although cyber threats continue to evolve, NATO's cyber defense capabilities remain prepared to handle them with strategic readiness. These preparations ensure that member nations can collectively create a safe and secure digital world through continued collaboration and innovation for future generations.

References

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. Journal of Innovation and Entrepreneurship, 8(1), 3, 5. https://doi.org/10.1186/s13731-019-0105-z

Hasanov, A. H., Iskandarov, K. I., & Sadiyev, S. S. (2019). THE EVOLUTION OF NATO'S CYBER SECURITY POLICY AND FUTURE PROSPECTS. Journal of Defense Resources Management, 10(1), 9. https://www.proquest.com/docview/2229616469/fulltextPDF?accountid=12967&pq-origsite=primo&sourcetype=Scholarly%20Journals

Mad'ar, T. (2019). Lagging colossus or a mature cyber-alliance: 20 Years of Cyber Defence in NATO. *Obrana a Strategie*, *19*(1), 1, 17-18. https://doi.org/10.3849/1802-7199.19.2019.01.005-022