**ANALYSIS OF NATO CYBER DEFENSE POLICY**

Today I will be doing an analysis of the NATO Cyber Defense Policy. I have chosen this policy because of the growing cyber attacks happening around the world and with the cyber domain becoming more and more important to nations and civilians it has become of utmost importance for our nations within the nato alliance to be able to defend ourselves from cyber attacks as well as be competent in delivering our own cyber warfare to our enemies as a means of deterrence(Nato, n.d.). This policy from NATO details in detail how the alliance will increase our resilience to cyber attacks as well as developing collective response frameworks that will allow for effective and quick responses to cyber breaches. This is very important in today's world especially with the rise of great power competition and the growing rate of hybrid warfare that use cyber attacks to not provoke an armed response from a nation(Giordano, 2024). Now that you understand why we are having this analysis, let's go over the different sections we will be covering today. For starters we will be explaining what a cybersecurity policy is then we will conduct a policy overview which will also explain why it was made followed by what the policy will do and how it will be applied. Now let us begin with our first section “what is a cybersecurity policy”.

Before we can begin going further into the details of NATOs new cyber defense policy you must first understand what I mean by a policy more specifically a cybersecurity policy which is what NATOs new policy is. Simply this type of policy is a set of rules and guidelines that a company or government needs to follow in order to ensure they are efficiently using their resources appropriately to secure their digital infrastructure. Now that you understand what this type of policy is, let's go over the policy overview.

This policy is a framework created by NATO to ensure our member states are able to strengthen our resilience to modern day cyber security threats especially those posed by adversary nations. This policy outlines and makes clear the importance of digital security and how it will lead to greater national security for all of its member states if correctly applied leading to a stronger state and alliance overall. It also addresses integration cyber security response and security between member states to further increase our ability to contain and defend against any cyber threats using the combined resources of everyone within the alliance allowing us the ability to have the best possible response, security, and breach containment possible(Nato, n.d.-b). Now let's go into more depth into what this policy will actually do. Now that you understand the general idea of this policy lets go over how it will be implemented.

NATO is going to implement this policy by a few different means which include political, military and technical authorities within the decision making body to monitor its progress and for political oversight to ensure everything is on track and doing what it is supposed to do(Nato, n.d.). This also makes sure that individual member states stay committed to developing and implementing the necessary technologies to ensure the success of this policy. More specifically the political body is responsible for making sure everything stays on task, time and budget while the military body's technical authorities are responsible for developing and operating the cyber defenses being developed.(Nato, n.d.)

In conclusion this policy is being made to ensure that NATO and its members are able to defend itself from cyber attacks especially those from adversary nations by  having a strong interworking system that allows for all of its members to work together to ensure security amongst the alliance, which will allow for faster, more efficient responses and containment of any cyber breach going forward and then for The implementation of this new policy. NATO will

be splitting the responsibility of implementation amongst its three bodies which include its political, military and technical body. This will ensure that everything going together to make this happen flows well and without interference.

SOURCES

Giordano, P. (2024, December 3). *Strengthening Cyber Resilience: NATO's Cyber Coalition and Collective Defence - NATO's ACT*. NATO's ACT. https://www.act.nato.int/article/cyber-coalition-collective-defence/

Nato. (n.d.). *Cyber defence*. NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm

Nato. (n.d.-b). *Stratégie de mise en œuvre de la transformation numérique de l'OTAN*. NATO. https://www.nato.int/cps/fr/natohq/official_texts_229801.htm?selectedLocale=en