NATO Cyber Defense Policy: A Breakdown

James F. Keith

CYSE425W: Cybersecurity Strategy and Policy

Professor Hamza Demirel

February 2, 2025

NATO Cyber Defense Policy: A Breakdown

According to Blessing et al. (2021), “After Estonia’s 2007 cyber incident, NATO members had a greater urgency to address cyberspace challenges and, in January 2008, approved an initial *Policy on Cyber Defense*” (p. 266). The NATO Cyber Defense policy has since been updated in both 2011 (Blessing et al. (2021)) and in 2021, when President Biden and leaders from the other nations that make up NATO endorsed a new cyber defense policy that determines the circumstances necessary to invoke Article 5 on a “case-by-case basis” (Gill, 2021). The NATO Cyber Defense Policy is the guide that both NATO and its members use to secure their critical infrastructure and information systems from outside attacks. With this strategy, NATO can ensure its defense posture is solidified while enhancing its members' resilience as cyber threats evolve.

In choosing the NATO Cyber Defense Policy, I chose a policy that I feel closely relates to my future career path and one that I am familiar with. I have closely followed NATO news and guidelines for the past few years as I learned more about the alliance, especially once Finland and Sweden joined. NATO is a unified alliance of countries that relies on Article 5 protection, which states, "If a NATO allied nation is attacked, it would be considered a mutual act of violence against all other members who will take actions to respond” (Gill, 2021).

The NATO Cyber Defense Policy was developed after Estonia was subjected to massive cyberattacks from Russia in 2007. It took several years after the hybrid attack on Estonia for NATO to fully understand the necessity of creating a cyber defense policy. Still, it took the unveiling of the Stuxnet virus in the late 2000s to show that Cyberspace protection was critical. According to Slobodchikoff et al. (2021), “In 2016 NATO declared that cyberspace would be the

new domain of Warfare. Nations pledged to promote their own cyber defenses and various NATO means and measures were enhanced, including a NATO cyber range" (p. 153).

The declaration significantly changed how NATO and its members secured their digitally based infrastructure. Protection of military data and communication was given the same, if not higher, priority over the security of physical assets, and individual nations worked to ensure that they had the means to protect their citizens and data. However, these protections can only go so far, as governments cannot secure data that is not stored on government-owned servers or devices. Most data is controlled by private third-party providers with their own vendors, systems, and security measures. Though nations are working with the private sector to ensure the necessary precautions are in place, vulnerabilities still need to be patched to ensure that cyber attacks are unsuccessful.

As with all policies, the NATO Cyber Defense policy only guides the organization and its member states. Each member state has specific guidelines and regulations for securely storing data. However, the evolution of hybrid warfare by enemy states has grown significantly over the past 20-25 years, requiring all Alliances and countries to enhance their defense posture towards cyber threats. The US-Israeli Stuxnet virus served as a wake-up call to all nations that cyber-attacks can do significant damage with minimal blowback. Therefore, it's in the interest of NATO to be ready for all cyber threats and have the necessary policies to protect the alliance and its member states.

References

Blessing, J., Elgin, K. K., Ewers-Peters, N. M., & Tiderman, R. (2021). NATO 2030: Towards a New Strategic Concept and Beyond (pp. 266-267). Brookings Institution Press. https://muse.jhu.edu/pub/11/oa_edited_volume/book/99306/pdf

Gill, J. (2021). NATO Members Endorse New Cyber Defense Policy. Inside the Pentagon's Inside the Navy, 33(24). https://www.proquest.com/docview/2543413345/fulltext/DBFACC3BF7254463PQ/1?accountid=12967&sourcetype=Trade%20Journals

Slobodchikoff, M. O., Davis, G. D., & Stewart, B. (2021). The Challenge to NATO : Global Security and the Atlantic Alliance (pp. 153-154). Potomac Books, Incorporated. https://ebookcentral.proquest.com/lib/odu/reader.action?docID=6715587&ppg=1